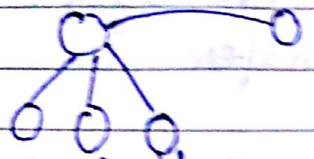
ATM switches: ATM switches can directly communicated with other ATM switches.



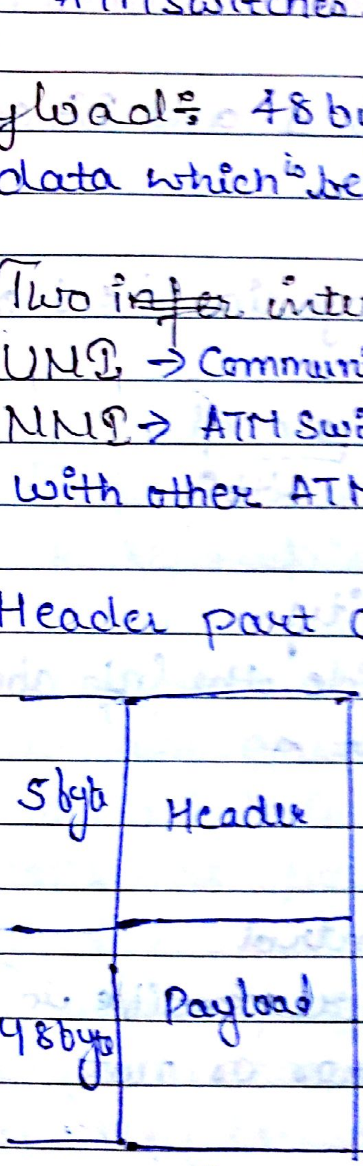
End point : if communication within the single ATM switches.

Payload: 48 byte, which is used to carry ~~to~~ actual data which is being transfered.

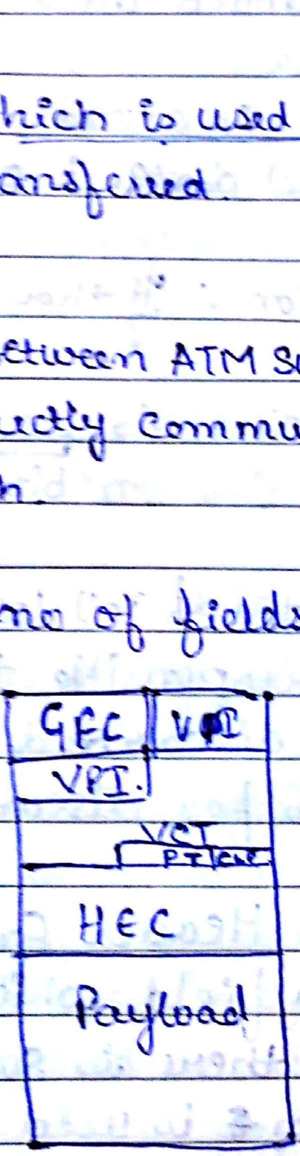
Two ~~infer~~ interface

1) UNI → Communication between ATM Switch and end points
2) NNI → ATM Switch directly communicate ~~b/w ot~~ with other ATM Switch.

Header part consist no of fields:



Cell



UNI cell

It consist info about which IP is exist in a Header part

GFC: General flow control

- It is a field which provide the info. how many end points are connected with ATM Switch.
- It is set on a default value.

Date

Page

- VCI → virtical channel Identifier f in particular way. how many routers and IP ~~are~~ address are used.
- VPI → virtual path Identifer., it a way through which data is transfer.

- PT → Payload Time It consist of actual data or controlled data. Bits are used to notify the data

Bit set in actual data is 1 and Bit set for controlled data is 0

Conjestion : If there is conjestion i.e 1 other wise 0

Cell recieve is $\underbrace{\text{last}}_{\text{bit 1}}$ or $\underbrace{\text{more cell}}_{\text{bit is 0..}}$.

CLP : Stand for Cell loss priority

It is responsible to provide the info about wheather cell is discarded or not

1 bit is for discarding.

HEC → Header Error Control

It is a field which is responsible to check whether there is some error or not

Checksum ~~f~~ is used.

