CCT/CCNA All-in-One Exam Guide

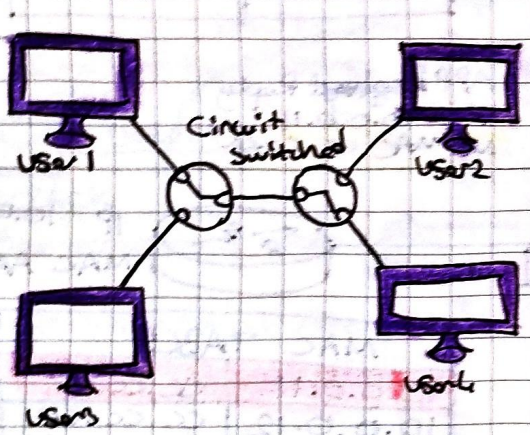
Local Area Network (LAN)

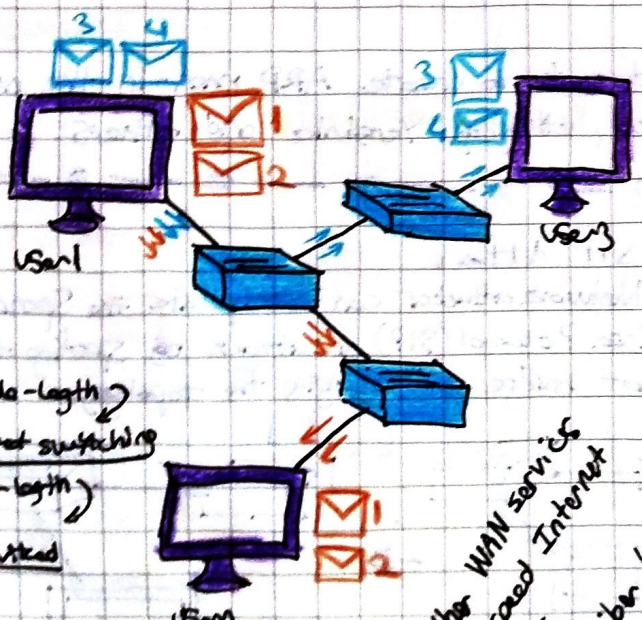
are used to connect networking devices that reside in a close geographic area such as a floor of a building, building itself or within a campus.

Includes different types of devices; PC's, Servers, switches, routers multilayer switching, voice gateway firewalls and another.

Media types: copper and fiber cabling

Ethernet, Fast Ethernet (FE)
Gigabit Ethernet (GE), Token Ring
Fiber Distributed Data Interface (FDDI)





- variable-length packet switching
- fixed-length cell switched

Wide Area Network (WAN)

are used to connect multiple LAN's together. Whereas a corporation provides its own infrastructure of a LAN, WAN's are leased (circuits) from carrier networks such as telephone companies and Internet Service Providers (ISPs).

Connections;

- circuit switched
- cell switched
- packet switched
- dedicated connection

- Analog Dialup
- (ISDN)
- Integrated Services Digital Network
- Asynchronous Transfer Mode (ATM)
- Frame Relay
- X.25

Circuit Switched

- provide temporary connection across a phone circuit.
- are typically used for backup of primary circuit and for temporarily boosts of bandwidth
- CELLULAR WIRELESS SERVICES (3G and 4G)

Dedicated Circuit

- is a permanent connection between two sites in which the bandwidth is dedicated to company use
- voice, video and data

Cell Switched

- provide the same features that dedicated circuit offers.
- advantages over dedicated connection, it enable a single device can connect to multiple devices on the same interface

Packet Switched

are similar to Cell switched services, except cell switched switch fixed-lenght packets called cells and packet switched services switch variable-lenght packets.

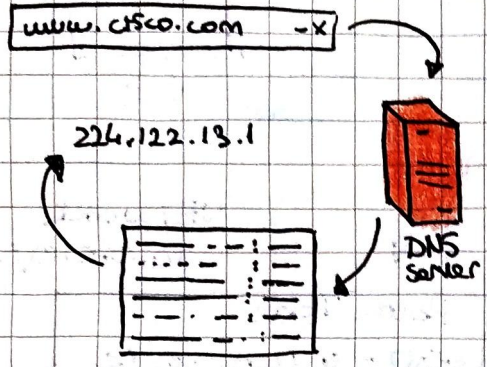
- Two other WAN services for high speed Internet connections.
- Digital Subscriber Line (DSL)
- Cable
- DSL provider (Mbps) connection and cost Less. Limited range
- Cable is (coaxial copper and fiber connections, higher datarate but cable must be shared with other customers. and security risk

GIPTA

Common Network Services

DNS Server

is responsible for resolving fully qualified domain name (FQDNs) to IP addresses.



FTP Server (File)

is used to hold all of the data files for a company. has lots of file storage space.

SMTP / POP

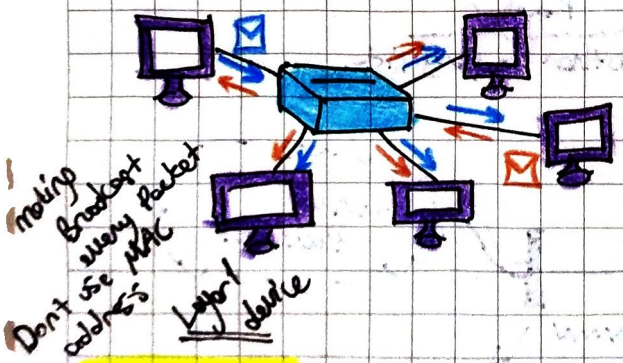
runs spasific protocols that enable the e-mail software to send and read. SMTP is for sending e-mail, pop is for reading e-mails.

Common Network Devices

Hub

All system connected to the hub to provide network communication.

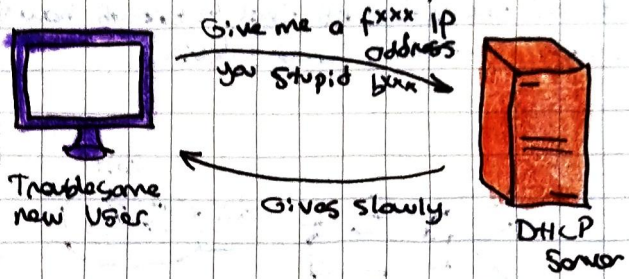
- No filtering, when a system send data to another system, hub send broadcast



- Collusions, hub is not full duplex its half duplex. Users sent data or receive data at the same time.
- Security

DHCP Server

is responsible for assigning IP addresses to computer and devices when they connect to the network.



HTTP Server

is responsible for hosting web pages that can be delivered to clients that connect to the web server.

Application Server

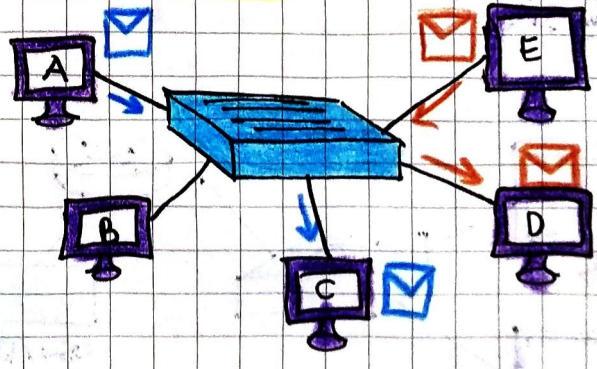
has specified application installed to provide services on the network. An database or e-mail applications installed on application server.

