Page No.:
Date : / /

INDEX

Se. No	TOPIC	Page no
1.	**Network Models**	
	1.1 What is Models	
	1.2 OSI Vs TCP/IP Models	
	1.3 Walking through OSI and TCP/IP	
	1.4 Meet the frame	
	1.5 The MAC Address	
	1.6 BroadCast Vs UniCast	
	1.7 Introduction to IP Addressing	
	1.8 Packets and Ports	
2.	**Cabling And Topology**	
	2.1 Network Topology	
	2.2 Coaxial Cabling	
	2.3 Twisted pair Cabling	
	2.4 Cat Ratings	
	2.5 Fiber optic Cabling	
	2.6 Fire rating	
	2.7 Legacy Network Connections	
3.	**Ethernet Basics**	
	3.1 What is Ethernet	
	3.2 Ethernet Frames	
	3.3 Early Ethernet	
	3.4 The Daddy of Ethernet, 10BaseT	

Page No.:
Date: / /

3.5 Terminating twisted pair
3.6 Hubs Vs Switch

4. Modern Ethernet
4.1 100 Base T
4.2 Connecting Switches
4.3 Gigabit Ethernet & 10Gigabit Ethernet
4.4 Transceivers
4.5 Connecting Ethernet Scenarios

5. Installing a Physical Network
5.1 Introduction to Structure Cabling
5.2 Terminating Structured Cabling
5.3 Equipment Room
5.4 Alternative Distribution Panels
5.5 Testing Cable
5.6 Troubleshooting Structure Cabling
5.7 Troubleshooting Structure Cabling 2
5.8 Using a Toner and Probe
5.9 Wired Connection Scenarios

6. TCP OR IP Basics.
6.1 Introduction to IP addressing Binary
6.2 Introduction to ARP
6.3 Class full Addressing
6.4 Subnet Masks
6.5 Subneting with CIDR

6.6 More CIDR Subnetting Practice
6.7 Dynamic and static IP Addressing
6.8 Rogue DHCP servers
6.9 Special IP Addresses.
6.10 IP Addressing Scenarios.

7. # ROUTING

7.1 Introducing Routers
7.2 Understanding Ports
7.3 Network Address Translation.
7.4 Implementing NAT
7.5 Forwarding Ports
7.6 Tour of a SOHO Routers.
7.7 SOHO vs Enterprise
7.8 Static Routers
7.9 Dynamic Routing
7.10 RIP
7.11 OSPF
7.12 BGP

8. # TCP or IP Applications.

8.1 TCP and UDP
8.2 ICMP and IGMP
8.3 Handy Tools.
8.4 Introduction to wireshark
8.5 Introduction to netstat
8.6 Web Server
8.7 FTP
8.8 E-mail Server and client

Page No.:
Date: / /

8.9 Security E-mail
8.10 Telnet and SSH
8.11 Network Time Protocol
8.12 Network Service Scenarios

9. Network Naming
9.1 Understanding DNS
9.2 Applying DNS
9.3 The Host file
9.4 Net Command
9.5 Windows Name Resolution
9.6 Dynamic DNS
9.7 DNS Troubleshooting

10. Securing TCP or IP
10.1 Making TCP/IP Secure
10.2 Symmetric encryption
10.3 Asymmetric encryption
10.4 Cryptographic Hashes
10.5 Identification
10.6 Access Control
10.7 AAA
10.8 Kerberos EAP
10.9 Single sign-on
10.10 Certificates and Trust
10.11 Certificates Error Scenarios

11. Advanced Networking Devices

Page No.:
Date: / /

11.1 Understading IP Tunneling
11.2 Virtual private Network.
11.3 Introduction to VLANs.
11.4 Inter VLAN Routing
11.5 Interfacing with managed Switch.
11.6 Switch Port Protection.
11.7 Port Bonding
11.8 Port Mirroring
11.9 Quality of Services
11.10 IDS vs IPS
11.11 Proxy Server
11.12 Load balancing
11.13 Device placement Scenarios.

12. IPV6

12.1 Introducing to IPv6
12.2 IPv6 Addressing
12.3 IPv6 in Action.
12.4 IPv4 and IPv6 Tunneling

13. Wireless Networking

13.1 Introduction to 802.11
13.2 802.11 Standards
13.3 Power over Ethernet (PoE)
13.4 Antennas
13.5 Wireless Security Standards.
13.6 Implementing wireless security
13.7 Threats to your wireless network
13.8 Retro threats

13.9 Wi-fi Protected setup (WPS)
13.10 Enterprise wireless
13.11 Installing a wireless network.
13.12 Wireless Scenarios
13.13 More wireless Scenarios

14. Virtualization And Cloud Computing

14.1 Virtualization Basics
14.2 Cloud ownership
14.3 Cloud implementation
14.4 Your first Virtual machine
14.5 NAS and SAN
14.6 Platform as a Service (PaaS)
14.7 Infrastructure as a service (IaaS)
14.8 Software as a Services (SaaS)

CompTIA NETWORK + Cert. (N10-007)

★ Introduction ⇒ Network + is a CompTIA Computer networking certification that includes Computer network Concepts, installation and configuration, media and topologies, management and security.

Network models

- OSI (Seven layer models) ↓ (Open Systems Interconnection model)
  - 7) Application
  - 6) Presentation
  - 5) Session
  - 4) Transport
  - 3) Network
  - 2) Data link
  - 1) Physical
- TCP/IP (model) (Transmission Control protocol / Internet protocol)
  - 4) Applications
  - 3) Transport
  - 2) Internet
  - 1) Network Interface

Low to High

OSI model + TCP model.

OSI model		TCP model
7) Application	}	4) Application.
6) Presentation	}	
5) Session	}	
4) Transport	=	3) Transport
3) Network	=	2) Internet
2) Data link	}	1) Network Interface (link)
1) Physical	}	

=> (NIC) Network interface Card

=> multipule Computer Connected through the ethernet

Quick Review

Frames or Packets are created and destroyed inside the network interface Card (NIC)

Devices on a network Send and received data in discreet Chunks Called frames/packet

frames are a maximum of 1500 bytes in sizes.

MAC address

* Media Access Control (MAC) address

Physical address ⇒ MAC address

MAC address ⇒ 40 - 8D - 5C - 1C - 5A - 50

⇒ each character is a 4 bit and the total character is 12 than the mac address is 4 × 12 = 48 bit. 48 bit = 6 bytes.

⇒ The first three paired is called Original Equipment manufacturer (OEM). And the last three paired they know as Unique ID.

CRC ⇒ Cyclic Redundancy Check
CRC is just the use to Verify the Data is good. If the bad Data the Data is refuse the load

A MAC address is a unique 48-bit identifier for a NIC

Frames / packets have destination and source MAC addresses

NICs use MAC addresses to decide whether or not to process a frame

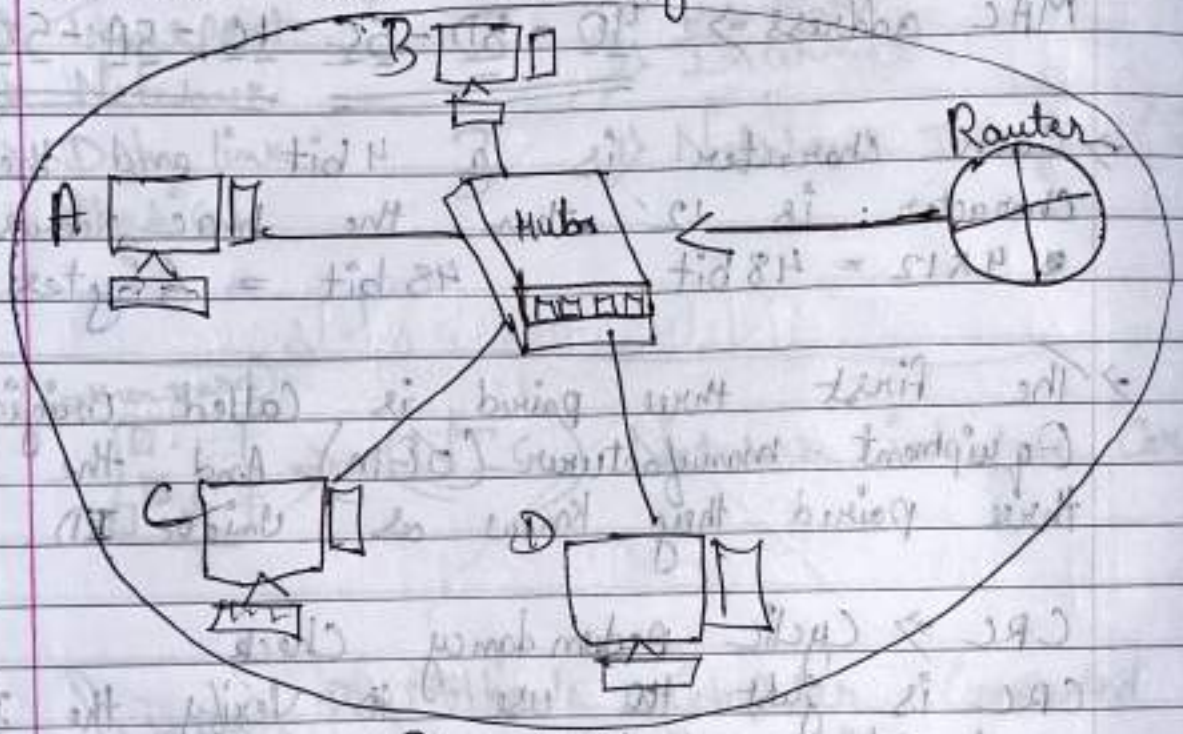
A Unicast Communication is from one device on the network to another device on the Network.

Multicaste Communication is from one device on the network to many But not all device on the network.

@shwetket

Broadcast Vs Unicast

⇒ A Broadcast Domain is a logical division of a Computer network, in which all nodes can reach each other by broadcast at the data link layer.



Broadcast

Quick Review

Unicast transmission is addressed to a single device on a network.

A Broadcast transmission is sent to every device in a broadcast domain

A Broadcast address looks like this :-

FF - FF - FF - FF - FF - FF

A Broadcast Communication is from one device on the network to all device on the network.

OSPF => open system path first

Page No.: 05
Date: / /

IP Address

=> An IP address is a unique address that identifies a devices on the internet or local network. IP stant for "Internet protocol". which is the set of rules governing the format of data sent via the internet or local network.

device # router #

IPv4 31.44.17.231
IPv6 2001:0DB8:FE01::

} IP address looks likes this

A router Connects multiple local area network.

The IP packets within the frame never changes.

Packets and ports

=> ports numbers are unique to individual application that is used all over the internet.
For ex => port 80 is used for (HTTP) Hypertext Transfer protocol.

=> There are 0-65535 ports But the first 1024 port are reserved or well known ports.

(Segment)

TCP => Transmission Control protocol

=> Transmission Control protocol is a Connection oriented Conversation. TCP is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP include mechanisms to solve many of the problems that arise from packet based messaging, such as lost packets, out of order packets, duplicate packets, and Corrupted packets.

(Datagram)

UDP => User Datagram protocol

=> User Datagram protocol is a Connectionless Conversation. UDP is a Communication protocol that is primarily used to establish low-latency and loss-tolerating Connection between applications on the Internet. UDP is an alternative to Transmission control protocol.

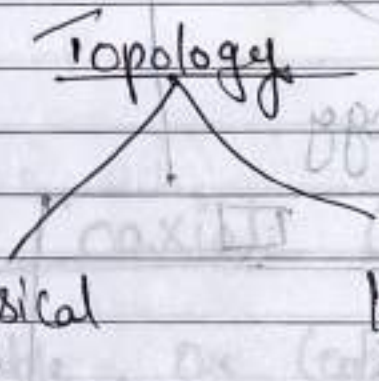
---

quick review

Port number help direct packet traffic between the Sources and destination.
packets have Sequence number so the network Software can reassemble the file correctly.
TCP is Connection-oriented, UDP is Connectionless

NETWORK TOPOLOGIES

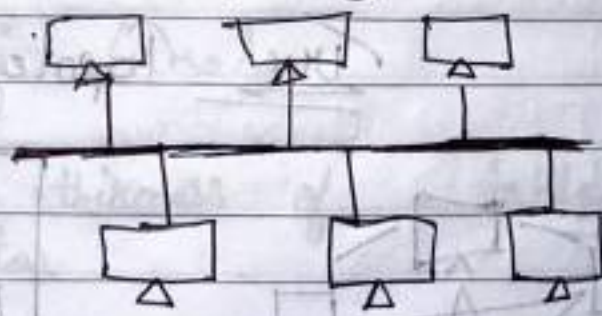
⇒ Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology



- Physical topology is the geometric representation of all the nodes in a network.