In ~~UNI~~ NNI cell ~~there~~ ~~is~~ GFC field is not available

Layered Architecture of ATM or ATM refference Model:

It consist of three layer.
ATM Adoption layer. it is also known as AAL
ATM layer
Physical layer

ATM Adoption Layer:- Classes of AAL: ie
AAL1
AAL2
AAL3/4
AAL5

(1) Physical layer of ATM Protocol: ATM physical layer has four function

(1) Cell are converted into bits stream.
(2) Transmission and recipt of bits on the physical medium are controlled.
(3) ATM cell boundary are crack
(4) cells are packaged into the appropriate frame

Physical layer is divided into two Subparts:
(1) Physical medium dependent (PMD): It provide
(2) two Key funcrions
(1) It synchronize transmission and reception by ~~of~~ sending and recieving a continous flow of bits with associated time information
(2) It specify the physical media for the physical medium including ~~Collector~~ Connector type and cables

(II) ~~T~~C (Transmission convergence): ~~T~~ TC Sublayer has four functions :-

1) Cell dalination.
2) Header error control/
~~3)~~ squence verification & generation
3) Cell Rate decoupling
4) Transmission frame Adaptation

II :- ATM layer :- This layer combine with ATM Adaptation layer, ATM layer is roughly analogous to the data link layer of the OSI reference model.
ATM layer is responsible for the simontaneous Sharing of virtual circuit over a physical link and passing cells through the ATM network. To perform this particular task, It uses the BVPI and VCI information in the header of each ATM cell.

III :- ATM Adaptation layer :- ~~It~~ combine with ATM layer. This layer is reaponsible for isolating higher layer protocol From the detail of the ATM processes. The Adaptation layer prepare users data for Conversion into cells and segments The data into 48 byte cells payload.

	IPV4	IPV6
①	IPV4 addresses are 32 bit length	IPV6 address are 128 bit length
②	Fragmentation is done by sender and forwarding Router	Fragmentation is done by Sender.
③	No packet flow identification	Placket flow identifiation
④	Checksum field is available	No checksum field is availble
⑤	Broadcast Manages are available	Broadcast manage are not available.

Header part Consist of no of fields.

① General flow Control (GFC) ÷ Provides local functions, Such as identifying multiple Stations that Share a Single ATM interface. This field is typically not used and is set to it default value of 0

② Virtual Path Identifier ÷ In conjunction with the VCI, identifies ~~multiple~~ the next destination of cell as it passes through a Series of ATM Switches on the way to its destination.

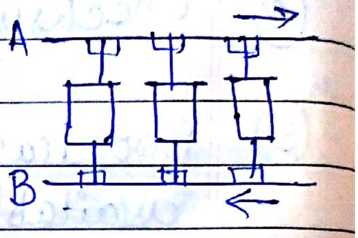
③ Virtual Control Identifer.

④ Payload Time ÷ Indicates in the first bits whether ~~the~~ cell contain user data or control data the cell contain user data, the bit is set to 0

If it contain Control data it is Set to 1.

Cell Loss Priority (CLP) ÷ If the CLP bit equals 1 the cell should be discarded in prefrence to cells with CLP bit equal to.

DQDB ÷ Distributed Queue Dual bus ÷ It is a protocol which is work under the network i.e MAN. Coxial-Cable used.
Standard used for DQDB protocol i.e IEEE 802.6.



Both bus are capable ~~of 5~~ to travel a cell of 53 byte cell
Packet transfer rate is high

→ DQDB Protocol / Message ÷

1. Buzy
2. Request

Buzy ÷ When any station wants to travel packet at any destination i.e is Buzy protocol. Request is 0 & Buzy = 1

Request ÷ Destination request from any source at that particular time Request is 1 & Buzy = 0

DQDB Cell format ÷

5 byte	1 byte	1 byte	44	1 byte	1 byte
Header	ST	MID	information	LEN	CRC

ST ↓ Segment Time

MID ↓ Manage Identifier

LEN ↓ Length of data

CRC ↳ cyclic Redundancy check
• To Check out the Checksum

DQDB Header format÷

<table>
<tr><td>Bits</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td></td></tr>
<tr><td></td><td colspan="8">ACF (Access Control field)</td><td>1</td></tr>
<tr><td></td><td colspan="8">VPI (virtual path Indentifier)</td><td>2</td></tr>
<tr><td></td><td colspan="8">VCI (Virtual channel Identifier)</td><td>3 Octets</td></tr>
<tr><td></td><td colspan="3">VCI</td><td colspan="2">PT</td><td colspan="3">CLP</td><td>4</td></tr>
<tr><td></td><td colspan="8">HEC</td><td>5</td></tr>
</table>

DQDB÷ IEEE defines a MAN standard. It is distributed Queue data interface & put up as IEEE 802.6 Standard.