FTP

enable someone to connect the network and transmit, transfer files across the network or Internet. Uses TCP. TFTP → UDP

LAN Switch

Layer 2 switch tracks every devices MAC address (keeps MAC address table) and then associates that devices MAC address with the port number on switch.



MAC TABLE		
port1	---	MAC A
port2	---	MAC B
port3	---	MAC C
port4	---	MAC D

Full duplex

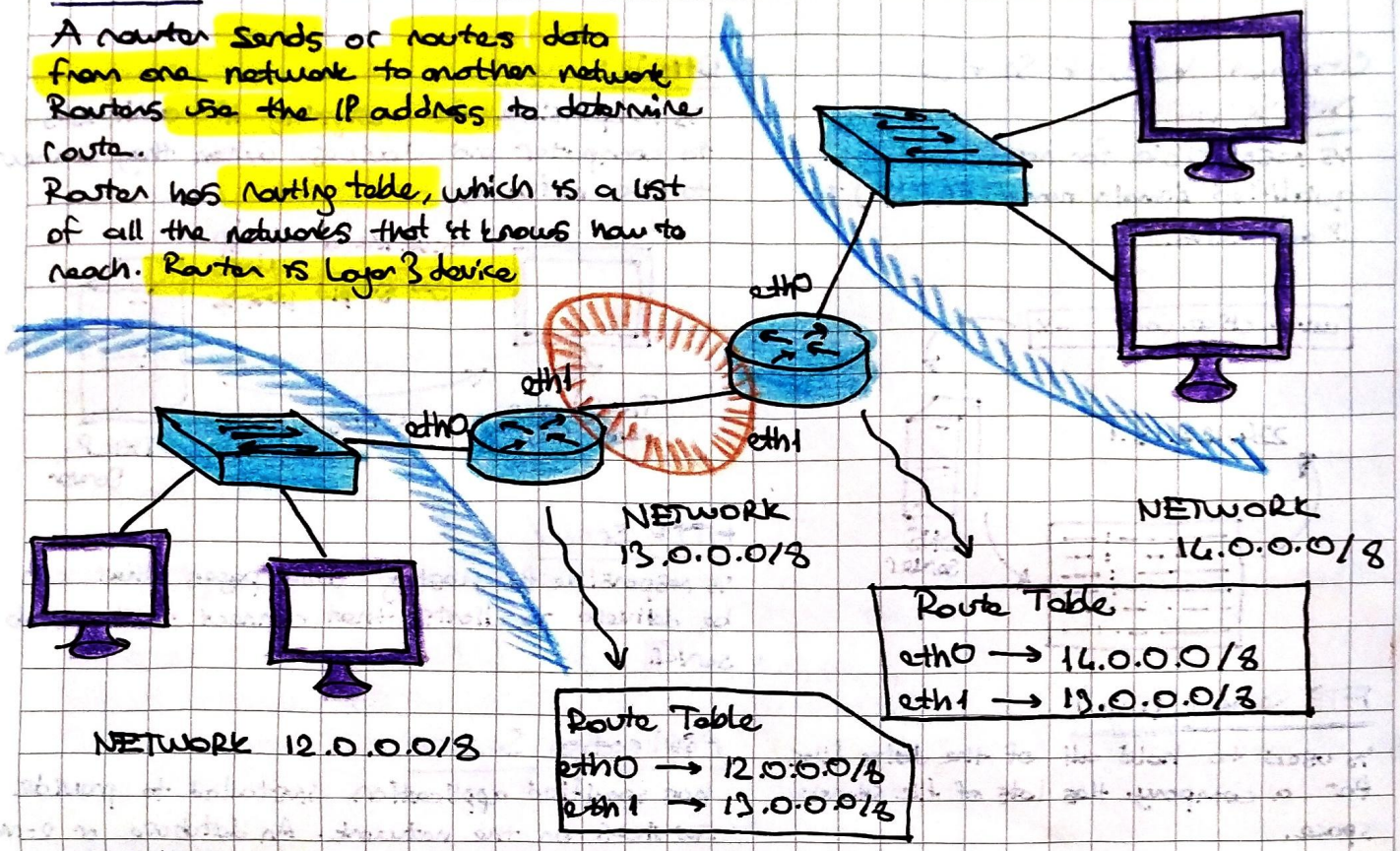
keeps MAC address table on their memory to send data to only associated connectors

GIPTA

Router

A router sends or routes data from one network to another network. Routers use the IP address to determine route.

Router has routing table, which is a list of all the networks that it knows how to reach. Router is Layer 3 device

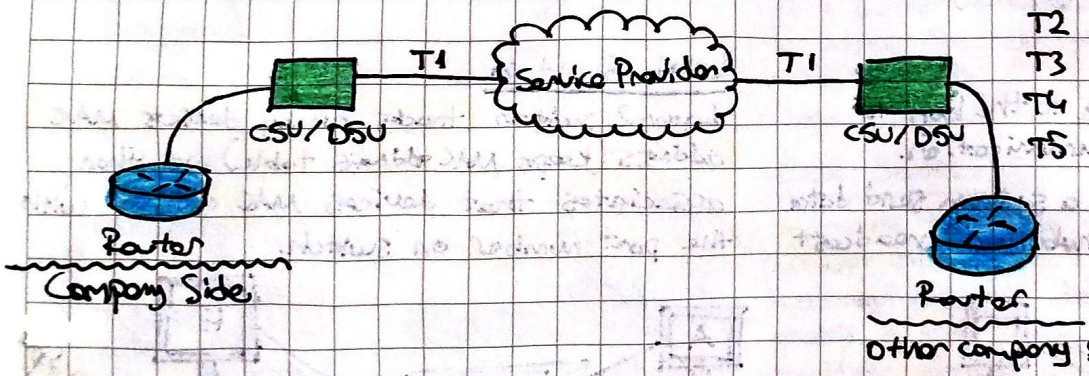


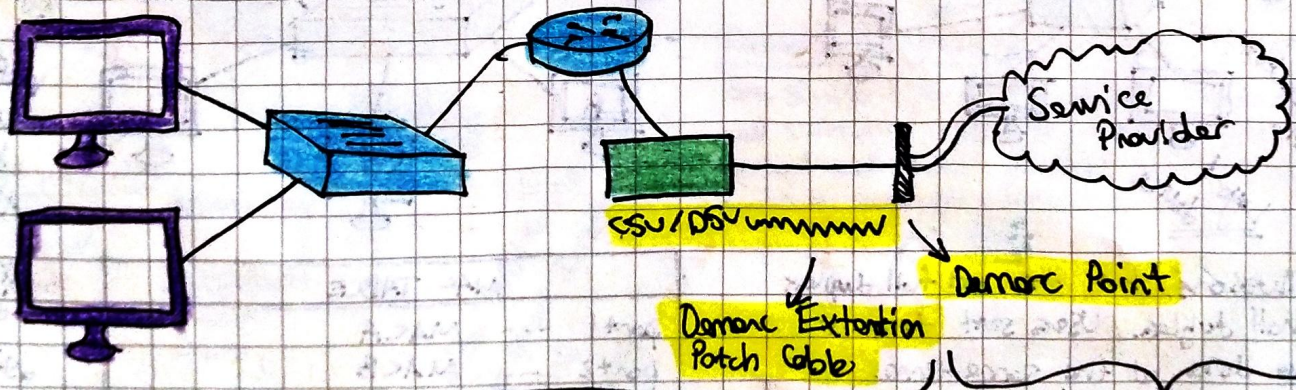
CSU/DSU Channel Service Unit / Data Service Unit

is a device that enables an organization to connect a high speed data link from ISP to the organizations router for access to and from LAN & WAN. This high speed connections are usually T1 or T3 connections.