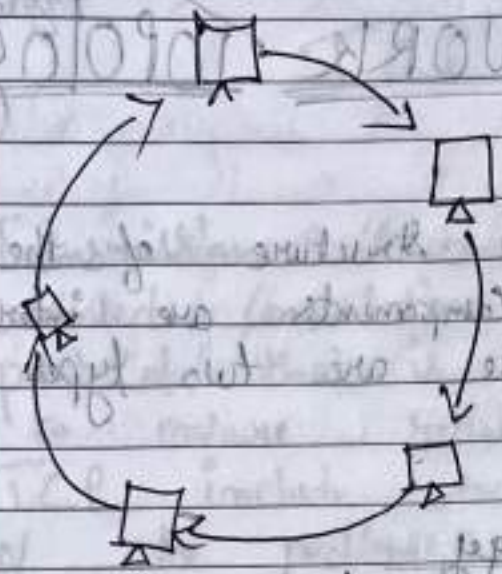
* Type of Network Topology :-

1. BUS
2. Tree
3. Ring
4. Star
5. Mesh
6. hybrid.
7. point to point.

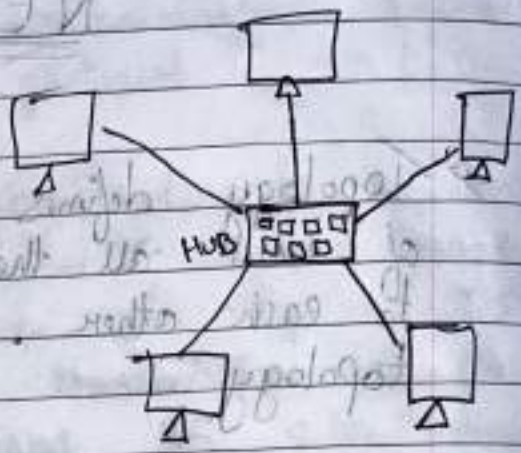


Bus Topology

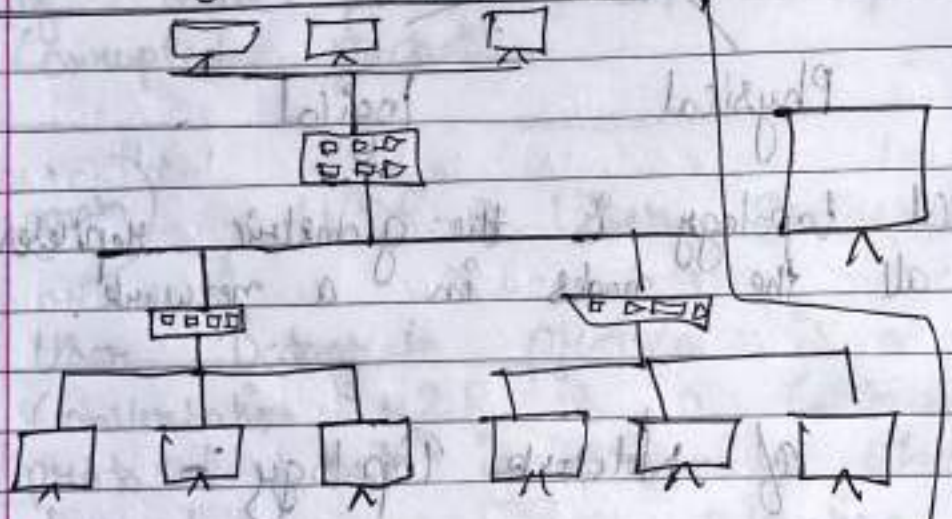
Page No.: 08
Date: / /



Ring Topology.

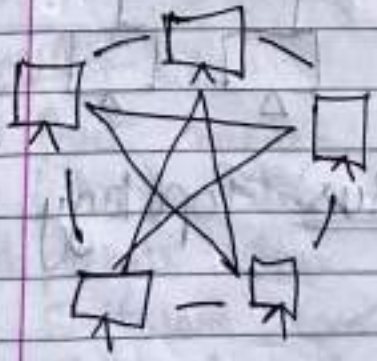


Star Topology.

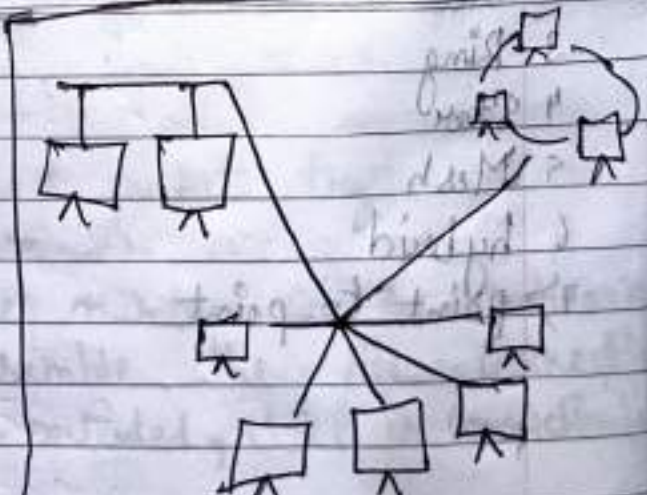


Tree Topology

Point to point Topology.



Mesh Topology



HYBrid Topology.

Quick revision

Star-bus topology is considered a hybrid topology

when each host is interconnected this is considered a fully meshed topology.

Logical topology is the electronic circuit flow of frames.

Coaxial Cabling

⇒ Coaxial Cable, or Coax is a type of electrical Cable consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric; many coaxial cables also have a protective outer sheath or jacket.

RG ⇒ Radio Grade

RG Define the thikness of a Cable and the thickness of conductor.

OHMs is a messurement of ressisdent

* There are many types of Coaxial Cable like:

1) RG-58 — 50 OHMs
2) RG-59 — 70 OHMs
3) RG-6 — 75 OHMs

Quick Review

RG specifies the thickness of the Conductor insulation, and Shielding.

Coaxial Cable has two Conductors, one Center point, and a tubular Conducting layer.

RG-59 has a 75 ohms rating and uses a threaded F-type Connector

Twisted Pair Cabling

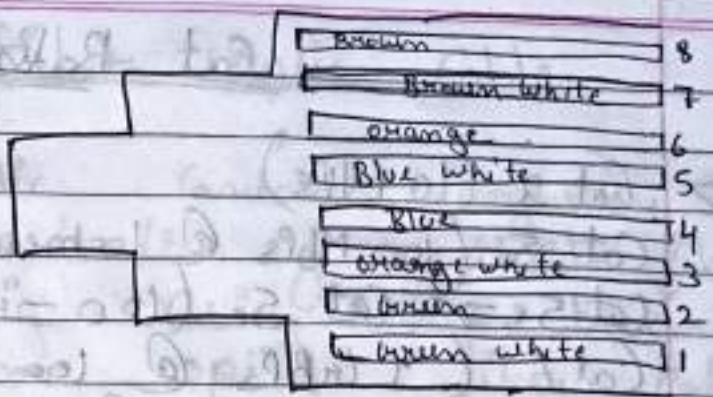
=> Twisted pair Cabling are a type of guided media. It was invented by Alexander Graham Bell. Twisted pair Cable have two Conductors that are generally made up of Copper and each Conductor has insulation. These two Conductor are twisted together, thus giving the name twisted pair Cable.

UTP => Unshielded twisted pair
STP => Shielded twisted Pair.
RJ 45 is a Connector.

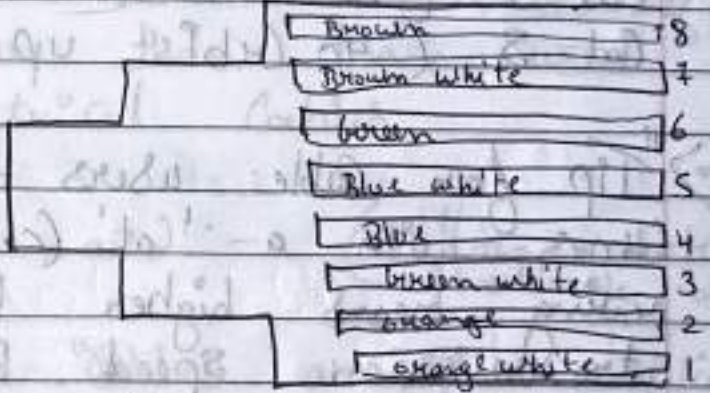
There are Two big Standard to Connect the Cable into Connector.

(1) EIA/TIA 568A (TIA is a Current Standard)
(2) EIA/TIA 568B

568 A



568 B



only orange & Green are change there places

Quick Review

Modern twisted pair has 4 or more pairs of Cable.

UTP Cable is unshielded and subject to signal interface from environment factors.

568A and 568B are wiring standards for how the wires are connected to a connecto

Cat Rating

=> Cat 3 (10 MbPs)
Cat 5 (100 MbPs @ 100 meters)
Cat 5e -> Cat 5e (100 - 1000 MbPs @ 100 meters)
Cat 6 (1 GbPs @ 100 meters)
Cat 6a (10 Gbps @ 100 meters)
Cat 7 (10 Gbps @ 100 meters, Shielded)
Cat 8 (40 Gbps up to 30 meters).

=> "Tip for Cable users - Each Ethernet cable comes with a 'Cat' (category) rating. Higher Cat rating means higher bandwidth and data transmission speeds". Run a speed test on their network to determine the actual speed. For ex - Cat 7 cable for a 50 Mbps connection could be overkill.

Quick Review

UTP Cat Rating define the speed and cable length specifications.

Cat ratings have a different number of twists per inch.

Cat 6a and Cat 7 are both rated for 10 GBPs speed and up to 100-meter cable length.

fiber optic Cable

=> A fiber - optic contains anywhere from a few to hundreds of optical fibers within a plastic casing. Also known as optic Cables or optical fiber Cables, they transfer data signals in the form of light and travele hunderds of miles significantly faster than those used in traditional electrical Cables.

Type of Cable are :- (Difference between multimode fiber & singlej

Simplex => Simplex Cables are fiber optic Cables with a single optical fiber. They are used in application that only require on-way data transfer. Simplex is available in Sigle mode and multimode.

Duplex => Duplex Cable are fiber optic cables with two optical fibers. They are usually set up side-by-side and can be used for application that required simultaneous, bidirectional data transfer. Duplex fiber is available in single mode and multimode.

Multimode Cables Carry LED Signals.
Eg. Single-mode Cable Carry laser signals.
for the test, be able to recognize the diffrente types of fiber Connectors.

DNS type

Fire rating

⇒ The Cable that will continued to operate in the presence of a fire is called fire-resistive or fire-rated Cable.

Quick Review

Plenum-rated Cable is the most fire resistant.

Cable fire rating is normally clearly marked on the manufacture's box.

Non-plenum is not considered fire/smoke resistant.

Lagacy Networks Connections

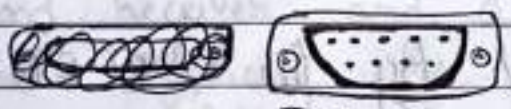
⇒ A legacy network is the generic name assigned to any old network, which is really used today and not part of the TCP/IP protocol suite. Legacy network are mostly propitary to individual Vendors.

* Serial Ports ⇒ a serial port is a serial communication interface through which information transfers in or out sequentially one bit at a time. This is in contrast to a parallel port, which communicates multiple bits simultaneously in parallel.

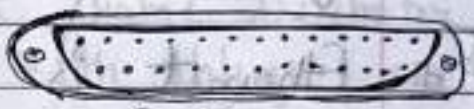
Rain II — 7 Pages PPT / file

Page No.: 15
Date: / /

* Parallel ports ⇒ Parallel ports is a type of interface found on early computers for connecting peripherals. The name refers to the way the data is sent; parallel ports send multiple bits of data at once, as opposed to serial communication in which bits are sent one at a time.



DB-9
serial ports



DB-25
parallel ports

Quick Review

DB-9 and DB-25 are legacy Serial Network Connections.

Parallel ports were typically used with printer.

A yost (or rollover) Cable is a serial cable used to configure a router or switch.

Ethernet

=> Ethernet is a family of wired computer networking technologies ~~computing~~ commonly used in local area network (LAN), metropolitan area network (MAN) and wide area network (WAN). For the OSI Model, Ethernet provides services up to and including the data link layer.