Two parallel unidirectional buses are laid down in the area to be converied by the network. The Stations are attached to both the buses in parallel. Each bus has had, which generates steady Stream of 53 bytes cell. Each can travels downstream from the head end.

Each cell holds two protocol bits.

① Busy ÷ Busy set to indicate the cell is occupied
② Request ÷ which can be set when a station wants to make a request

To transmit a cell, a station has to known whether the destination is either Right or left side. If the destination is to be right, the sender uses bus A otherwise it was bus B

In 802.6 protocol it queue up data and becomes ready to transmit in FIFO order

Section-B

Network layer Protocol

- On Network layer Packet is responsible to ~~delivery~~ carry of ~~pathe~~ information.

- Router is a device which is used to provide Connectivity between two different network

- Hope count : It is in case of Router. For delivery of packet how many router is used in between the source & destination. It is also known as Matric

- Protocol is responsible for delivery of packet

To successfully perform Routing it is divide in two part

1. Routing protocol
2. Routed protocol

✓ (1) Routing protocol : Which one is the benifical way b/w source & destination & less no of Hope count is used, Provide vitrual physical path with Low Conjection.

It provide a way or link.

(2) Routed protocol : It provide Connectivity b/w source & destination eg of Routed protocol is IP, Apple talk

Imp (1) Routing protocol is divided into three categories.

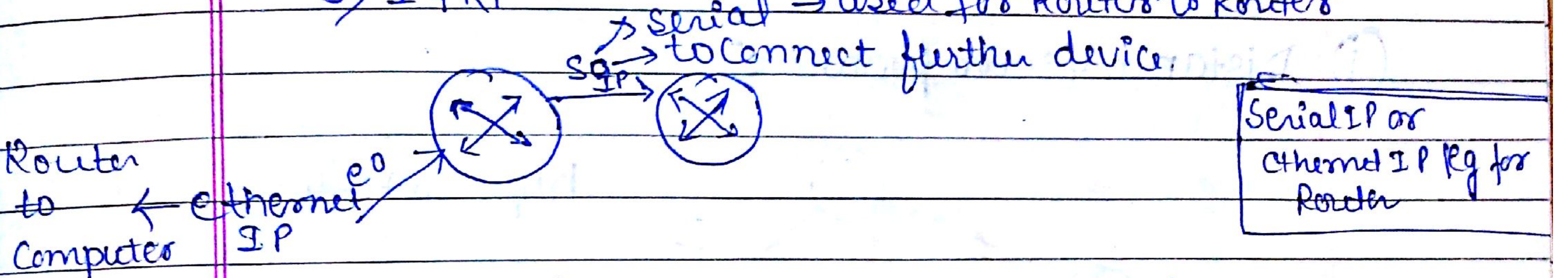
R.P.

Distance Vector | Link State | Hybrid.

Protocol used 1.) RIP
2) RIPV2
3) IGRP

1) OSPF

1) EIGRP


Serial → used for Router to Router
→ to Connect further device.
S0 IP
e0
Router to Computer ← ethernet IP
Serial IP or ethernet IP Rq for Router

- RIP:- Stand for Router Interrelation Protocol
- IGRP:- Interior gateway ROuting protocol.
- OSPF:- Open Shortest path first
- EIGRP:- Enhanced interior gateway Routing protocol

(2) Routed protocol is divide in three category:-

Routed protocol.