- Many routers come with internal CSU/DSU module installed.

Name	Capacity
T1	1.544 Mbps
T2	6.312 Mbps
T3	44.736 Mbps
T4	274.176 Mbps
T5	400.352 Mbps





GIPTA

Firewalls

control which traffic is allowed to enter a network which traffic should be blocked. When configuring firewalls, creating rules for allowing and denying traffic based on the protocols, port numbers, direction of packets.

Packet Filtering Firewall (Stateless)
can filter traffic based on the source and destination ip addresses, the source and destination port numbers and the protocol used. Simple packet filtering firewalls does not understand the context of the traffic. Easy to pass with bad traffic

Stateful packet inspection firewall
Like packet filtering firewall. It also understands the context of traffic and will not allow a packet through the firewall unless a suits a specific scenario.

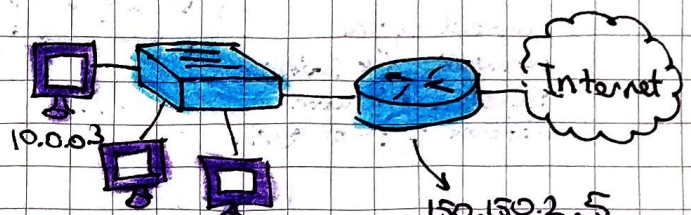
Next Generation Firewall (NGFW)
Layer 7 device that can inspect the application data and detect malicious packets

Intrusion Prevention System (IPS)

is a security device that monitors activity, log and suspicious activity and takes some form of corrective action

Network Address Translation (NAT)

NAT enables us to hide our internal network structure from the outside world by having NAT device receive all outbound packets, take the internal source address out, and replace it with the public IP address of the NAT device



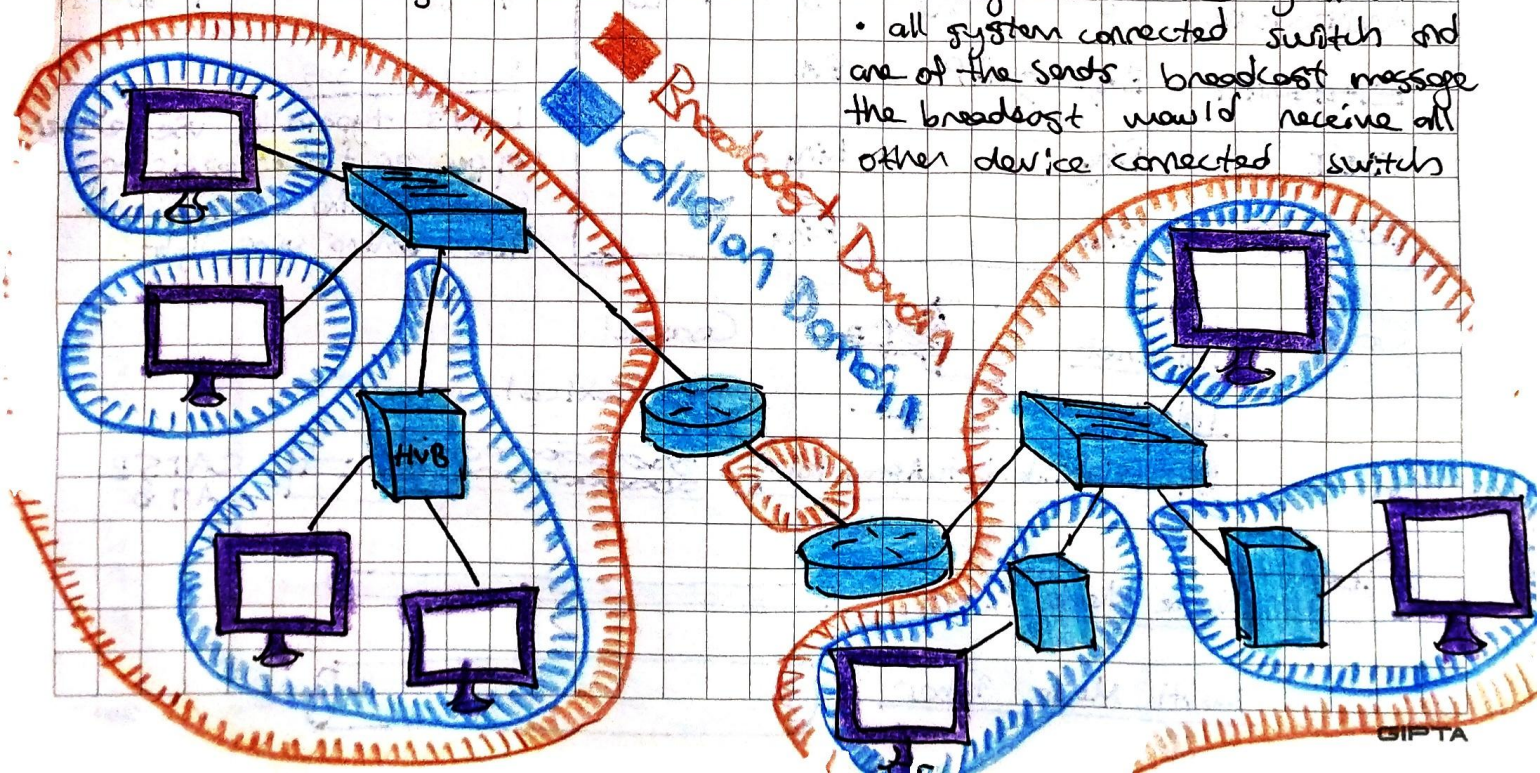
Private IP addresses

Public IP - Only One IP we have

Collision Domain - Broadcast Domain

Collision Domain
Data transmission collisions occur.
- All network port on a hub are considered portso of a single collision domain
- Each port on a switch would create its own network segment

Broadcast Domain
is a group of systems that can receive one another broadcast messages.
- If all network port in hub, and if one system sends broadcast message the message is received by all other.
- all system connected switch and one of the sends broadcast message the broadcast would receive all other device connected switch