Quick Revision

Ethernet is defined by the IEEE 802.3 Standard

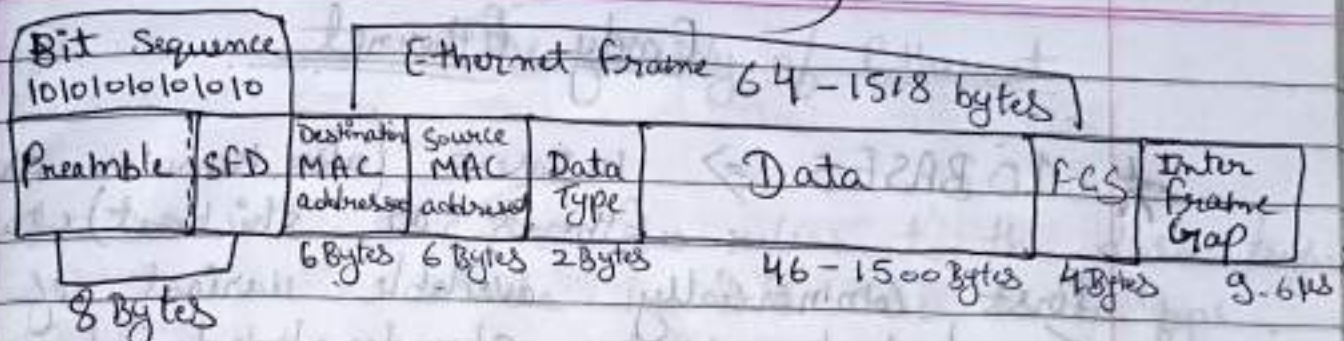
The IEEE has define many versions of Ethernet

For the test, be able to recognize the Ethernet.

Ethernet frames

=> When transmitting data over Ethernet, the Ethernet frame is primarily responsible for the correct rule making and successful transmission of data packets. Essentially, data sent over Ethernet is carried by the frame. An Ethernet fram is between 64 bytes and 1518 bytes big depending on the size of the data to be transported.

(Protocol Data units)



The packets Starts with preamble that Controls the Synchronization between Sender and receiver and a "Start frame Delimiter" (SFD) that Defines the frame Both Values are bit sequence in the format "10101010..." in which the actual frame contain information about Source and destination address (MAC format), Control information (in the case of Ethernet II the type field, later a length specification), followed by the transmitted data record. A frame Check Sequence (FCS) is an error-detecting code that Closes the frame (expt for the preamble and SFD). The packet is completed by an "Interframe Gap", which defines a 9.6 µs transmission pause.

Quick review

Ethernet frames consist of a preamble, destination MAC, Sources MAC, data type, Data, pad, and FCS.

A jumbo frame can carry 9000 bytes.

FCS is used for error detection.

Early Ethernet

* 10BASE-5 => 10 Base-5 (also known as thick Ethernet or thicknet) was the first commercially available variant of Ethernet. The technology was standardized in 1982 as IEEE 802.3. 10Base5 uses a thick and stiff coaxial cable up to 500 metres (1600 ft) in length.

(CSMA/CD) => Carrier-Sense multiple access with Collision detection.

Terminating resistor => Termination resistor is a single resistor placed at the end of an electrical transmission line.

* 10 Base-2 => is among the family of Ethernet network standards for local area network (LAN) that uses a thinner version of coaxial cable to establish a network path or medium and operates at a speed of 10 Mbps to carry out baseband transmission. 10Base-2 is also known as cheapernet, thinwire, thinnet and thin Ethernet.

Quick Review
CSMA/CD stands for Carrier Sense multiple access Collision detection
10Base5 and 10Base-2 require terminating resistors at both ends of a Segment (Cable)
When connecting to 10Base-2, always use a "T" connector

The Daddy of Ethernet

=> 10 Base-T => The 10 refers to the data trafer rate in this case is 10Mbps. The word Base refers to base band, as oppose to broad band. T means twisted pair, which is the cable we use for the Network. 10Base-T System operate at 10 Mbps and uses baseband transmission method. and also called Twisted pair Ethernet.

MSAU => Multistation access unit.

10 Base-T runs at 10 Mbps over Cat3 or better UTP

10 Base-T Can have up to 1024 nodes per switch

10 Base-T Cable runs are a maximum of 100 meters between the Switch and node.

Terminating twisted pair

=> It mean the Cable are end One to other side that called Terminating twisted pair (Ethernet). There are two type of Cable Straight through Connector and Crossover Connector.

* Straight through Connector are start and end with a 568A Cable management. One side

into the Switch and other side into the Desktop.

* Crossover Cable is a Crossover Cable for Ethernet used to connect computing device together directly It is often used to connect two devices of the same type Eg/ two computer or two switches to each other.

* 8P8C Connector = RJ-45
This Connector is used for the Ethernet Cable to Connect the Switch or PC.

Quick Revise # An RJ-45 (8P8C) Connector is used to Connect to most network Cards.

Watch the position of the wires when Crimping to follow 568A or 568B Standards

Straight-through Cables are the most Common used Cable in Networks.

Hub Vs Switch

Quick Revise # Switch forward frames based on MAC Addressed

Hubs use CSMA/CD to avoid Collisions

Switches create and use MAC address tables to map Ports and host devices.

Collision Domain => Collision Domain is a network segment (medium) connected by a shared medium or through repeaters where simultaneous data transmissions collide with one another.

Crash

Page No.: 21
Date

Hub Vs Switches

=> Hub => Hub is a networking devices which is used to transmit the signal to each port (except one port) to respond from which the signal was received. Hub is operated on physical layer. In this packet filtering is not available. It is of two types: Active Hub, Passive Hub.

=> Switch => Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on Data link layer. In this packet filtering is available. It is type of full duplex transmission mode and it is also called efficient bridge.

Hub	Switch
=> Hub is operated on physical layer of OSI model	while switch is operated on Data link layer of OSI Model
=> Hub is a broadcast type transmission.	While switch is a unicast, multicast and broadcast type transmission
=> In hub, there is only one collision Domain.	While in switch different ports have own collision domain
=> Hub is not an intelligent device that send message to all ports hence it is comparatively inexpensive. Hub is a simply old type of device is not generally	While Switch is an intelligent device that send message to selected destination so it is expensive. Switch is very sophisticated device & widely used.

Quick Review

100 Base T

⇒ Introduction in 1995 and officially the IEEE 802.3u Standard, 100 Base-T is a 100 Mbps Version of the 10 Mbps 10 Base-T like 10 Base-T, 100 Base-T is a Shared media LAN when used with a hub (all nodes shared the 100 Mbps) and 100 Mbps between each pair of nodes when used with a Switch.

Quick Review

Full-duplex mode allows both sides of a Conversation to occur at the same time.

100 Base (a.k.a 100 Base Tx) runs at 100 Mbps up to 100 Meters.

100 Base fx, a fiber Solution, runs at 100 Mbps up to 2 kilometers.

Connecting Switch

⇒ There are two types of Table are:-

1. Straight-through Cable. (Describ in Twisted pair)
2. Crossover Cable. (" ")

Quick Review

Straight-through Cables have identical ends. Such as 568B or 568A

Crossover Cables have different ends - 568A and 568

Connect Switch directly with Crossover Cable.

Transceiver

-> The transceiver is an important part of fiber optics network and is used to convert electrical signals to optical (light) signals and optical signals to electrical signals. It can be plugged into or embedded into another device within a data network that can send and receive a signal.

Fiber-optic cable supports multiple connection types from various vendor MSAs (multisource Agreement)

SFP and SFP+ are small form-factor transceivers (small form factor pluggable) (Enchanced small form-factor pluggable)

QSFP is designed for 40 Gbps Ethernet

Connecting Ethernet Scenarios

Introduction of Structure Cabling

=> In telecommunications, structured cabling is building or campus cabling infrastructure that consists of a number of standardized smaller element (hence structured) called subsystem. Structure cabling components include twisted pair and optical cabling, patch panels and patch cables.

Quick Revision
Structured cabling defines how we install cabling
TIA standards specify wiring standards for structure cabling.
Patch panels terminate one end of horizontal runs
Patch cable connect switches to patch panels and computer to wall outlets.

Terminating Structure Cableing

=> Cable Termination is the connection of the wire or fiber to a device, such as equipment, panel or a wall outlet, which allows for connecting the cable to other cables or device.
During Termination, you press the cable between two edges of a metal clip, which displaces the insulation and exposes the copper conductor.

Quick Reference
RJ-45 Crimps are used only on patch cable
Horizontal run are terminated with 110-punchdown
Patch panels and RJ-45 Connectors also have Cat Ratings.

Equipment room

=> An equipment room is a room or space within a building for the storage or installation of mechanical or electrical/electronic devices.
The main Equipment Room (ER) serves as the demarc location for the building. It is the transitional point from the voice, data and video building feeds to house cable running to telecommunication closets.

Quick Review
The primary equipment room is called the main distribution frame (MDF)

Rack-mounted equipment is standardized at 19" wide and a multiple of 1 3/4" tall (called a U or RU unit)
The Demarc separates the telecom company's property from your responsibity.

Alternative Distribution panels

A 66-punchdown block is a very old patch panel typically used in non-VoIP telephone systems.

A 110-punchdown block patch panel is the way to distribute copper wired networks.

A fiber distribution patch panel is used to distribute fiber-optic network.

TDR => Time Domain reflectometer

Page No.: 26
Date: / /

Testing Cable

=> WireMap => A wiremap checks the wiring sequence of UTP Cable. The test show whether the installer properly or improperly connected the wires to the jack or plug. Any wire that is open is actually broken at some point inside the wire or is not properly connected.

Quick Review
understand how to read and interpret the wiremap feature of a cable tester.
Continuity testing will show if the cable has any breaks
A Time domain reflectometer (TDR) will show the length of the cable and help pinpoint mid-cable brea

Troubleshooting structured cabling (part 1)

Quick Review
Loopback plugs test the NIC's ability to send and re
Loopback plugs aren't effective (But network+ think toy
Patch cable and wall outlets are the most common part of structured cabling to fail.

Troubleshooting structured cabling (part 2)

Voltage monitors track and record problems with power
Environmental / Temperature monitors track and record problems with heat and humidity.
TDRs are great tools to check for break on horizontal runs.

Using Toner and probe

=> A tone and probe kit is the tool that job. It can trace wires inside walls, under floors and above ceilings.

Tone generators and tone probes are used to locate cables and connections.
Tone generators create the signal for the probe
Tone probe translate the signal into an audible Tone

Wired Connection Scenarios

(1) => Attenuation in networking => Attenuation is the loss of signal strength in networking cables or connections. It may cause signals to become distorted or indiscernible.

(2) => Jitter in networking => Jitter is when there is a time delay in the sending of these data packets over your network connection.

(3) => Incorrect Cable
(4) => No Connection
(5) => Bent Pins

Quick Revise
For jitters in VoIP and Video Streaming, consider buffering or increasing speed.
Make sure the patch specification is up-to-date with the network speed.
If switch light are not blinking, try different ports or check if it's an uplink port.

If you convert IP addressed to Binary or Binary to address, watch this video (unit-7 TCP or IP Basic)

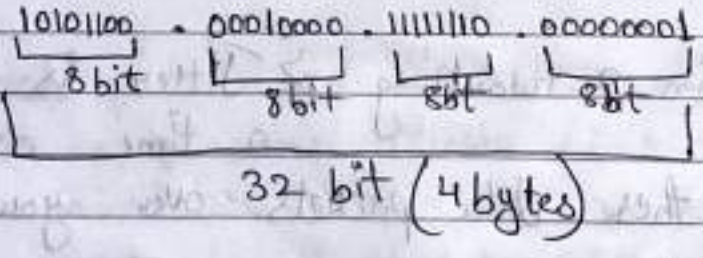
Introduction to IP addressing and Binary

=> IP address stand for internet protocol address it is an identifying number that is associated with a specific computer or computer network.

An IP address is a Thirty-Two-bit binary number. The Thirty two bits are separated into four groups of eight bits called octets. However, an IP address is represented as a dotted decimal number (for example :-

205.57.32.9 => (IP addressed)

=> 172.16.254.1 (Dotted-Decimal notation)



Quick Review

Each Computer on a TCP/IP network must have a unique IP address

IPv4 addresses are written as four octets, such as 192.168.4.12

Each octet represents a binary string; 192 for Example, is 11000000

Introduction of ARP

=> The Address Resolution Protocol is a communication Protocol used for discovering the link layer address, such as a MAC address.