Static Routed | Dynamic Routed | Default Routed

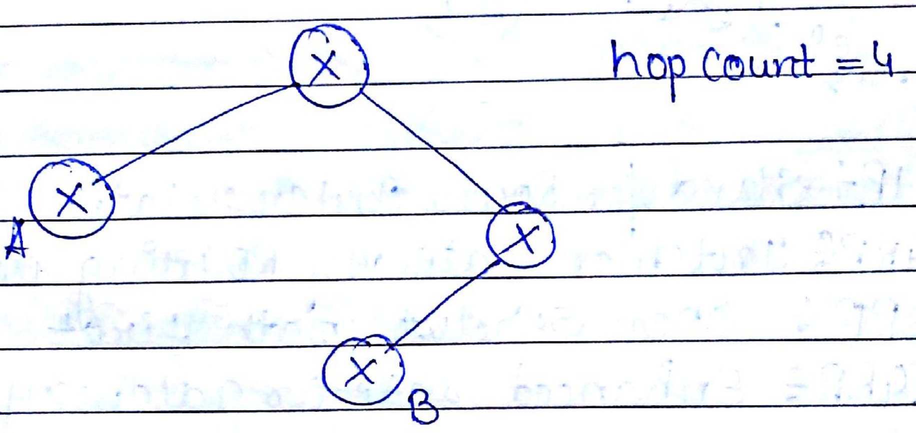
- A Router is a type of internetworking device that passes data packets between network based upon layer three address
- The purpose of Router is to examine incomming packet, choose the best path for them through the network and then

Switch them to the proper outgoing port

Gateway ÷ It operates on all the layers of OSI model.

(2) It is a protocol convertor.
(3) It can accept a packet for a one protocol and convert it into a packet format for other one protocol.

(1) Distance Vector protocols:



- It is responsible to provide shortest path ~~Shortest path means less no of Hop Count~~
- It responsible to find out in which way less no of hop count is used with low conjection.

(2) Link State: It provide the information about the neighbourhood router

Information related to logical address is state by link state

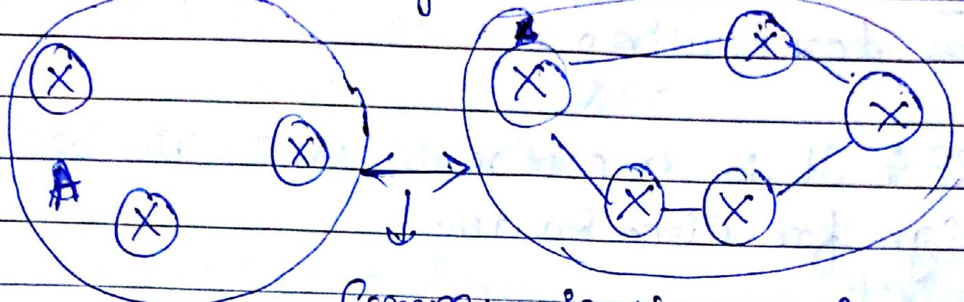
Routing information ~~upate~~ update.

③ Hybrid protocol:- It is Combination of Distance vector & Link State

According to region router are count in Hybrid protocol.

Region to Region information Stored.

AS → Autonomus System → Outside no router intefere



Communication provide → AD is responsible. } → Trust

Information Stored in two way:-

Autonomus System:- It is a Collection of group of router under a Common adminstration i.e About Autonomus system

~~AD~~ CA

In Case of region layout the packet is delivered with Accurate information.

→ Adminstrative Distance:- It is a value either 0 or 1

0-255 numeric value is assign if value assign is 0 then trust is full Value increase trust decrease

• It is used for Trust worthyness of packet

→ • RIP:- It is responsible to provide the about No of hops.

② It is a protocol which is responsible to update the routing information about every 30 second

③ for single It provide information about 15 Hops

- It provide ~~15~~ max ~~#~~ 15 hope of information.
- RIPV$_1$ provides the Connectivity for class ~~less~~ full Routing
- RIPV$_2$ is responsible to provide the Connectivity Class less Routing .