GIPTA

NETWORK DESIGN MODEL

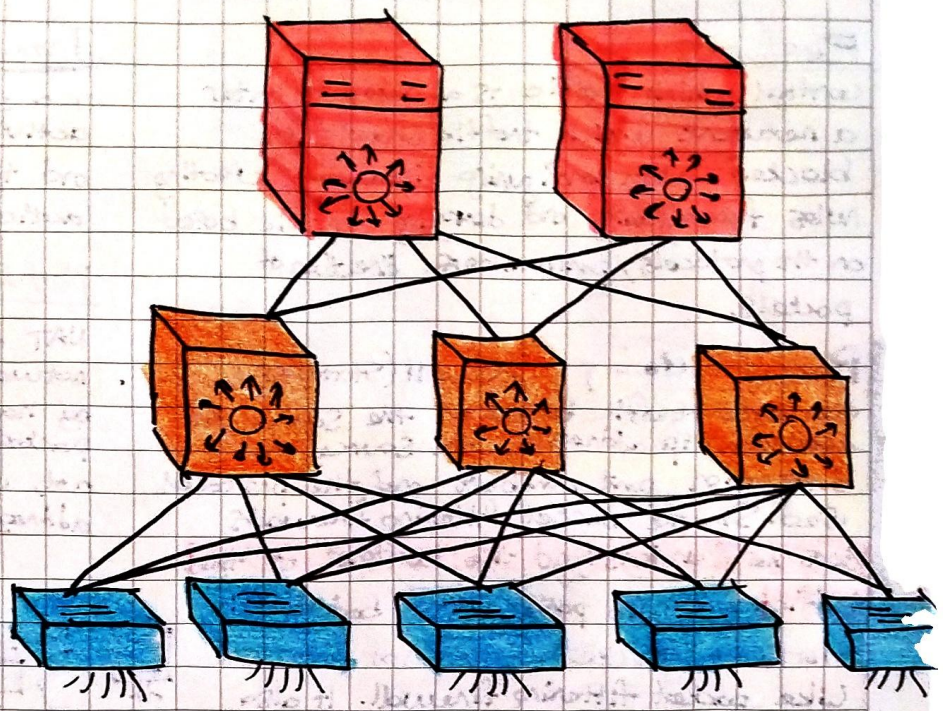
Three Tier Architecture

Collapsed Core Two-Tier Architecture

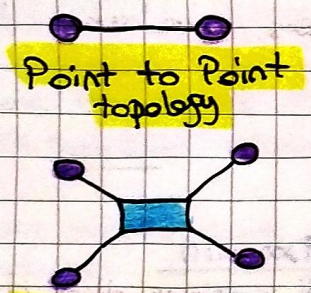
Core — Backbone of the network. Responsible for delivering traffic to and from network

Distribution — Enable you to control who can access the networks such as routing, ACL's, policies
Layer 3 switch

Access — Enables to end users connect to the network via switches
Isolate traffic with different type of users.

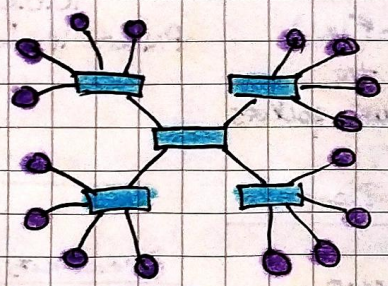


NETWORK TOPOLOGIES.

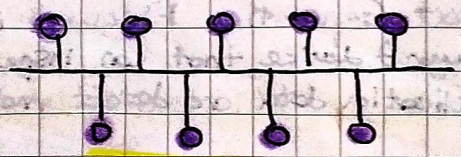


Point to Point topology

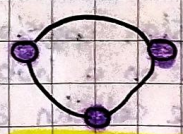
Star topology



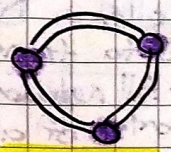
Extended Star Topology



Bus Topology



Single Ring Topology



Dual Ring Topology

Network Architecture	Physical Topology	Logical Topology
ETHERNET	Bus, star, PtP	Bus
FDDI	Ring	Ring
Token Ring	Star	Ring

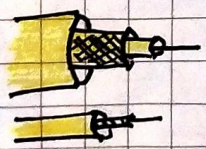
Cable Types

LAN's typically use either copper or fibber optic or Copper cabling uses voltage fiber cabling uses light.

Copper

Thicknet

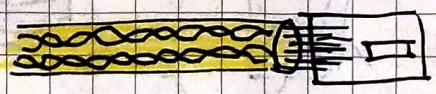
Thinnet



Coaxial

Thin Coaxical

UTP (Unshielded twisted Pair)

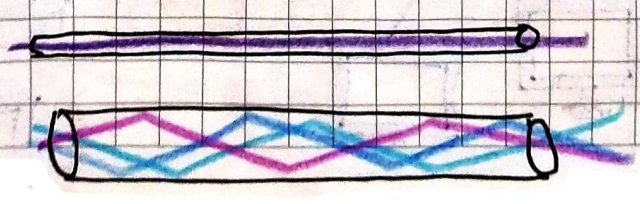


CAT5E
CAT6

Fiber

Single Mode fiber

Multi Mode Fiber

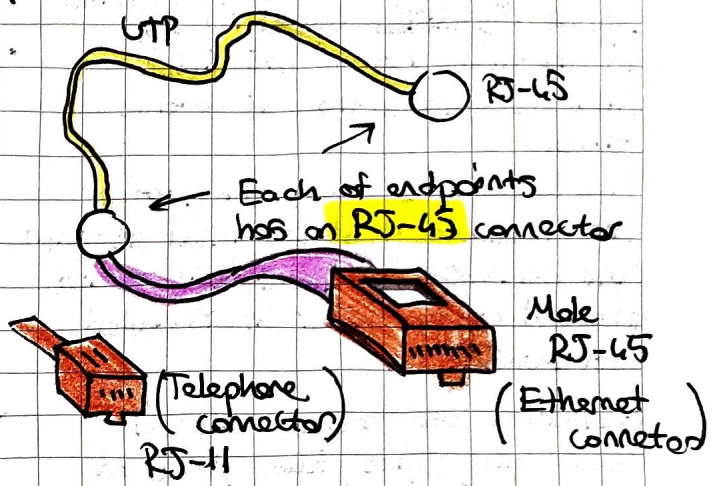


GIPTA

Copper Cabling

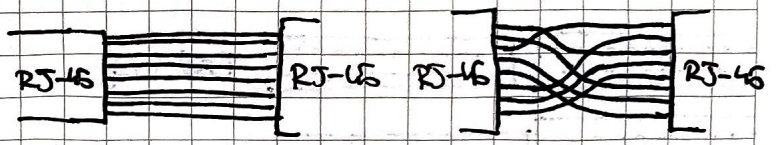
Copper Cabling is less expensive
Three types of copper cabling
Thicknet, ThinNet, UTP
UTP is most common cable because is cheapper, easier to install and troubleshoot.
But it is suspectible to electro-magnetic interference (EMI) and radio frequency interference (RFI)
Distance of cabling is limited. (100 meter)

Eight (8) wires inside the cable is colored, some solid some striped. Two pairs of the wires carry a true voltage called "tip" (T1 - T4), and the other carry negative voltage called "ring" (R1-R4). Generally calls positive and negative wires respectively.



Category	Description
CAT1	Telephone connection (not data)
CAT2	Data, 4Mbps, Token Ring
CAT3	Data, 10Mbps, Ethernet 10BaseT
CAT4	Data, 16Mbps, Token Ring
CAT5	Data, 100Mbps, Ethernet
CAT5E	Data, 1Gbps, Ethernet
CAT6	Data, 1bbps(big), Ethernet
CAT6A	Data, 10Gbps, Ethernet
CAT7	Data, 10Gbps, Ethernet

Two types of implementation are used for a pinouts of the two sides of the wiring - Straight-through and Crossover

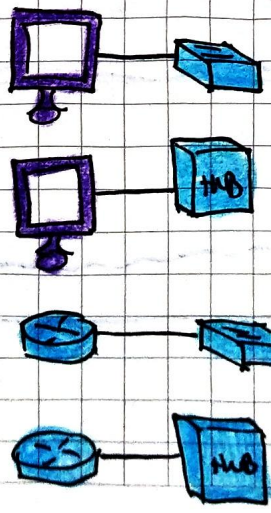


TIA-EIA 568

Pin	Color
1	Orange-white
2	Orange
3	Green white
4	Blue
5	Blue white
6	Green
7	Braun White
8	Braun
1	Green White
2	Green
3	Orange-white
4	Blue
5	Blue-white
6	Orange
7	Braun-white
8	Braun