ARP broadcasts a request packets to all the machines on the LAN and asks if any of the machines are using that particular IP address. When a machine recognized the IP address as its own, it send a reply So ARP can update the cache for future reference and proceed with the communication.

Quick Revise
ARP resolves IP addressed
ARP is what a computer uses when it knows the IP address, but needs the MAC address
Type arp -a to see the ARP cache.
ARP requests are broadcast over a network

Classful addressing

=> In classfull addressing, the address space is divided into five classes : A, B, C, D and E. Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and Experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

Quick Revise
1. # Classful Subnetting was the first efforts to devide network IDs
2. # Class A, B and C licenses
3. # Memorize the first octet to know your class licenses.

Subnet Mask

→ A Subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more network is called Subnetting.
A Subnet mask is a 32-bit number used to differentiate the network components of an IP address by dividing the IP address into a network address and host address. A Subnet mask is also knows as an address Mask.

Quick Revision
Each host needs a Subnet mask
The host uses the Subnet mask to know if the destination is on the local network or a remote network
Each host knows the default gateway so that it can forward traffic to remote networks.

Subneting with CIDR

→ Classless inter-Domain Routing (CIDR) notation is a compact methode for specifying IP addresses and their routing suffixes. for example, we can express the idea that the IP address 192.168.0.1 is associated with the netmask 255.255.255.0 by using the CIDR notation of 192.168.

Quick Revision
CIDR - Classless Inter-Domain Routing
Subnet masks have all 1's on the left and all 0's on the right
The more subnets you the less hosts are available.

* Router is also a DHCP

Dynamic and static IP addressed

-> When a device is assigned a static IP address the address, the address does not change. Most device use dynamic IP address, which are assigned by the network when they connect and change over time. A Dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP (Dynamic Host Configuration Protocol) or PPPoE. (Point-to-point protocol over Ethernet)

Each broadcast domain must have only one DHCP Server
Every modern operating System comes with DHCP enabled by default.
DHCP Relay enables a single DHCP Server to service more than one broadcast Domain.

Rogue DHCP Server

(APIPA) [Automatic Private IP addressing]

-> A rogue DHCP Server is a DHCP Server on a network which is not under the administrative control of the network staff. It is a network device such as modem or a router connected to the network by a user who may either unaware of the consequence of their action or may be knowingly using it for network attack such as man in the middle # If you get an APIPA address

If you get an IP address other than your correct network ID. You may have a rogue DHCP Server.

Check to see if you are connected to a DHCP Server # If you are connected to a DHCP Server & still get an APIPA address, make sure the DHCP Server is working.

Special IP Address

=> There are several IP address that are special in one way or another. These addresses are for special purpose are are to be put to special use.

* Addresses significant to every IP subnet
① Network Address
② Broadcast Address

* Address significant to individual hosts
① Loopback Address

* Special Address of Global Significance
① Private Addresses
② Reserved Addresses

Quick Review
Special internal IP addresses are: 10.0.0.0, 172.16.0.0 to 172.31.0.0 and 192.168.0.0
The loopback address for IPv4 is 127.0.0.1 and for IPv6 is ::1
An APIPA address (169.254.0.0) indicates the DHCP Server is Down.

IP address scenario

Quick Review
IPConfig (windows) and ifconfig (Linux) display the IP address information.
Virtual machines can be a Sources of duplicate MAC address errors.
All the computer in our broadcast domain have the Same Subnet

Introducing Routers

=> A Router is a device that connects two or more packet - switched network or subnet works. It serves two primary function: managing between these networks by forwarding data packet to their intended IP addresses, and allowing multiple device to use the same internet connection.

Router => A box that connects network IDs

Gateway router => A gateway is simply a device or hardware that acts as a "gate" between the network.

- # Router only care about destinations.
- # Router can use any network medium.
- # All router have a routing table.

Understanding ports

=> A Port is a Virtual point where network connections start & end. Ports are software based and managed by a computer's operating system. Each port is associated with a specific process or service. A Port is a logical construct that identifies a specific process or a type of network services.

- # Every TCP Packets has two port number.
- # Well known port number runs from 0 to 1023
- # Clients generate ephemeral number that are always between 1024 to 65,535.

Network address Translation (NAT)

=> Network Address Translation (NAT) is a process that enables one, unique IP address to represent an entire group of computers. In network address translation, a network device, often a router or NAT firewall, assigns a computer or computer inside a private network a public address.

There are 3 ways to configure NAT :-

(SNAT) (1) Static NAT - In this, is one-to-one mapping of a private IP address to a public IP address. Static NAT (network address translation) is useful when a network device inside a private network needs to be accessible from internet.

(DNAT) (2) Dynamic NAT - Dynamic NAT can be defined as mapping of a private IP address to a public IP address called as NAT Pool. Dynamic NAT established a one-to-one mapping between a private IP address to a public IP address

(3) PAT NAT => Port address Translation (PAT) is another type of dynamic NAT which can map multiple private IP addressess to a single public IP address by using a technology know as Port address Translation.

Quick Revise
PAT translates internal IP address to an internet address and tracks the packets.
SNAT Sends specific traffic to one internal IP address
DNAT has a limited pool of internet addresses to give to a number of internal devices.

Implementing NAT

Quick Revise
SOHO (Small office / Home office) router ship with NAT enable
NAT on a SOHO router can be disabled from the router's Configuration page
Some older routers call this Setting gateway/ router mode

Forwarding Ports

⇒ In computer networking, port forwarding or Port mapping is an application of network address translation (NAT) that redirects a communi-cation request from one address and port number combination to another while the packet are traversing a network gateway, such as a router or firewall.

Quick Revise
Port forwading allows external devices to have internal communication through a router.
Port triggering will open an alternative assigned port when the initial port is connected (e.g. FTP)
Enabling DMZ when setting up port forwarding places that devices outside the protection of that router.

Tour of a SOHO Router

=> A SOHO router is a broadband router built and marketed for small offices and home offices. Since the workload for these businesses is primarily on the internet, they require a local area network (LAN), meaning their network hardware is structured for that purpose.

All home routers have a default IP address user name & password.
Almost all home routers are DHCP Servers.
Router WAN Connections are commonly DHCP Clients by default.

SOHO Vs Enterprise router

=> Enterprise router => A network device that forward data packets from one network to another. The "enterprise" means that implementation requires a knowledgeable network proffessional. Enterprise router have numerous Ethernet port and can be very large and costly handling millions of packets of internet Traffic Per Second.

SOHO router are for small groups (5-6 devices) and can have build-in capability for switches, firewall and
Enterprise router have expanded connection Cabability to other devices (Ex - router, switches, & wifi
SOHO router often have web-based interfaces; enterprise router topically have their own OS interface

Static Router

=> Static Routing is also known as non-adaptive routing which doesn't change routing table unless the network administrator change or modify them manually. Static routing does not use complex routing algorithms and it provides high or more security than dynamic routing.

A Static route is a fixed route that is manually configured and persistent
Use route print or netstat -r to Display current known routes from the routing table
Routing table Contain address information for destination, subnet mask, gateway, and NIC.

Dynamic routing

=> Dynamic routing is a technique in which a router learns about routing information without an administrator's help and adds the best route to its routing table. A router running a dynamic routing protocol adds the best route to its routing table and can also determine another path if the primary route goes down. Example of dynamic routing protocol are BGP, EIGRP, OSPF and RIP.

Dynamic routing protocol use metrics to determine routes and are either distance Vector or link state.
Dynamic routing protocol are either IGP (Interior Gate way Protocol) or EGP (Exterior Gateway protocol)
BGP is the EGP Protocol used for inter-Autonomous System routing.

RIP (Routing information Protocol)

⇒ The routing information Protocol is one of the oldest distance-Vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loop by implementing a limit on the number of hop allowed in a path from sources to destination.

RIP is a Distance Vector protocol that uses hop count to determine routes
RIP 1 used only class full network.
RIP's maximum hop count is 15.

OSPF (open shortest path first)

⇒ Open shortest path first (OSPF) is a link State routing protocol that was developed for IP network and is based on the Shortest Path first (SPF) algorithm. OSPF is an interior gateway protocol (IGP).

OSPF is a link State Protocol # OSPF uses Area IDs # OSPF Converges very quickly.

BGP (Border Gateway protocol)

⇒ BGP (Border Gateway protocol) is the protocol underlying the global routing system of the internet. BGP is a standardize exterior gateway protocol designed to exchange routing and reachability information between autonomous System (AS) on the internet.

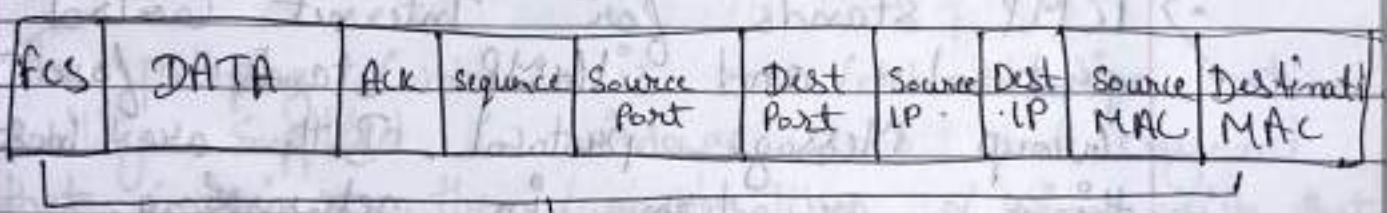
BGP is a hybrid protocol.
BGP is the primary protocol for the internet
BGP is based around the concept of autonomous system.

* TFTP uses UDP
* Internet uses TCP

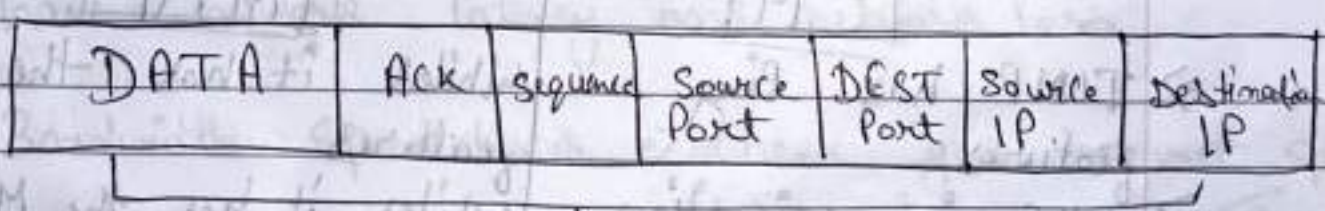
TCP and UDP protocol

=> TCP is a Connection oriented protocol, whereas UDP is a Connectionless protocol. A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler and efficient protocol, however, retransmission of lost Data packets is only possible with TCP.

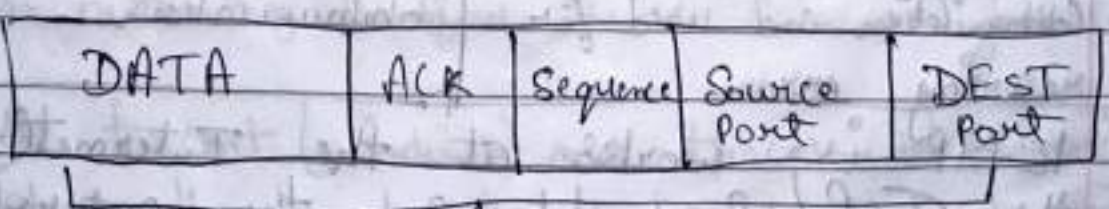
PDU => Protocol Data units.
TFTP => Trivial File Transfer protocol
Example :-



Ethernet frame



IP Packets



TCP & UDP

Ethernet frames are used by switch and router.
PDU is the information used by the different protocols provided in frame segments.
TCP is connection-oriented; 2-way communicat initiated by a 3-way handshake process (Syn, Syn-ack, ack).
UDP is a connectionless-oriented protocol, has low overhead with one-way communication.

ICMP and IGMP

=> ICMP stands for Internet control Message protocol and IGMP stands for Internet Group Message protocol. Both are most important things or term in networking.

ICMP	IGMP
=> ICMP has Ping features	while it has the Multicast features
=> ICMP is unicasting	while it has the Multicast
=> It controls the unicast communication and used for reporting error.	It controls the multicast communications.