3) IGRP ÷ It is a protocol which is basically Design for Cisco Router

- It is responsible for 255 hops of information.
- It is used for long distance
- It is a protocol which is responsible to update the information after 90 seconds

Timer are used ÷

(1) update timer
(2) Invalid timer
(3) Hole down timer

Que1) A Computer circuit board. install on a ~~Com~~ Computer So that it Can be connected to a network

[✓ (1) NIC] (2) ~~Ethear~~ Switch (3) RJ45 (4) HUB

Que2) A NIC card can be used for

(1) FTTI [✓ (2) Ethernet] 3:) ~~#~~ Microwave (4) Wi-fi

Que3) Which of the following is unbound transmission media :

(1) UTP (2) Co-axial [✓ (3) Microvare] (4) fiberoptic

Que4) which of the following memory needs to be refresh
(1) SRAM [✓ (2) D-RAM] (3) ROM (4) All of the above

Ques5) which is the reserved address for private Network
[✓ (1) 10.0.0.0 to 10.255.255.255]
(2) 128.0.0.0 to 191.255.255.255
(3) 150.0.0.0 to 150.255.255.255
(4) 202.40.55.0 to 202.40.55.255

Que6 which one is the least expensive device typically work at physical layer OSI ~~ka~~ model.
(1) Router (2) Bridges [✓ (3) Repeater] (4) Gateway

Que7.) Frames from one lan can be transmitted to an another lan with the device
(1) Router [✓ (2) Bridge] (3) Repeater (4) Modem

Que8) which of the following condition is used to transmitt two packet over a medium at the same time
(1) Contension [✓ (2) Collision] (3) Synchronous (4) asynchronous 5) None of the above.

Que9 which answer correctly list the OSI, PDU in order
(1) Data, Packet, Frame, Segment, Bit
(2) Bit, Data, Packet, segement, Frame
[✓ (3) Data, segment, Packet, Frame, Bit]
(4) Bit, Frame, Segment, Packet, Data

Que10) which transport layer protocol provide connection oreinted, reliable transport.
(1) TFTP [✓ ii) UDP] 3) Ethernet 4) TCP 5) Secure Shell.

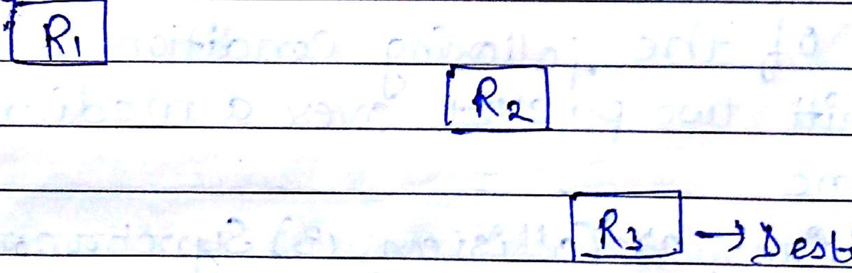
Que Diff b/w TCP & OSI reference mode
Que Design Self formant for UNI or NNI

✓ Link State Routing Protocol.
→ OSPF

Link State:
To get information regarding the neighbours & on which topology it is based
OSPF layer is reponsible for info regarding the neighbo

Each Router Generate Routing table it include Current id, Destination id, Neighbourhood Router

① Advertisement → it is also Known as Link State Adver tisement (LSA) → ~~To~~ a particular network what IP is assign, on which ~~it~~ topology it depend, nod Router for established for Particular network.



Features of OSPF: ① It is a protocol which is based on class less network
② It is Scalable & extendable
③ It is faster than distance Vector protocol
④

EIGRP :- ① It is upgradation of IGRP & RIP protocol.

② It is a protocol which is used for class full routing.

③ It uses hello packet to get neighbour routing information

④ It has a capability to support multiple protocol.

Routed protocols:-

→ Static → Responsibility on Administrator.

→ Dynamic → ~~S~~ Set of Routing protocol are being used

→ Default.

Q On which mode router is Configure

→ Source id

→ Destination id,

→ Subnet Mask.

→ Syntax to provide path:-

# Source id Destinationid SubnetMask.

<table>
<tr><td>VER</td><td>HL</td><td colspan="3">Types of Services</td><td>Total length</td></tr>
<tr><td colspan="2">Indentification</td><td>▨</td><td>D F</td><td>M F</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to live</td><td colspan="3">Protocol.</td><td>Header Checksum</td></tr>
<tr><td colspan="6">Source address</td></tr>
<tr><td colspan="6">Destination address</td></tr>
<tr><td colspan="6">option.</td></tr>
</table>

IPV4 header is of 32 bits.
Header is divided into no of field

① VER → Version

② IHL → IP Header length ① Total length header & total length of information.