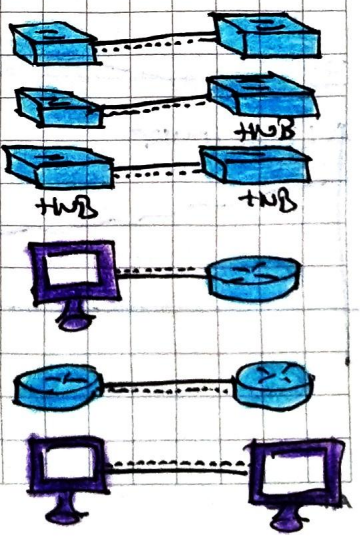
1-1
2-2
3-3
4-4
5-5
6-6
7-7
8-8

Connect devices (dissimilar)



1-3
2-6
3-1
4-7
5-8
6-2
7-4
8-5

Connect devices (similar)



Fiber Cabling

provide very high speeds
span connections across very long distances
It is expensive, difficult trouble-shoot, difficult to install

NOTE: Fiber cabling is not affected by EMI and RFI

The loss factor is used to describe signal degradation or any signal loss in the fiber before the light source gets to the end of the fiber.
The longer the fiber, the greather the likelihood that the signal strength will decrease by the time it reaches the end of the cable. This is called attenuation.

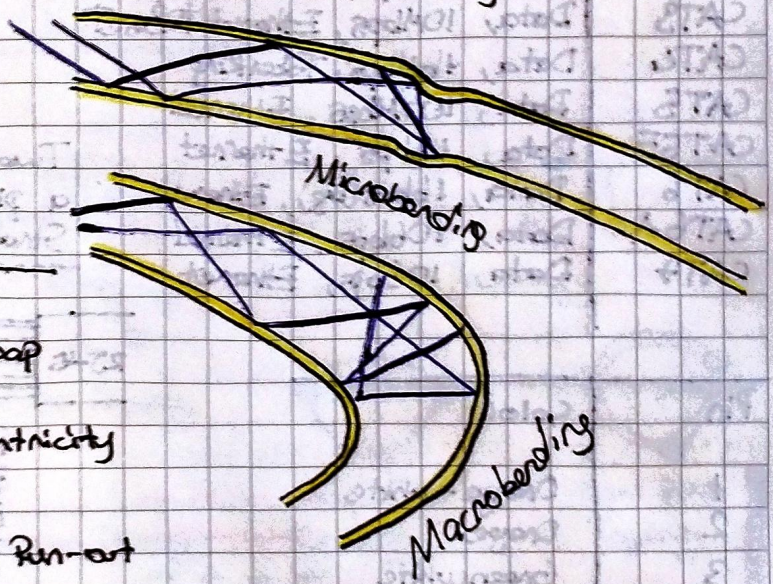
Connector loss occur when a connector joins two pieces of fiber; a slight signal loss is expected

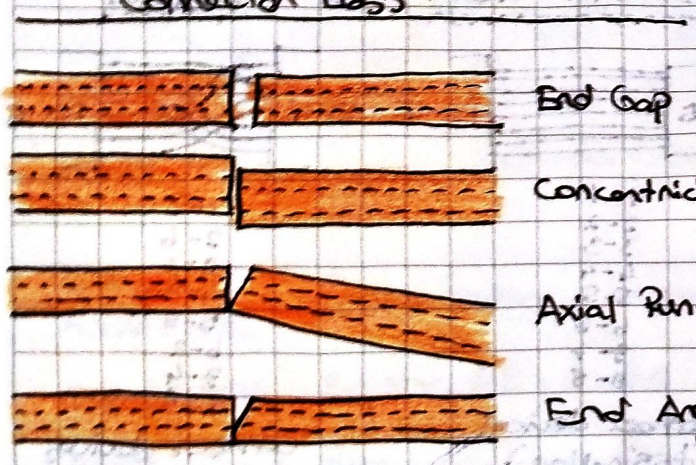
Fiber cabling are used for data connections

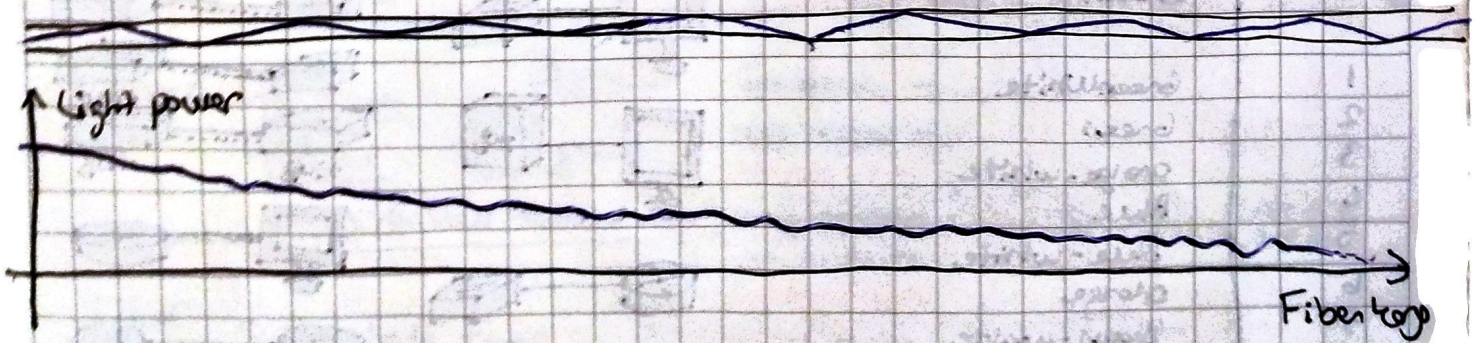
Multimode Fiber (MMF)
- 850–1300 nanometer wavelengths of light
- Fiber thickness for MMF 62.5/125 microns
- Terahertz range (THz)
- Using LEDs

Single mode Fiber (SMF)
- 1300–1550 nanometer wavelengths of light
- more than 10 km range
- 100 Gbps
- SMFs very small core diameter than MMFs
- Using Lasers

Loss factors
- Connector loss
- Attenuation
- Microbending
- Macrobending







GIPTA

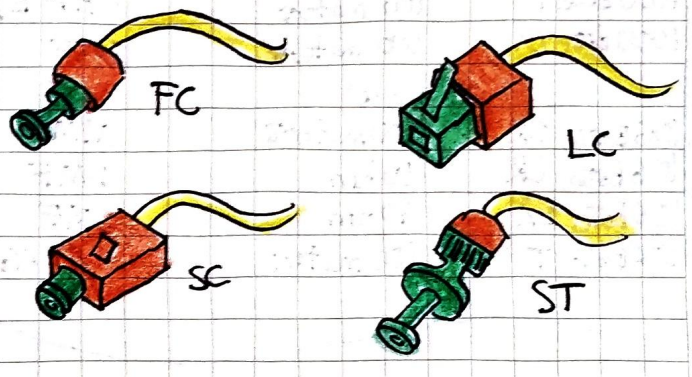
Two main standards are used to describe the transmission of signal across a fiber;
- SONET (Synchronous Optical Network)
- SDH (Synchronous Digital Hierarchy)

SONET is defined by Exchange Carriers Standards Association (ECSA) and American National Standards Institute (ANSI) and is typically used in North America

SDH	SONET
Developed by ITU-T	Developed by ANSI
Deployed in North America extensively	Deployed in Europe and Japan
Data transmission synchronously	Data transmission also available Asynchronously
Overhead 2 bytes	Overhead 9 bytes

Fiber Optic connectors

- Fiber Channel (FC) — Used by service provider in their patch panels
- Local connector (LC) — Used for enterprise equipment and commonly connected to small form-factor pluggable (SFP) modules
- Standard connector (SC) — Used for enterprise equipment
- Straight Tip (ST) — Used for patch panels because of their durability.