Quick revision

ICMP is works at the Internet(2) layer in the TCP/IP model and the network(3) in the OSI model.
IGMP provides multicasting support
Multicast address always start with 224

Handy Tools

- Commands :-
  tracert (windows) = traceroute (Linux)

=> The Traceroute command (tracert) is utility designed for displaying the time it takes for a packet of information to travel between a local computer and a destination IP address or domain.

=> Commands :-

pathping

The pathping command is a command-line network utility supplied in windows 2000 and beyond that combines the functionality of ping with that of tracert. It is used to located spots that have network latency and network loss.

=> Bandwidth Speed tester => Cheak your internet spead in under 30 sec. The speed test usually transfers less than 40MB of data but may transfered more data on fast connections.

Both tracert (windows) and traceroute (Linux) commands display the hops through a router to reach a destination.
using the alternative command pathping can get a quicker ping response from the routers.
Bandwidth speed testing helps verify the upload and download speeds to an individuals computer.

Introduction to wireshark

=> Developed in 1998, wireshark has become the de-facto Standard for analyzing and inspecting network packets. In short, it's a packet analyzing tool which lets you sniff the network and helps to view the traffic which goes in and out of your network adapter (either wired or wireless). Wireshark capture network traffic from Ethernet, Bluetooth, wireless (IEEE 802.11), Token Ring, Frame Relay Connections and more.

tcpdump => Alternative capture tool.
↓
Commands

=> tcpdump is a data-network packets analyzer Computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

wireshark is a protocol analyzer, integrated with a frame capture tool
wireshark displays the traffic flow of Ethernet frames and can drill down into the frame - Viewing various protocols, ports, timelines, and servi
wireshark can segment and organize the Data into consumable information to help in trouble - Shooting.

Introduction to netstat

-> The netstat Statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connection, routing tables, port listening, and usage statistics are common uses for this command.

The netstat command lists all open ports and network connections on a computer.
Run netstat at the command prompt.
Make sure to know the netstat switches display in the episode.

Web Server

-> A web server is a computer that runs websites. It's a computer program that distributes web pages as they are requisitioned. The basic objective of the web server is to store, process and deliver web pages to the users. This intercommunication is done using Hypertext Transfer protocol. (HTTP). Leading web servers include Apache, Microsoft Internet information Services (IIS) and Nginx -- pronounced engine X.

Web Servers host web sites; Web clients access web server
HTTP uses TCP Port 80 by default
HTTPS uses TCP Port 443 by default

FTP - is not an encrypted protocol.

The GET command downloads and PUT command uploads

FTP (File Transfer protocol)

=> The file transfer protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client-server model architecture using seprate control and data connection between the client and the server.

FTP is a file transfer protocol, consider SFTP as a more secure method.

FTP servers listen on port 21 and send data back to the client on port 20.

FTP is not encrypted so all passwords and data are sent in the clear.

Email Server and Client

=> A mail server is a software that runs on a server (computer machine) and constantly communicates over the internet. It processes any ~~recipient~~ received email and sends each email to a recipient, designated by the sender. The mail client is an software application, the program you use to view your message and manage them. The server stores incoming mail for distribution to local users and sends out outgoing message. This uses a client-server application model to send and receive messages using simple mail Transfer protocol (SMTP).

SMTP uses port 25
POP3 uses port 110
IMAP uses port 143.

TLS => Transport Layer Security

SMTP -> Simple mail Transfer Protocol

POP3 => Post office protocol (version 3)

Securing E-mail

=> STARTTLS => startTLS is an email protocol command that tells an email server that an email client, including an email client running in a web browser, wants to turn an existing insecure connection into a secure one.

★ Encrypting email

- Traditional email => SMPT port 25 - unencrypted
  POP3 port 110 - unencrypted
  IMAP port 143 - unencrypted
- Implementing TLS => IMAP 143 -> 993 encrypted
  POP3 110 -> 995 encrypted
  SMTP 25 -> 465 encrypted
- STARTTLS => IMAP, POP3, SMTP - port 465
  TLS/STARTTLS conflicted with port 465
  STARTTLS Change to port 587

IMAP => Internet Message Access protocol.

Quick Review

SMTP, POP3, and IMAP are unencrypted e-mail protocols
Implementing unencrypted e-mail protocols with TLS has complex port assignments.
The STARTTLS extension used only one port 587 for encrypted communication.

Telnet and SSH (Secure Shell)

=> Telnet -> is a application protocol used on the internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. port number is 23.

=> Secure Shell (SSH) => The secure shell protocol is a cryptographic network protocol for operating network services securly over an unsecured network. Its most notable application are remote login and command-line execution. SSH application are based on a client-server architecture connecting an SSH client instance with an SSH server. port number is 22.

Telnet is unencrypted and run over TCP port 23.
SSH runs over port TCP port 22.
SSH is fully encrypted and has almost completely replaced telnet.

Network Time protocol

-> Network Time protocol (NTP) is a protocol that allows the synchronization of system clocks (from desktops to servers). Having synchronized clock is not only convenient but required for many distributed applications. Therefore the firewall policy must allow the NTP service if the time comes from an external server.

NTP is a networking protocol for clock synchronization.
NTP uses port 123, There are hundreds of NTP Server worldwide.

Network Service Scenarios

=> DHCP issues => A(DHCP) Dynamic Host Configuration prototol problems are :- Server not giving out address. Client receiving address already statically assigned to Server or reserved device. Client unable to reach external network (off subnet). Client unable to use the internet with domain names. Client not receiving domain name suffix.

=> DHCP Scope => A DHCP scope is a valid range of IP addresses that are available for assignment or lease to client computers on a particular subnet. In a DHCP Server, a scope is configured to determine the address pool of IPs that server can provide to DHCP clients.

=> IPAM => IP address Management (IPAM) is the administration of DNS and DHCP, which are the network services that assign and resolve IP addresses to machines in a TCP/IP network. Simply put, IPAM is a means of planning, tracking, and managing the internet protocol address space used in a network.

DHCP Scope ranges need to consider gateways, printers, and other types of hosts to provide for IP reservation.
MAC reservation can be used to define devices that have top priority for address assignment
IPAM tools track and manage allotted IP addresses, keeping address requirement available for server and VM farms

---

NETWORK NAMING

Understanding DNS

=> The Domain Name system (DNS) is the phonebook (contactlist) of the Internet. Human access information online through domain names, like nytimes.com or espn.com. Web browsers interact through internet protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load internet resources.

* FQDN => A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the internet. The FQDN consists of two parts: the hostname and the Domain name. For example, an FQDN for a hypothetical mail server might be mymail.somecollege.edu.

Root Domain -> includes Domain name and top-level Domain.

Example :-

Domain name (or) Second level Domain.

URL -> www . totalsem . com

Uniform Resource Locator

Hostname

Root Domain

Top level Domain (TLD)

-> Host name -> In Computer networking, a hostname is a lable that is assigned to a device connected to a computer network and that is used to identify the device in various form of electronic communication, such as the World Wide Web. Hostnames may be simple names consisting of a single word or phase, or they may be structured.

Hostname is the unique identifier that Servers as name of your Computer or Server Can be as long as 255 characters and consists of numbers and letters.

-> Domain name -> A Domain name is a unique, easy-to-remember address used to access a website, such as "google.com" and "facebook.com". User can connect to websites using domain names thanks to the DNS System.

-> Top-level Domain -> A Top-level Domain is one of the Domain ~~name System~~ at the highest level in the hierarchical Domain Name System of the internet after the root Domain. The top level Domain names are installed in the root zone of the name space. # DNS resolves FQDNs to IP address
www.totalsem.com is an example of an FQDN
.com and .edu are example of Top-level Domain (TLDs)

Applying DNS

=> SOA -> The DNS 'Start of authority' (SOA) record stores important information about a domain or zone such as the mail address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETE Standards.

=> Name Server -> A DNS name server is a server that stores the DNS records, such as address (A, AAAA) record, name server (NS) records, and mail exchanger (MX) records for a Domain name (see also list of DNS record types) and responds with answer to queries against its database.

A is for IPv4 & AAAA is for IPv6

=> A Canonical Name or CNAME record is a type of DNS record that maps an alias name to a true or canonical domain name. CNAME records are typically used to map a subdomain such as www or mail to the domain hosting that subdomain's content.

Quick Revision

CNAME record Creation makes an alias name, or "know name", often Created for user interfacing.
A reverse lookup zone will resolves an IP address to an FQDN, and are used by mail servers.
TXT record, DKMI, SPF are used to identify e-mail users and reduce SPAM.

The Host file

=> A Host file is a file that almost all computer and operating systems can use to map a connection between an IP address and domain names. This file is an ASCII text file. It contains IP addresses separated by space and then a domain name. Each address gets its own line.

* Select file > open. In the file name field, enter C:\Windows\System32\Drivers\etc\hosts. Select open. Make the necessary changes to the file.

The hosts file contains IP addresses and other corresponding names
Every computer that runs TCP/IP has a hosts file
The hosts file takes precedence over DNS.

NET Command

=> In Computing, net is a command in IBM OS/2, Microsft windows and ReactOS. used to manage and configure the operating system from the command-line. It is also part of the IBM PC network program for DOS.

The net command is a very old command that helps manage a network.
The net command has many difference options to manage a network (net use, net share, etc).
The net View command shows everything that is on the network.

Windows Name resolution

=> Name resolution is the function of resolving a name to one or more IP addresses. Name resolution in windows can resolve DNs fully qualified domain names (fqDNS) and single lable name. Single lable names can be resolved as both a DNS name and a NetBIOS name.

* NETBIOS => NETBIOS is an abbreviation of network Basic input/output System. The primary purpose of NetBios is to allow application on separate computers to communicate and establish sessions to access shared resources, such as files and printers, and to find each other over a local area network (LAN).

* Link-Local Multicast name resolution => The link-local Multicast name resolution (LLMNR) is a protocol based on the Domain name System (DNS) packets format that allows both IPv4 and IPv6 host to perform name resolution for hosts on the same local link. It is included in windows Vista, windows Server 2008, window7, window8 and windows 10.

* Nbstat => Nbstat is a utility that displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP), which helps troubleshoot NetBIOS name resolution issues. Normally, name resolution is performed

When NetBIOS over TCP/IP is functioning correctly.

Quick Revise

NetBios is an old protocol that manages the connections based on the names of the computers within a LAN

Link Local Multicast Name Resolution (LLMNR) is a protocol that allows hosts to name resolution for hosts on the same local link.

nb stat is a diagnostic command that can be useful but has some issues with LLMNR.

Dynamic DNS

> Dynamic DNS is a method of automatically updating a name server in the Domain Name System, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information. The term is used to describe two different concepts.
DDNS is a service that automatically and periodically updates your DNS 'A' (IPv4) or 'AAAA' (IPv6) records when your IP address changes.

Dynamic DNS enables you to use a DHCP-assigned IP address for connection.

DDNS providers can update IP information

phoenixnap.com

DNS Troubleshooting

→ 1) Check TCP/IP settings.
2) Flush the DNS cache.
3) Release the Renew DHCP Server IP.
4) Change to public DNS Server.
5) Use Dig
6) use nslookup (command).
7) use host
8) Use Traceroute or tracert

Use an IP address of a web site to test connectivity without DNS.
Run ipconfig /flushdns to clear the DNS resolver cache.
Run nslookup or Dig to check the status of a DNS server.

SECURING TCP or IP

Making TCP/IP Secure

=> CIA => These three letters stand for Confidentiality, integrity and availability otherwise know as the CIA triad. Together, these three principles form the corners-tone of any organization's security infrastructure in fact, they (should) function as goal and objectives for every security program.

Data protected by CIA triad

* Confidentiality => Confidentiality refers to an organisation's efforts to keep their data private or secret. In practice, it's about controlling access to data to prevent unauthorized disclosure. Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unathorized are actively prevented from obtaining access.

* Integrity => In everyday usage, integrity refers to the quality of sometimes being whole or complete. In Info sec, integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.

* Availability => Systems, applications and data are of little value to an organization and its customers if they are not accessible when authorized user need them. Quite simple, availability means that networks, systems, and applications are up and running. It ensure that authorized users have timely reliable access to resources when they are needed.

* Authentication => Authentication is the act of validating that users are whom they claim to be. This is the first step in any security process.
Process :-
1) Passwords 2) one time pins 3) Authentication
4) Biometrics.

* Authorization => Authorization in System Security is the process of giving the user permission to access a specific resources or function. This term is often used interchangeably with access control or client privilege.