③ Type of Services :-

- Simple text
- Composite text, image
- ~~Veo~~ Video

1) Which type of data is required using
2) Which type of Connection we are using either Connection oriented & Connectionless

④ Total length :- ① Total length of header & total length of information.

⑤ Identification :-

DF :- Donot Fragment
If DF is 1 then it is actual data
If 0 the fragment is consider.

MF: More fragment
0-fragment is considered, flag is activated MF

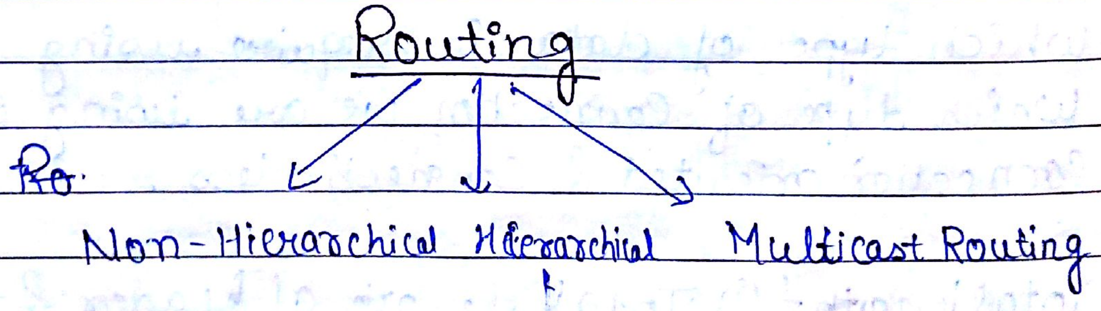
Fragment offset ÷ it provide info about that current Segement

Time to live: Max limit is 255 sec.

Protocol:

Header Checksum: It depend upon Security level.
Heao

Option ÷ It is for Security, strict Routing, loose routing



802.3

Ethernet | IEEE :- The term ethernet refers to the family of local area network implementations that include three prinicipal categories

- Ethernet & IEEE 802.3 :- LAN specification that operate at 10 mbps over coaxial cable.

- 100 mbps ethernet :- single LAN specification that operate at 100 mbps over twisted pair cable also known as fast ethernet.

- 1000 mbps ethernet - Single LAN Specification also known as Gigabyte Ethernet that operate at 1000 Mbps over fiber & twisted cable

Preamble	Destination address	Source address	type	data	FCS

Preamble	S O F	Destination address	Source address	length	802.2 header data	FCS

→ frame check sequence

- Preamble :- The alternative pattern of ~~o~~ one & zero tells that receiving station that a frame is coming. The ethernet frame includes an additional byte that is equivalent of start of frame (SOF)

SOF - The IEEE 802.3 delimiter bytes ends with two consecutive 1 bit which serve to synchronize the frame-reception portions of all stations on LAN SOF is explicitly specified in ethernet.

Destination & Source address;- The 1st three byte of address are specified by IEEE vendor. The last 3 bytes are specified by the ethernet or 802.3 vendor. The source address is alway unicast. The destination address ~~is~~ can be unicast, multicast or broadcast.

Type:- Type specifies the upper layer protocol to recieves the data after ethernet processing is completed.

length (IEEE 802.3):- Length indicates the no of bytes of data that follows this field.

Data(ethernet):- After physical layer & link layer processing is complete. The data contained in the frame is send to an upper layer protocol which is identified in the type field. Although ethernet version 2 does not specify any padding Ethernet except at least 46 bytes of data.

Data (IEEE802.3):- After physical layer & link layer processing is complete. The data is sent to an upper layer protocol which must be defined within the data portion of frame.

FCS:- The sequence contains a 4 bit cycle Redundancy check (CRC) value is created by the receiving device to ~~the~~ check for damaged frame.