ACCESS METHODS

An access method determines how a host will place data on the wire, does the host have to wait its turn or can it just place the data on the wire?

CSMA/CD

Popular

Carrier-Sense multiple access with collision detection

Every host has equal access to the wire and can place data on the wire when the wire is free from traffic. If a host wants to place data on wire, it will "sense" the wire and determine whether a signal is already present. If it is, the host will wait to transmit data, if the wire is free, the host will send the data.

If two systems "sense" the wire at the same time, they will collide with one another and the data will be destroyed. Consequently, after a collision each host will wait a variable length of time to retransmit data.

Token Passing

An empty packet is running around on the wire ("token")

To place data on the wire, the system needs to wait for token packet. Once the system has the token and it is free to data transmit. Since there is only one token and a host needs to have to talk with wire. It is impossible to collision

CSMA/CA

Carrier-Sense multiple access with collision avoidance

It is not as popular like CSMA/CD because before a host sends data on the wire it will "sense" the wire to see if it is free wire. If the wire is free the host will sends "avoid" signal on wire to other hosts to letting all others know they should wait before sending data. This help to prevent collision but includes sending more data on wire.

GIPTA

NETWORK ARCHITECTURES

Half-Duplex | Full-Duplex

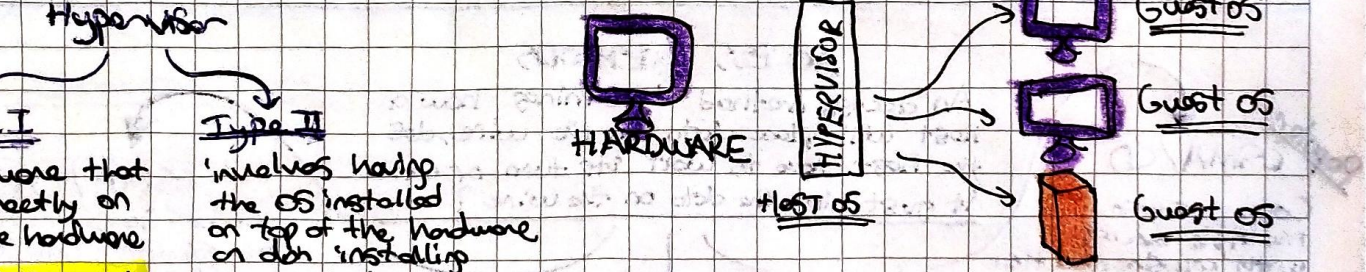
			Interface	Logical	Physical
Ethernet					
10Base5	500 meters	Coaxial (Thicknet)	AUI	Bus	Bus
10Base2	185 meters	Coaxial (Thinnet)	BNC	Bus	Bus
10BaseT	100 meters	UTP (CAT 3,4,5,5E,6,6A)	RJ-45	Bus	Star
FastEthernet					
100BaseTX	100 meters	UTP (CAT 5,5E,6,6A)	RJ-45	Bus	Star
100BaseFX	400 (half-dup) 2000 (full)	MMF (SC, ST)	RJ-45	Bus	Star
100BaseT4	100 meters	UTP (CAT 3,4,5)	RJ-45	Bus	Star
Gigabit Ethernet					
1000BaseCX	25 meters	STP			
1000BaseLX	3-10 km	SMF			
1000BaseSX	275 meters	MMF			
1000BaseT	100 meters	CAT 5E, 6	RJ-45		
1000BaseZX	100 meters	SMF			
10-Gigabit Ethernet					
10GBaseSR	400 meters	MMF			
10GBaseLR	10 km	SMF			
10GBaseER	40 km	SMF			
10GBaseT	100 meters	CAT 6A			

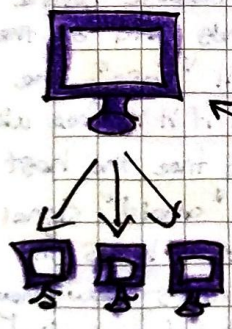
VIRTUALIZING COMPONENTS

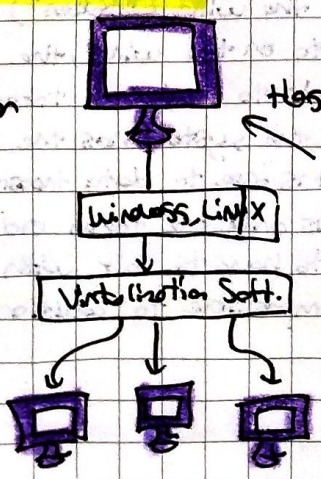
Hypervisors

Virtualization of systems is provided by hypervisors also known as virtual machine monitor (VM

The hypervisors is the software component that enables you to create and run virtual machines on the system.





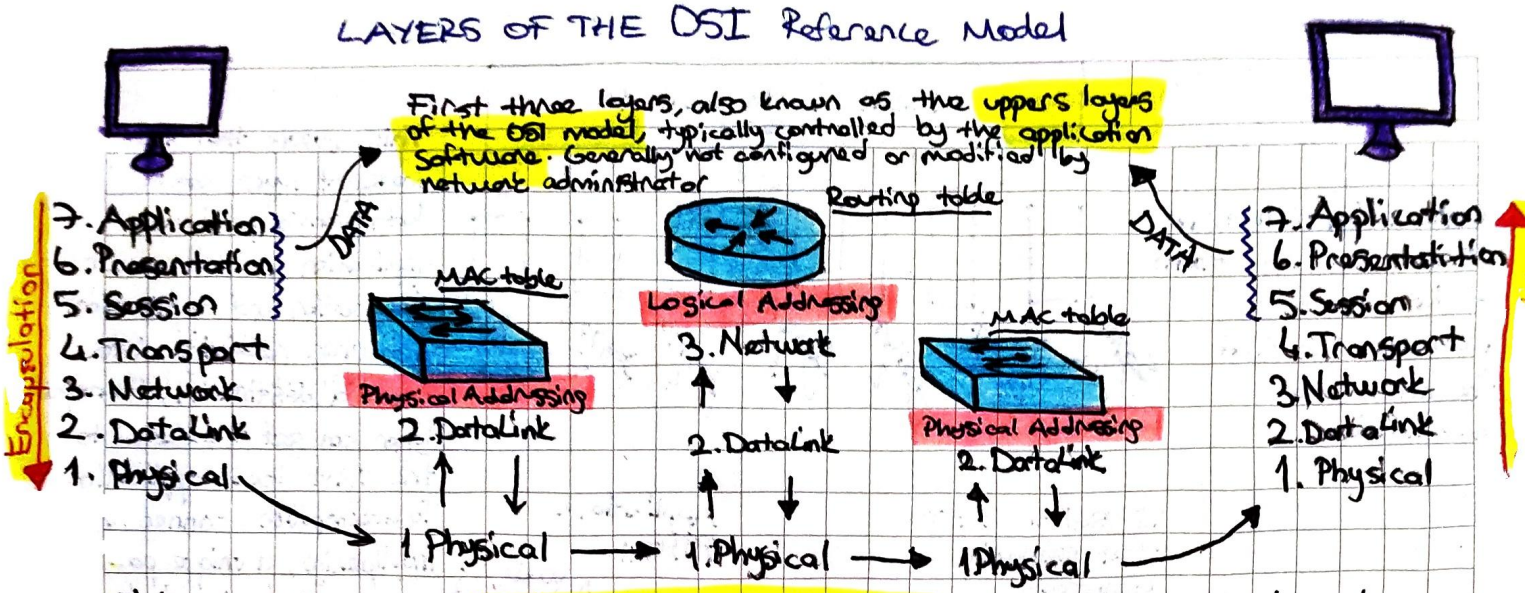


- Virtual Switches
- Virtual Routers
- Virtual Firewalls
- Virtual NIC's
- Software Defined Network (SD
- Virtual Desktops
- Virtual Servers