Quick revision
Security can be broken into three areas: confidentiality, integrity, and availability
Confidentiality can be addressed through encryp
Confidentiality and integrity must be balance with availability.

Symmetric encryption

⇒ Symmetric-Key algorithms are algorithms for cryptography that use the same cryptographic key for both the encryption of plaintext and the decryption of ciphertext. The key may be identical, or there may be a simple transformed to go between the two keys.

Blowfish, AES, DES, RC5 and RC6 are example of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256. The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Cleartext is any unencrypted data.
Algorithms use keys to encrypt cleartext into ciphertext.
An algorithm that uses the same key to encrypt and decrypt is symmetric encryption.

Asymmetric encryption

⇒ Public-key cryptographic, or Asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key and a private key. The generation of such key pairs depends on cryptography algorithms which are based on mathematical problem termed one way functions. A typical value is 256 bits. The public key is a group element, which is much larger than the private key. A typical value 2048 bits.

Examples of asymmetric encryption include :-

- Rivest Shamir Adleman (RSA)
- The Digital Signature Standards (DSS), which incorporates the Digital Signature Algorithm (DSA)
- Elliptical Curve Cryptography (ECC)
- The Diffie-Hellman exchange method.
- TLS / SSL protocol.

Asymmetric encryption uses a public and a private key
public key encrypt, private keys decrypt.
for two people to communicate, they must exchange public keys.

(CHF) Cryptographic Hash function

=> A Cryptographic hash function (CHF) is an equation used to verify the validity of data. It has many applications, notably in information security (User authentication).

A Cryptographic hash function translates data of various lengths - the message - into a fixed size numerical string - the hash. A CHF is a single direction work, making it extraordinarily difficult to reverse in order to recreate the information used to make it.

Hashes are used for verifying data, not for encryption # Hash values are always fixed in size
Two common hashes are MD5 and SHA-1

Identification

⇒ Identification ⇒ identification is the claim of a subject of its identity. This could be achived by a user id, process ID, a smart card etc. It is critical that the asserted credentials be unique to be able to differentiate among different subject in a system.

⇒ Authentication ⇒ After a subject identifies, it needs to be authenticated, that is the subject needs to prove who it claims to be. This proof of identity is achieved through providing credentials to the access control mechanism. The credentials being used for authentication can be categorized in four different groups, that are also called authentication methods/types. In short they are:

- Something You know - (also know as Type 1 authentication factor) such as a password, personal identification number (PIN) or passphrase.
- Something You have - (also know as Type 2 authentication factor) such as a ~~password~~ Smart card, ~~personal~~ memory card ~~identification~~ or a token.
- Something you are (biometrics) - (also know as Type 3 authentication factor), such as a finger print, palm topology, hand geometry, iris/retina scan or phase recognition.
- Something You do (behavioral biometrics) - (also know as Type 3 authentication factor), such as a typing pattern (keystroke dynamics), signature pattern (signature dynamics) or voice pattern.

- If an authentication system requires at least two credentials that are in different authentication catagories, this is called multi-factor authentication.

=> Authorization => Once a subject is authenticated the authentication mechanism knows who the subject is that wants to access to the object. Authorization then determines the access level (s) of the subject to the object. In other words, authorization determine what the privleges of the subject are and how can a subject interact with an object.

Authentication requires sharing of something you know something you have, or something you do.
A smartcard is an example of something you have, Security question are an example of something you ~~saw~~ know
Federated system trust is inherited from a different trusted system.

Access Control

=> Access Control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimize risk to the business or organization. There are Two type of access control physical and logical.

Three main types of access Control System are:-
- Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Mandatory Access Control (MAC).

Mandatory access Control (MAC) uses labels
Discretionary access Control (DAC) gives the Creators Control over permissions.
Role - based access Control (RBAC) uses groups.

AAA

=> AAA refers to Authentication, Authorization and Accounting. It is a framework used to Control and track access within a Computer network. Common network protocol providing this functionality include TACACS+, RADIUS, and Diameter

AAA implementation :- AAA Can be implemented by using the local database of the device or by using an external ACS Server.

A RADIUS client is an intermediary agent between a RADIUS supplicant and a RADIUS Server
A RADIUS Database of authenticated users and password may reside outside the RADIUS Server
RADIUS uses UDP ports 1812 - 1813 or UDP ports 1645 - 1646, and TACACS+ user TCP port 49

Kerberos EAP

=> We propose a new authentication mechanism in extensible authentication mechanism in extensible authentication protocol (EAP), called EAP - Kerberos II, by adopting a ticket in Kerberos. The proposed mechanism uses mutual authentication to resolve all these security issues.
The goal is that support for TLS in Kerberos V5 client should be as easy to implement and deploy as support for UDP/TCP.

Kerberos handles authentication and authorization for wired networks
Kerberos relies heavily on Time stamps
EAP enables flexible authentication.

Single sign-on (SSO)

=> Single sign - on (SSO) is an authentication method that enables user to securely authenticate with multiple application and website by using just one set of credentials.
With SSO, a user only has to entre their login credential (username, password etc.) one time on a single page to access all of their SaaS applications.

* SAML => Security ASsertion Markup Language is work by exchanging user information, such as login, authentication state,

identifiers, and other relevant attributes between the identify and service provider. As a result it, simplifies and secure the authentication process as the user only needs to log in once with a single set of authentication.

for blal area networks, use windows Active Directory for single Sign-on
SAML is used to manage multiple apps using a single account.
SSO linde provides a variety of service provider (SP) samples.

Certificate and Trust

=> A Certificate of trust is a Document that summarizes the detail of a Trust. The trust Certificate is typically given to third parties, like a financial institution, during a transaction as proof of the trust's existence and its authority over trust property.

* Web of Trust => WOT Services is the developer of MyWOT, an online reputation and internet Safety services which shows indicators of trust about existing websites.
* Public Key Infrastructure => A public key infrastructure (PKI) is a set of roles, policies hardware, Software and procedures needed to create, manage, distribute, use, Store and revoke digital

Certificates and manage public-key encryption.

Quick Review
Certificates include a public key and at least one digital Signature.
Web of Trust uses a Web of mutally trusting peers.
Public Key infrastructure uses a hierarchical structure with root servers.

Certificat Error Scenarios

→ Certificate errors occur when there's a problem with a certificate or a web server's use of the certificate. Internet Explorer help keep your information more secure by warning about certificate errors.

Quick Review
A self-signed Certificate can throw a 443 error, as the Certificate has not been issue by a Certificate authority.

An expired Certificate can be viewed, then fixed either by getting a new Certificate from its issuer or accepting the Certificate in its Current State.

The setting to query OCSP to Confirm the Current Vadility of Certificates is a good Security Setting.

There will be most important video of the module - (Device Placement scenarios) (13).

Page No.: 65
Date: / /

Advanced Networking Devices

Understanding IP Tunneling.

-> Tunneling involves the encapsulation of an IP packet within another packet. This encapsulation enables the packet to reach its destination through intermediary network that do not support the packet's protocol. Tunnels differ depending on the type of packet encapsulation that is used.
In the physical word, tunneling is a way to cross terrain or boundaries that could not normally be crossed.
Tunneling is often used in Virtual private network (VPN).

Very few internet protocol are encrypted

Tunnels can encapsulate unencrypted protocols to create encrypted communication channels

Tunnels are often used with remote access connections.

Virtual private Networks

=> A Virtual private Network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public network as if their computing device were directly connected to the private network.

Type of Virtual private Network (VPN) protocols

1. Internet protocol Security (IPSec): Internet protocol Security, known as IPSec, is used to secure internet communication across and IP network.

2. Layer 2 Tunneling protocol (L2TP): L2TP or Layer 2 Tunneling protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection.

3. Point-to-Point Tunneling protocol (PPTP): PPTP protocol generates a tunnel and confines the data packet. Point-to-point protocol (PPP) is used to encrypt the data between the connection.

4. SSL and TLS: SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the Web browser acts as the client and user access is prohibited to specific applications instead of entire network.

5. Open VPN: Open VPN is a open source VPN that is commonly used for creating point to point and site-to-site connection.

6. Secure Shell (SSH): Secure Shell or SSH generate the VPN tunnel through which the data trasfer occurs and also ensures that the tunnel is encrypted.

A VPN Creates a Secure Tunnel So a remote machine or network Can be part of a local network.

A Client - to - Site VPN Connects a remote Computer to a local network.

A Site - to - Site VPN Connects distant network into a Single network.

(practicalnetworking.net) Best site

Introduction to VLANs

=> A LAN is a grouping of two or more devices on a network. A VLAN is a Virtual LAN, a Subgroup within a local network. VLANs make it easy for network administrators to Separate a Single Switched network into multiple groups to match the functional and security requirements of their System.
For example => The two Switch port in the orange mini - switch might be assigned to VLAN #10. The Two ports in the red mini - switch might be assigned to VLAN #20. And Lastly the two Switch ports in the blue mini - Switch might be assigned to VLAN #30.

A VLAN Splits One broadCast domain into two or more broadCast domains.
A manage switch that Support VLANs requires Configuration.
Trunking enables VLAN to be on more than one Switch.

Inter VLANs routing

⇒ Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:-

-> Legacy inter-VLAN routing: This is a legacy solution. It does not scale well.

-> Router-on-a-stick: This is an acceptable solution ~~does not scale well~~ for a small- to medium-sized network.

-> Layer 3 switch using switch virtual interface (SVIs): This is the most scalable solution for medium to large organizations.

VLAN create separate broadcast domains.

Connect the broadcast domain with physical routers.

Broadcast domain can be connected with virtual routers using inter VLAN routing.

Interfacing with managed switch.

-> Enterprise Managed (or fully managed) switches These have a full set of management features, including command line interface, SNMP agent, and web interface. They may have additional features to manipulate configuration, such as the ability to display, modify, backup and restore configuration.

Managed switch requires configuration.

Connect to a managed switch via an IP address or a console port.

Cisco routers and switch use a Proprietary IOS

Switch port protection

=> Protected ports are one of the security mechanisms used on switch world. By default all the switch ports are unprotected and equal. But with protected port configuration, some ports are filtered an restricted to access each other.

If you configure a port as protected, data traffic on layer 2 is not transfered to other protected ports on this broadcast domain (or switch stack). Only control traffic is sent to these ports. To provide data traffic between these ports a layer 3 device is required. But if you use protected ports, you do not need this.

Simply we can say that protected ports do not send and receive traffic each other. But they can send and receive traffic without ports.

Switch port do not use IP addresses or work with Layer 3

Switch interconnection use STP to detect looping by deactivating the port, if necessary

BPDU guard is a Cisco method allowing only non-switch devices to connect to the switch.

Port Bonding

⇒ Network bonding is a process of combing or joining two or more network interface together into a single interface. Network bonding offers performance improvement and redundency by increasing the network through put and bandwidth. if one interface is down or unplugged the other one will work.

Port bonding links Switchport to increase bandwidth.
use LACP for the trunking protocol.
Set ports to active.

---

port Mirroring

⇒ Port mirroring is a method of copying and sending network packets transmitted as input from a port to another port of a monitoring Computer / Switch / device. It is a network monitoring technique implemented on network Switch and similar devices. port mirroring is also known as Switched port analyzer (SPAN) and roving analysis port (RAP).

Port mirroring enables the traffic flowing through one port to be monitoring on another port.
This feature enable administrators to remotely inspect traffic from a Suspicious machine.
Port mirroring is configured on a Switch by providing a source port and a destination port.

Quality of Services

=> Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flow in network traffic.

Quality of service controls help better manage available bandwidth.
One type of QoS control is traffic shaping
Simple QoS on SOHO routers allows priority setting for different protocols.

IDS vs IPS

=> IDS => An intrusion detection system (IDS) monitors traffic on your network, analyzes that traffic for signatures matching known attack and when something suspicious happens, you're alerted. In the meantime, the traffic keeps flowing.

=> IPS => An intrusion prevention system (IPS) also monitors traffic. But when something unusual happens, the traffic stops altogether until you investigate and decide to open the floodgates again.

Intrusion detection system detect and report possible attack to the administrators # Intrusion prevention system run in-line with network and act to stop detation attack.
A firewall filters, IDS notifies, IPS acts to stop.

Proxy Server

→ In Computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource.
Instead of connecting directly to a server that can fulfill a requested resources, such as a file or web page, the client directs the request to the proxy server, which evaluates the request and performs the required network trasaction.

There are two types of proxy server.