Transport layer ÷ It is responsible to provide smooth connection

A {
P } - End user laya
S
T

N {
D } - Create a network Connection
P

② Reliability

③ It act as interface between upper layer & bottom layer

④ It is individual layer ~~which~~ who is responsible to provide Quality of Services

→ Quality of services ÷

- Connection establishment delay ÷ It ~~include~~ provide total time limit to set up a connection between source & destination

- Connection establishment failure probability ÷ How many time network fails

- Throughput ÷ s ←→ d set persecond.

- Transit delay ÷

- Residual ~~accuray~~ error ratio ÷

- Priority ÷

~~Too~~ It used transport entity to transfer the packet efficient

Transport Entity ÷
Hardware or Software with in the transport layer than performs the debue work is known as the transport entity. The transport entity can be in the operating system Kernal in a library package bound into the network application or

On the Network interface card(NIC)
In some cases it may provide a reliable transport Service in which the transport entity lives on special interface machine to which the hosts connect

→ What is a difference b/w Data link layer & transport layer

- In Data Link layer :- ~~It~~ it is not necessary for a router to which router specify router it want to talk Each outgoing line uniquely specify ~~the~~ a particular Router

- In Transport Layer:- Explicit addressing of destination is require

Transport layer Primitives:-

① Listen :- Sender ~~sender~~ Send request ~~Send to~~ Destination then destination should analyze and set up a connection.

~~TPDU~~ → Segement is called TPDU (Transport Protocol Data Unit

S ←———→ D
TPDU=1 TPDU=0

② Connection ,③ .

③ ~~④~~ Data :-

④ Receive

⑤ Release Connection:- S ←——→ D
TPDU=0 TPDU=1

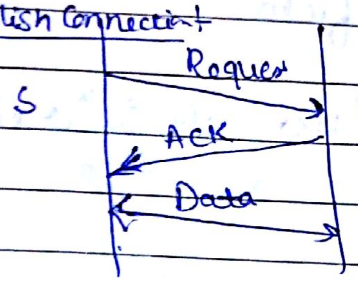
There Two main task are performed

(1) Establishment

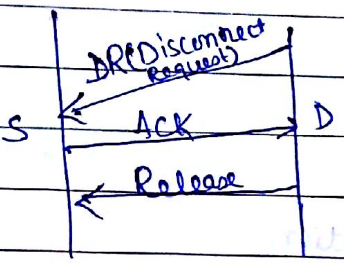
(2) Release Connection

It is a process which based on Three way handshaking

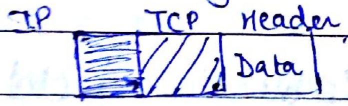
To Establish Connection:

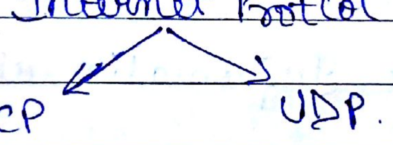


Release Connection:



TCP/IP:- They are bound with in a single unit





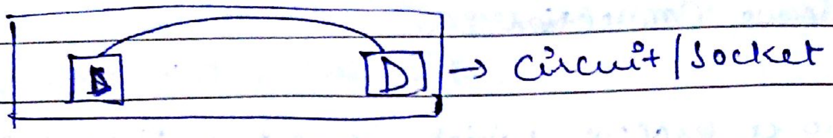
Total length of TCP is of 32bit ← TCP

Header Part TCP:-

<table>
<tr><td colspan="5">Source port</td><td colspan="4">Destination port</td></tr>
<tr><td colspan="9">Sequence Number</td></tr>
<tr><td colspan="9">Acknowledgement No.</td></tr>
<tr><td>Total header length</td><td>6 bit Blank field</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>window size</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="9">options (0 to 32 words</td></tr>
<tr><td colspan="9">Data</td></tr>
</table>

Port ÷ It is destination'id or source id

Circuit or socket ÷ ~~when destination~~ When these are Connected to each other



URG - Urgent it is 1bit field.

ACK - Acknowledgement no. It is in relation to URG.

PSH - Push

RST ÷ Reset

SYN - Syncronization.

FIN - Final/Finish.

→ Window Size ÷ It is variable size field. It varies on the actual size of data.

→ Urgent pointer ÷ Information about the next segment.