Virtual Networking components

GIPTA

LAYERS OF THE OSI Reference Model



Network communication starts at the application layer of the OSI model and works its way down through the layers of the physical layer. The data or information passes along the communication medium to the receiving system, which works its way back up to layers starting at the physical layers. to application layer.

7 Application	initiates requests (example HTTP)	DATA
6 Presentation	formats data; compression, encryption...	DATA
5 Session	Establishes and manage session	DATA
4 Transport	Breaks data into segments, ensures delivery	Segment
3 Network	Logical addressing, routing and delivering of packets	Packet
2 DataLink	Physical addressing converts frames to digital signals	Frame
1 Physical	Places signal on the wire	Voltage, Light

Layer 7 Application Layer

The application layer running on the sending system is responsible for initiating the actual request. This could be any type

+ a web request using HTTP
+ a mail delivery request using SMTP
+ telnet, Secure Shell (SSH), File transfer protocol (FTP), Post Office Protocol (POP3)

Layer 6 Presentation Layer

+ When the presentation layer receive a data from the application layer, it makes sure the data is in the proper format, if it is not the presentation layer converts the data accordingly.
+ When the presentation layer receives data from session layer on the receiver system, it make sure the data is in proper format and once again converts it if it is not.

Layer 5 Session Layer

Manages the dialog between computers by establishing, managing and terminating communications between them.

- Ready/Not Ready Signals - Windowing - Flow control - Segmentation - Connection Multiplexing

Another function of the support segment Sequencing.

Also enabled to specify options of "specifyn address" known as a port address. The port address enables the services or applications that are running on the system

TCP/UDP protocols

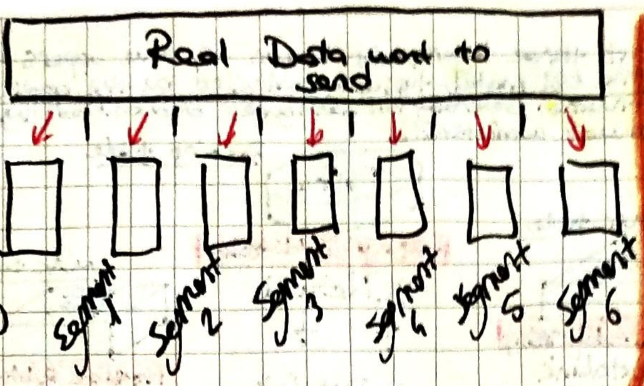
Layer 4 The transport Layer

For reliable transport layer, the transport layer works hard to ensure reliable delivery of data to its destination. On the sending system the transport layer is responsible for breaking data to into small parts. called segments so that if retransmission is needed only the missing segments will be sent. Missing segments are detected when transport layer receive acknowledgement (ACK) from the remote server

Connection Management
Connection Oriented
Communication ensures reliable delivery
Reliable and Unreliable
Connectionless
Communication don't ensures reliable delivery
Monitoring Flow Control Multiplexing

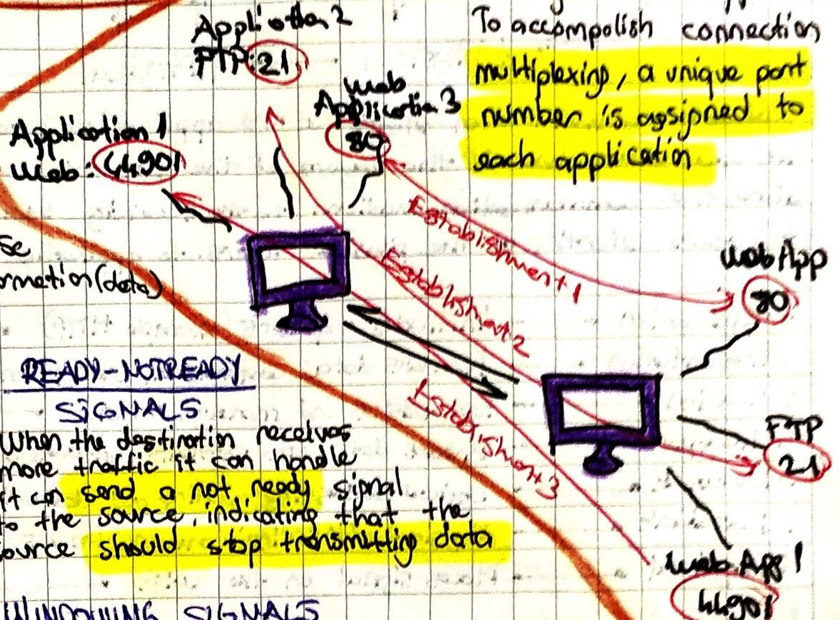
SEGMENTATION
SEGMENTASYON
Bilgiyi bölümleme

Segmentation is necessary to break up large amount of data into more manageable sizes that the network can accommodate



CONNECTION MULTIPLEXING

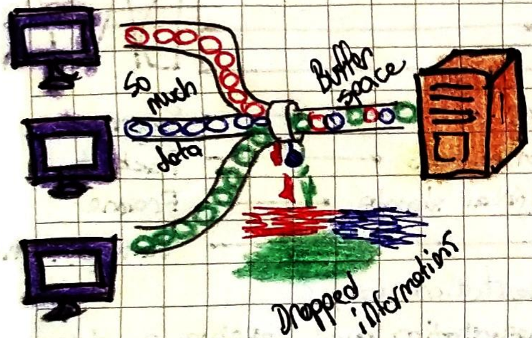
This ensure that the transport layer can send data from a particular application to the correct destination and application and when receiving data from a destination, transport layer can get the data to the right local application. To accomplish connection multiplexing, a unique port number is assigned to each application



FLOW CONTROL:
Paket Akış Kontrolü
Nekadar veri kaldırabilir
Hazır mı, değil mi?

is used to ensure that networking components don't send too much information (data) to the destination.