1. Forward proxy
2. reverse proxy

* A Forward proxy is the most common form of a proxy server and is generally used to pass request from an isolated, private network to the internet through a firewall. Using a forward proxy, requests from an isolated network, or intranet, can be rejected or allowed to pass through a firewall.
* A reverse proxy server is an intermediate connection point positioned at a network edge. It receives initial HTTP connection requests, acting like the actual endpoint. Essentially your network's traffic to the reverse proxy serves as a gateway between users and your application origin server.

Dv11

=> Transparent proxy - Transparent proxy also known as an inline proxy, intercepting proxy or forced proxy is a server that intercept the connection between an end-user or device and the internet. It is called "transparent" because it does so without modifying requests and responces.

Forward proxy servers hide the clients from the server by forwarding the message to the server.
Forward proxy server can be configured for caching content filtering, and firewall capability.
Reverse proxy servers hide the server, and can provide load balancing and caching for high activity pages.

Load Balancing

=> In computing, load balancing refers to the process of distributing a set of tasks over a set of resources, with the aim of making their overall processing more efficient. Load balancing can optimize the response time and avoid unevenly overloading some compute nodes while other compute nodes are left idle.

Load balancing can be configured as client-side or server-side and provides high availability.
Load balancing can route to the most available server, either by a configured list (round robin) or by least response time.
Server-side load balance uses a sophisticated hardware device that is located within the server.

IPv6

Introduction to IPv6

⇒ Internet protocol of the internet protocol (IP), the communication protocol that provides an identification and location system for computers on network and routes traffic across the internet.

An IPv6 address is a 128-bit alphanumeric value that identifies an endpoint device in an internet protocol version 6 (IPv6) network. IPv6 is the successor to a previous addressing infrastructure IPv4, which had limitation IPv6 was designed to overcome.

* IPv6 addressed :-

aOfO : 0001 : 0000 : 0001 : 0000 : 0001 : 0000 : 1234
4x4 16bit — 16bit — 16bit — 16bit — 16bit — 16bit — 16bit — 16bit

128bit (16 byte)

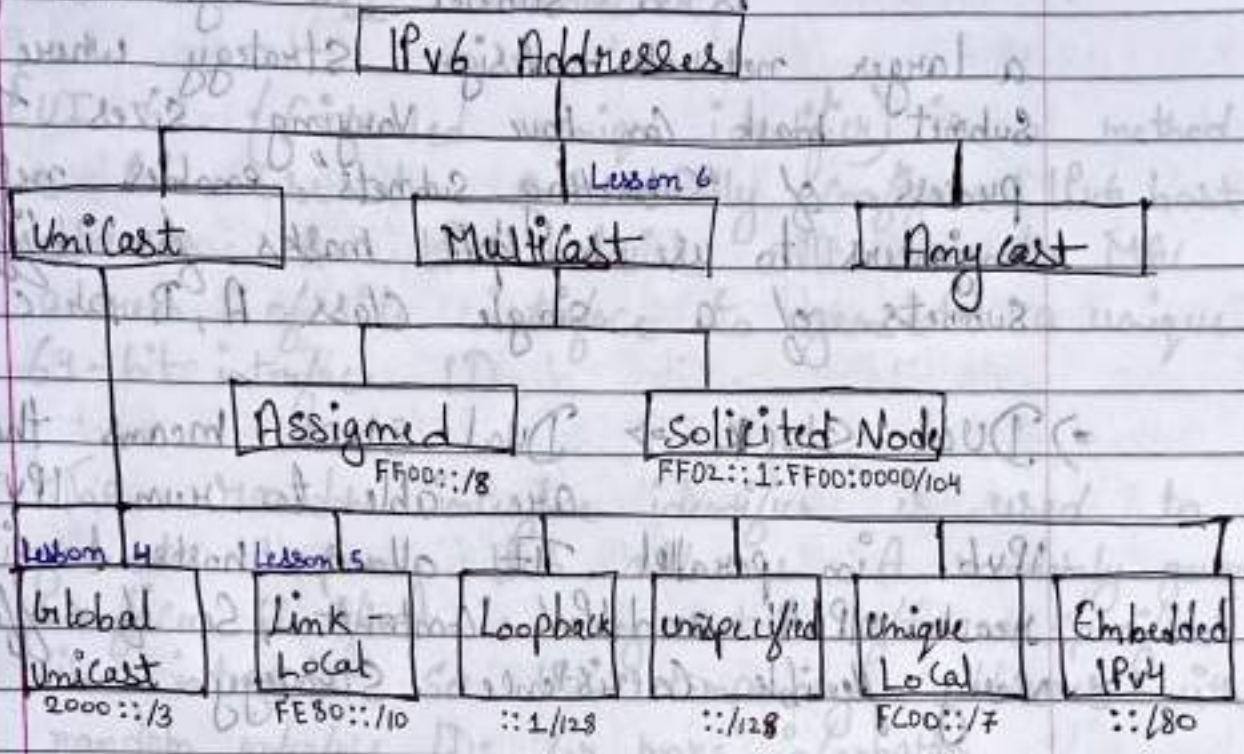
Quick Revision

IPv6 are 128 bits having a much larger address space than IPv4.

IPv6 address have 8 Segments Separated by 7 Colons.

IPv6 allows data to move much faster through the internet.

IPv6 Addressing



IPv6 Address Types

IPv6 address /64

1. Link-local

fe80:0000:0000:0000 = fe80::

2. MAC-address (48 bit address)

2a-3b-4f-09-45-01

EUI-64 = ff-fe (in the Middle of MAC add)

EUI-64 = 2a-3b-4f-ff-fe-09-45-01

IPv6 => fe80::2a3b:4fff:fe09:4501

=> VLSM => Variable Length Subnet Mask (VLSM) is a Subnet - a Segmented piece of a larger network - design strategy where all Subnet mask can have varying sizes. This process of "Subnetting Subnets" enables network engineers to use multiple masks for different subnets of a single class A, B or C network.

=> Dual Stack => Dual stack means that Devices are able to run IPv4 and IPv6 in parallel. It allows hosts to simultaneously reach IPv4 and IPv6 content, so it offers a very flexible coexistence strategy.

Quick Revision

IPv6 addresses can be shortended by removing leading zeros, but be familiar with the rules
IPv6 addresses have two IP addresses: a link-local address and an internet address.
The second part of the IPv6 address using EUI-64 is generated from the MAC address

=> IPv6 addressing is classified by the primary addressing & routing methodologies common in networking as follows.

- An unicast address identifies a single network interface.
- An any Cast address is assigned to a group of interfaces
- An multicast address is also used by multiple hosts.

- IPv6 addressing does not implement broadcast addressing, the use of the all-nodes group is not recommended, and most IPv6 addressing protocols use a dedicated link-local multicast group to avoid disturbing every interface in the network.

IPv6 initial action

→ EUI-64 Vs randomizer

* EUI-64 (Extended unique identifier) is a method we can use to automatically configure IPv6 host addresses. An IPv6 device will use the MAC address of its interface to generate a unique 64-bit interface ID.

* The random interface identifier is used to generate temporary IPv6 addresses. A randomly generated interface identifier is regenerated after a specified time interval. See IPv6 temporary addresses with random interface IDs for more information.

→ Stateful DHCPv6: There are three methods to configure a host with a global unicast address, default gateway DNS server, and a domain name:-

- Method 1: Configure the host manually This approach does not scale and is prone to human error;
- Method 2: Using SLAAC and a stateless DHCPv6 server. We have looked at this approach in our previous lesson;
- Method 3: Using a Stateful DHCPv6 Server.

EUI-64 uses the MAC address to generate a unique 64-bit ID to automatically configure a host address.
IPv6 uses router solicitation/advertisement to access interface route information # Application Sometimes request temporary IP addresses, this is easily supported by IPv6 stateless auto configuration.

IPv4 and IPv6 Tunneling

→ Tunneling provides a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic.

The key to a successful IPv6 transition is compatibility with the existing installed base of IPv4 hosts and routers. Maintaining compatibility with IPv4 while deploying IPv6 streamlines the task of transitioning the internet to IPv6. While the IPv6 infrastructure is being deployed the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.

IPv6 or IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways:

* Router-to-Router
* Host-to-Host
* Host-to-Router
* Router-to-Host.

Quick Review

If you are on IPv4 you need a tunneling protocol to get to the IPv6 internet.

Microsoft provides some tunnels, like Teredo and 6to4

Try the Gogo Client from www.gogo6.com

WIRELESS Connection NETWORKING

Introduction to 802.11

➢ IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards and specifies the set of media access control (MAC) and physical layer (PHY) protocol for implementing wireless local area network (WLAN) Computer communication. The Standard and amendment provide the basis for wireless network product using the wi-fi brand and are the world's most widely used wireless computer networking standards

Quick Revision

A WAP is a bridging device that connets into an Ethernet network and communicates via radio waves to wireless clients
A WAP has an SSID (service set identifier), a world or phase used to connect wireless device to the WAP device.
CSMA/CA (carrier sense multiple access with collision avoidance) is the method used to prevent wireless collisions.

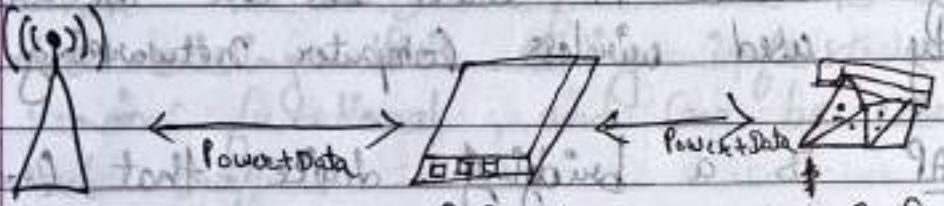
802.11 Standards

➢	IEEE Standards	Rf used	Spread Spectrum	Data Rate in (Mbps)
1.	802.11	2.4GHz	DSSS	1 or 2 Mbps
2.	802.11	2.4GHz	FHSS	1 or 2 Mbps
3.	802.11a	5GHz	OFDM	54 Mbps
4.	802.11b	2.4GHz	DSSS	11 Mbps
5.	802.11g	2.4GHz	DSSS	54 Mbps
6.	802.11n	2.4/5GHz	OFDM	600 (theoratical)

Q.R
Early wireless standards were 802.11b (2.4-GHz) and 802.11a (5-GHz).
First widely-used standards was 802.11g (2.4-GHz)
Current fastest standards are 802.11n and 802.11ac.

Power over Ethernet

→ Power over Ethernet (PoE) is technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP Cameras, and VoIP phones in addition to the data that cable usually carries. It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each.



PoE-Enable wireless access point — PoE Switch — PoE-Enable VoIP Phone

Quick Review

A PoE WAP needs to use a PoE switch or a PoE injector but does not need a directly connected IIO plug.

PoE uses 802.3af originally, but has been replaced with PoE+ using the 802.3at Standard that supports the newer WAPs supporting up to 30 watts.

Antennas

→ In radio engineering, an antenna or aerial is the interface between radio waves propagating through space and electric current moving in metal conductors, used with a transmitter or receiver.

Type of Antennas

* Omni directional antennas
* Dipol
* Patch
* Directional / Yagi
* Parabolic / Directional

⇒ SMA (subMiniature Version A) Connector.

Quick Review
Difference types of antennas have different radiation patterns and can be placed to provide a radiation pattern to meet wireless requirements.
Patch antennas are regularly used on exterior walls
Antenna placement and the gain should be consider when selecting antenna types, location, and security boundaries.

Wireless Security Standards

⇒ There are three types of wifi encryption protocols are: Wired Equivalent privacy (WEP), Wi-Fi protected Access (WPA), and Wi-Fi protected Access Version 2 (WPA2).
These encryptions have one things in common - protecting the data on your network - but the main difference lies in how to well they do so.

Quick Review
The 802.11 Standards are used on both SoHo routers & enterprise routers. # 802.11i was slow to release, so WPA created using TKIP encryption protocol.
WPA uses CCMP-AES as the encryption Protocol and is more secure.

Implementing wireless Security

Q) What can you do to minimize the risk to your wireless network?

- Change default passwords
- Restrict access
- Encrypt data on your network.
- Protect your Service set identifier (SSID)
- Install a firewall.
- Maintain antivirus software
- Use file sharing with caution.
- Keep your access point software patched and up to date.
- Check your internet provider's or router manufacturer wireless security options.
- Connect using a Virtual private Network (VPN).

Quick Review

Disable SSID broadcast
Use MAC filtering
Limit the number of DHCP-issued addresses.