Overflowing is receiving buffer space and cause it to drop some of the transmitted information (data)

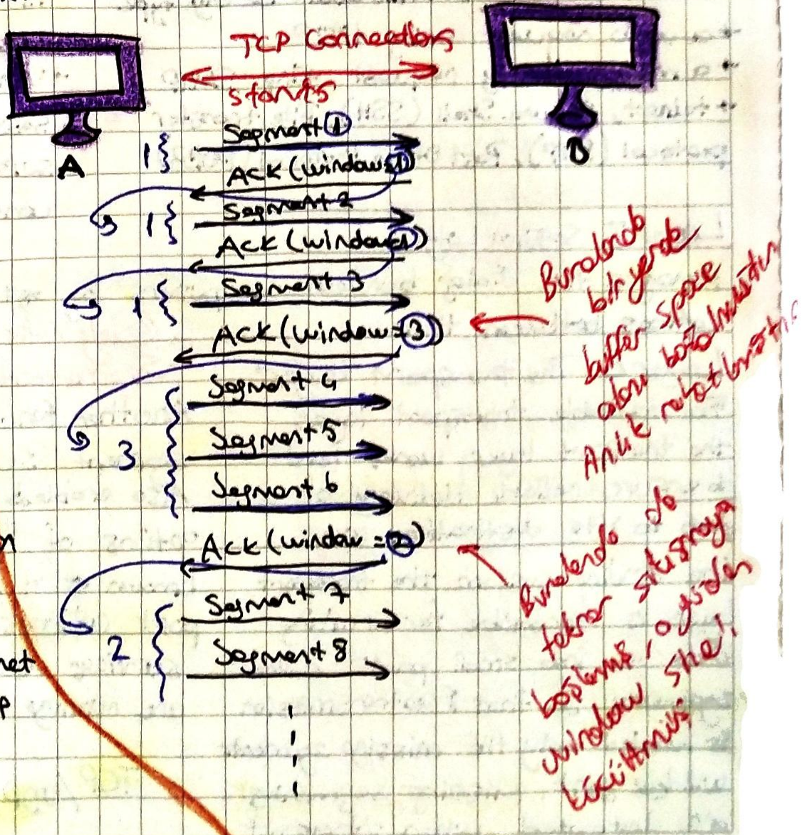


READY-NOTREADY SIGNALS

When the destination receives more traffic it can handle it can send a not ready signal to the source, indicating that the source should stop transmitting data

WINDOWING SIGNALS

A window size is defined that specifies how much data (segments) can be sent before the source has to wait for an acknowledgement (ACK) from the destination



Layer 3 – The Network Layer

is responsible for managing network logical addressing information in the packets and the delivery, or routing of those packets by using information stored in a routing table. The routing table is list of available destinations that are stored in memory on the routers.

Logical addresses uniquely identify a system on the network. In OSI/ISO model it is IP addresses.

- DEFINES LOGICAL ADDRESES USED at Layer 3
- FIND PATHS, based on the network numbers, of logical addresses to reach destination components.
- CONNECTS DIFFERENT LAYERS TYPE WITH EACH OTHER, such as Fiber to Ethenet
- DEFINE SEGMENTATION Via the use of PACKETS to transport Information.

GIPTA

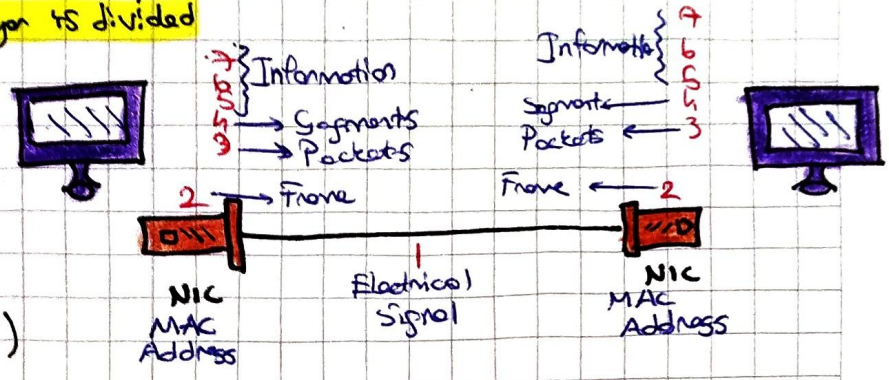
Responsible for error correction and controls functions.

Logical Link control (LLC)

Media Access Control (MAC) → This determine the physical address of the host. How the host places traffic on the medium. (CSMA/CD)

Layer 2 – Datalink Layer

The data is converted from packet to a pattern of electrical bit signals. On the receiving system the electrical signal will be converted to packets by the datalink layer. DataLink Layer is divided into two sublayers.



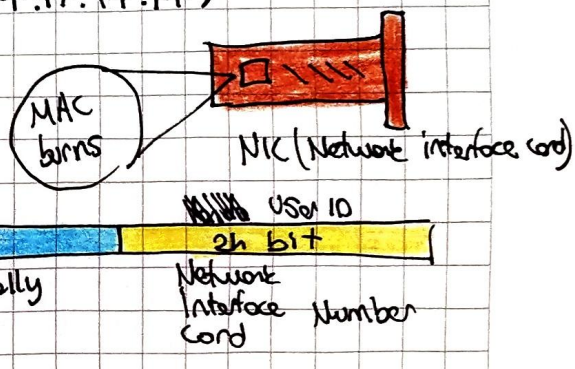
Examples of Layer 2 protocols

LAN
- 802.2 Ethernet II
- 802.3 FDDI
- 802.5

WAN
- ATM (Asynchronous Transfer Mode)
- HDLC (High-Level Data Link Control)
- PPP (Point to Point)
- SDLC (Synchronous Data Link Control)
- SLIP (Serial Line Internet Protocol)
- Frame Relay
- X.25

MAC ADDRESS

48 bit lenght, represents with 12 hexadecimal character. To make easier read the MAC address dotted hexadecimal format (FFFF.FFFF.FFFF) or (FF:FF:FF:FF:FF:FF)



COMMUNICATION TYPES

- UNICAST – single device communication
- BROADCAST – every device on a segment
- MULTICAST – a group of device on a segment

Broadcast MAC destination → FFFF.FFFF.FFFF
Multicast MAC destination → 0100.5EXX.XXXX

Layer 1 – Physical Layer

Moving bits data on network medium. Encoding and timing of bit transmission and reception.

- The type of interface used on networking device
- The type of cable used for connection devices
- The connectors used on each end of the cable
- The pin patterns used on connection on the cable
- The encoding type of message to converting byte to electrical signal

HUBS - REPEATERS - CABLE → Layer (1)
SWITCHES, BRIDGES, NICS → Layer (2)
ROUTERS → Layer (3)

ENCAPSULATION - DEENCAPSULATION

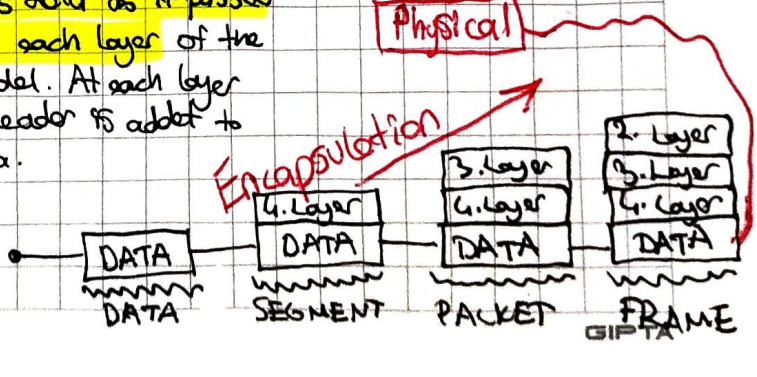
Refers to the fact that as data is passed down to seven layers of the OSI model Header information is added to the message.

De-encapsulation continues up the seven layer of the OSI model. Reverse of encaps:

PDU (Protocol Data Unit) describes data as it passed through each layer of the OSI model. At each layer a new header is added to the data.

PDU terms

Data → Application, Presentation, Session → Segment → Transport → Network → Datalink → Physical → Bits



GIPTA