Threath to your wireless network

Q) The 7 most common wireless network threath are

1. Configuration problems: Mis configuration, incomplete configurations.
2. Denial of Services: Sending large amounts of traffic (or viruses) over the network with the intent of hijacking resources or introducing backdoors.

3. Passive Capturing : Eavesdropping within range of an access point to capture sensitive information.
4. Rogue (or unathorized/Ad-Hoc) Access points : fool device into connecting with a false access point.
5. Evil Twin Attack : Impersonating legit access point with a stroger signal to entice authorized user to sign on.
6. Hacking of Lost or stolen wireless Devices : By passing the password to gain access.
7. Freeloading : Piggybacking on a connection or intercepting file sharing.

quick revision

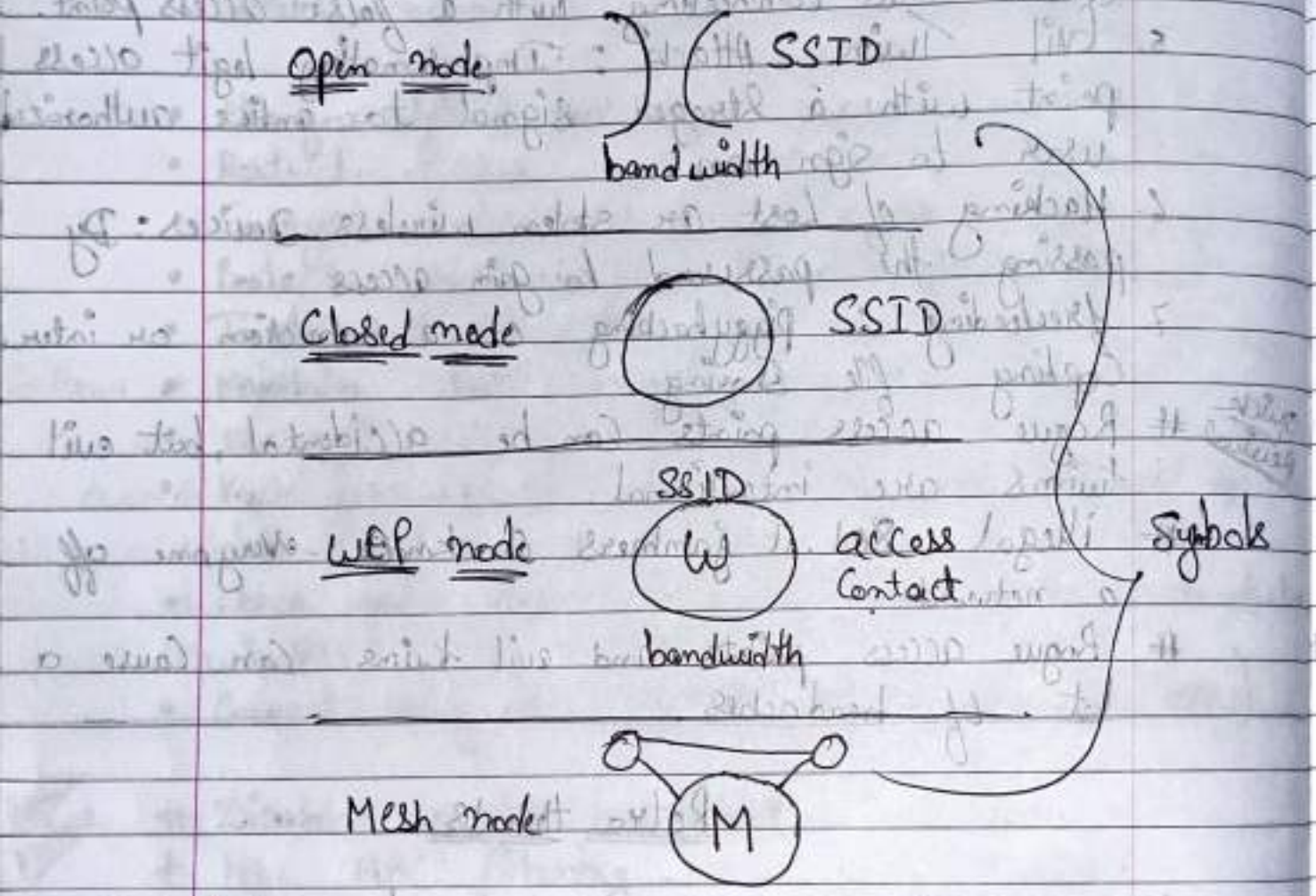
Rogue access points can be accidental, but evil twins are intentional.
illegal 802.11 jammers can knock everyone off a network.
Rogue access points and evil twins can cause a lot of headaches.

Retro threats

=> WAR Driving => War Driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a City or elsewhere.

=> War Chalking => War chalking is the drawing of symbols in public places to advertise an open wi-fi network. Inspired by hobo symbols, the warchalking marks were combined by a group of

friends in june 2002 and publicised by Matt jones who designed the set of icons and produced a downloadable document containing them.



war driving is the act of driving around and mapping the location and state of wireless access points.

war chalking is drawing a symbol on the side walk indicating the current state of a present WAP

Thus, war driving might seem like a things of the past However, security specialists still use it to research wi-fi security.

Wi-fi protection setup (WPS)

⇒ Wi-fi Protected Setup (WPS) is a standard for the easy and secure establishment of a wireless network. Traditionally, user would have a manually create a wireless network name (SSID), and then manually enter the security key on both the access point, and client to prevent unwanted access to their wireless network.
Wi-fi protected setup allows the owner of wi-fi privileges to block other users from using their household wi-fi. The owner can also allow people to use wi-fi.

WPS enables one-button setup of wireless devices
All modern wireless devices are WPS-enabled.
WPS can be security threat

Enterprise wireless

⇒ Enterprise wi-fi is an enterprise-grade wireless network that enables users to access wi-fi connection on a business property using mobile device, laptop and other technology. Enterprise wi-fi may include both a secure, private network for use by employees as well as an open, public network for guests and customers.

Enterprise wireless system have multiple WAPs that can all have the same wireless controller for configuration setup.
The wireless controller can monitor traffic set up various zones or access areas and define service access to specific WAP destinations.

The 802.11 standards are used on both SOHO routers and enterprise routers.

Installing a wireless network

=> Coverage, capacity, users, devices, application interference, power requirements, and security, are all consideration that need to be input into your design model. Sound difficult? It doesn't have to be. Not long ago, wireless network design involved a floor plan, and plotting location for access points with a protector.

If you install a wireless network you know where to install the patch or Yagi to connect the great signals.

Interface, reflections, and absorption are all environment issue that can affect the wireless signal.

A wi-fi signal is different on various devices; match radiation patterns and 802.11 specifications to the signal requirement.

Pay attention to the bandwidths and use channels with the least amount of congestion.

Wireless Scenarios

Interference can disrupt or slow wireless connection.

Source of interference can include other WAPs, wireless mice and keyboard, and even microwaves.

Remove sources of interference or change the WAPs frequency to avoid interference.

More wireless Scenarios

Adding or updating access points with more robust 802.11 standard devices should be considered for slow wireless network.
Be aware of gain loss due to length of cable and keep cables short when possibles.
Antenna placement is a bit of an art; test and retest to ensure expected coverage.

Virtualization and Cloud Computing

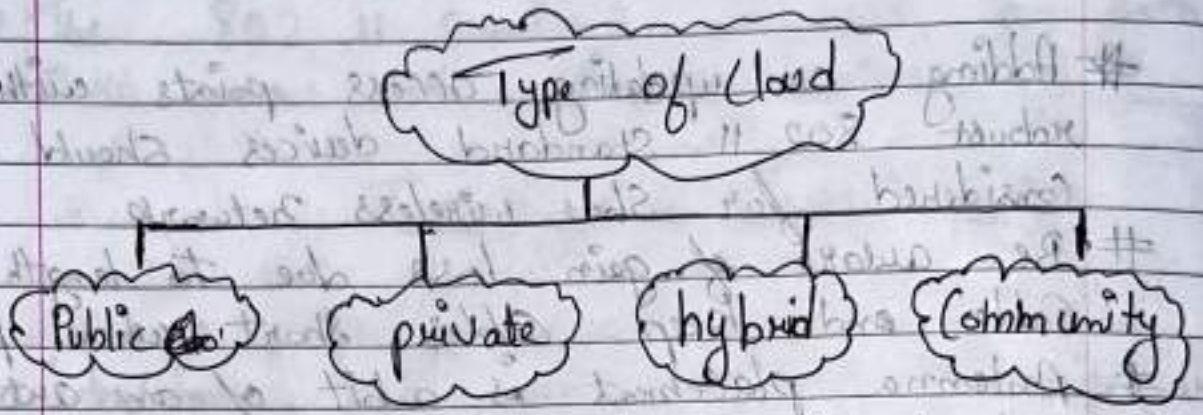
Virtualization Basics

⇒ In computing, virtualization or virtualisation (sometimes abbreviated V12n, a numeronym) is the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. Virtualization is a method of logically dividing the system resources provided by mainframe computers between different application.

⇒ Hypervisor => A hypervisor, also know as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing. There are two type of hypervisors referred to as "Type 1" (or "bare metal") and "Type 2" (or hosted)

There are two types of hypervisors: Type 1 (bare metal) and Type 2 (hosted) # Dont confuse virtualisation with emulation
Recognize the benefits of virtualization.

Cloud ownership

→ 

* Public Cloud is open to all to store and access information via the internet using the pay-per-usage method. Computing resources are managed and operated by the Cloud Service provider.

* Private cloud is also known as an internal cloud or corporate cloud. It is used by organizations to build and manage their own data centers internally or by the third party.

* Hybrid Cloud is partially secure because the service which are running on the public cloud can be accessed by anyone, while the service which are running on a private cloud can be accessed only by organization users.
Hybrid cloud = public cloud + private cloud.

* Community cloud allows system and services to be accessible by a group of several organizations to share the information between the organization and a specific community.

Private clouds allow access to members only
public cloud are available to anyone.
A private cloud with contracted managent is considered a hybrid cloud.

Cloud implementation

⇒ VPC - Amazon Virtual private Cloud / Amazon VPC enable you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

VPC (Virtual private cloud) depends on the services requested, including IaaS (infrastructure as a service) and PaaS (platform as a Service)

VPC services are very flexible, expandable, and can provide many types of services.

Building web servers on cloud applications is very easy but there can be costs associated with the service.

Your first Virtual machine

⇒ In this lecture mike teach How to create a Virtual machin in your host operation System

Virtual machine need an operating System.

Snapshots store the current state of a Virtual System

Most Virtual hardware can be changed.

NAS and SAN

⇒ Storage Area network (SAN) is used for trasferring the data between the servers and the storage devices fiber channel and switches. In SAN (storage Area Network), Data is identified by disk block. protocols that are used in SAN are: SCSI, SATA etc

=> In Network Attached Storage (NAS), data is identified by file name as well as byte offset. In Network Attached storage, file system is managed by Head unit such as CPU and memory. In this for backup and recovery, files are used instead of block by block copying technique.

NAS is file level.
SAN is block level.
SANs will either use fiber channel or ISCSI

Platform as a Service (PaaS)

=> Platform As a Service (PaaS) is a Cloud delivery model for application composed of services managed by the third party. It provides elastic scaling of your application in which it allows developers to build application and services over the internet and deployment include public, private and hybrid.

PaaS enables access to a Software development platform without the need to personally host it.
Heroku is a great example of PaaS.
A PaaS allows very quick access to Software running live on the internet.
~~PaaS enables quick configuration of resource~~
SaaS enables access to application via subscription.
Microsoft office 365 is a great example of SaaS.
Other SaaS example include Dropbox and google Docs.

Infrastructure as a Service

=> Infrastructure As a service (IAAS) is means of delivering Computer infrastructing as ondemand services. It is one of three fundamental cloud service model servers storage network operating system. In the user purchasing server software data center space or network equipment and rent those resources as a fully outsourced service (on demand model. It allows dynamic scaling and resources are distributed as a services. Generally includes multiple-user on a single piece of hardware.

IaaS enables quick configuration of IT network resources hosted by someone else.
Amazon web services (AWS) is a great example of IaaS
AWS, like most IaaS providers, only charges for the time a server is actually running.

Software as a service

=> Software As a service (SaaS) allows user to run existing online application and it is a model software that deployed as a hosting delivery model. during which software and its associated data are hosted centrally and accessed using their client usually an online browser over the web. SaaS services are used for the development and deployment of modern application.