→ Header of UDP ÷

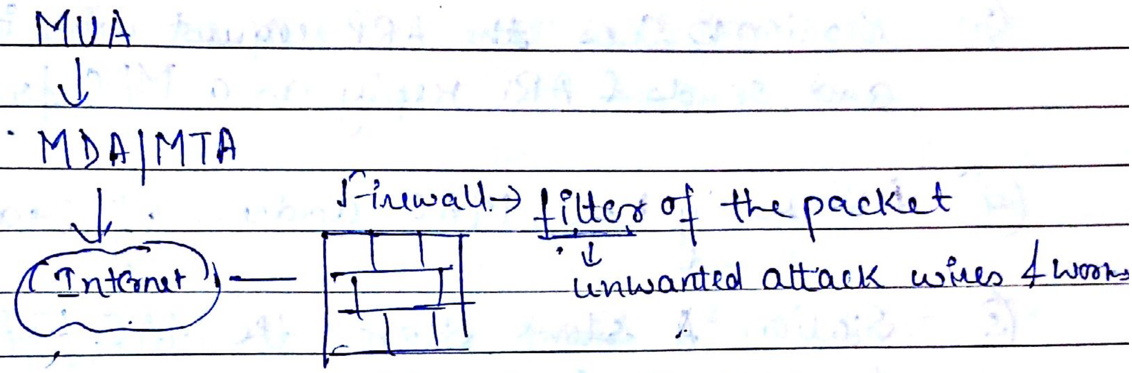
Source Port	Destination Port
UDP length	UDP Checksum

Application layer:

WWW: It is Know as 3w. It is a web.

→ It is a directory which consist of a no of web pages on global platform.

Inner working of E-mail+


MUA
↓
MDA/MTA
↓
Internet
Firewall → filter of the packet
↓
unwanted attack wires & worms

ARP & RARP, TCP, UDP, IP, ICMP

~~ARe~~ ARP → Address Resolution protocol →

1. An IP address identify the logical access to an IP network
2. ~~M~~ The Station can be reach without any further addressing if with physical network consists only of point to point connection.
3. On a share media LAN, MAC addresses are used to delivered packet to a Specific Station ~~a~~
4. ~~A~~ mapping b/w IP address & MAC address is needed
5. A mapping b/w MAC & protocol address on a LAN can be static (Table entries) or dynamic (ARP protocol)

~~A mapping b/w MAC & protocol address on a LAN Can be Static~~

Operation of ARP :-

(1) Station A wants to Send to Station B and doesn't Know the MAC address (Both are connected to Same LAN)

(2) A Sends a ARP request in form of MAC broad cast, ARP request holds IP address of B

(3) Station B Sees the ARP request with its IP address and sends & ARP reply as a MAC frame

(4) ARP reply holds MAC address of Station B

(5) Station A ~~Stores~~ Store the MAC/IP address mapping for station B in its ARP Cache

(6) For Subsequent packet from A to B or from B to A the MAC address are taken from the ARP Cache.

(7) Entries in the ARP cache are deleted if they are not used for define period. Usually 5 minutes

→ ~~AR~~ RARP :-

(1) ARP assume that an IP Station knows the IP address (stored in ~~a~~ NVRAM, in harddisk, inconfiguration file etc)

(2) Diskless machine doesnot have such means, So they must retrieve an IP address for network ~~working~~ booting

③ Reverse ARP provides IP address for Unconfigured stations.

RARP operations :-

① A station sends a RARP request broadcast

② One station, the RARP Server looks up the IP address for the MAC address in ~~the~~ a database and reply.

Session Layer

→ Dialog management :- There are many different points for achieveing application check point depending upon the specific implementation. Tool can be classified as having serveral property

① Amount of state saved :- ~~This~~ property refers to the abstraction problem used by the technique to analysis an application It can range by application as a black box, hence storing ~~all~~ application data, to selecting specific relavent ~~Course~~ ports of data in order to achieve a more efficient & portable operation

② Automatization level :- Depending on efforts needed to achieve fault tolreance ~~to~~ through the use of specific Checkpointing solution

③ Portability :- wheather or not the same state can be used on different machines to restart the application

④ System Architecture :- How is the checkpointing technique implemented inside a library by the compiler on at operating system level

Synchronization :- It refers to twodistinct but related concepts

① Synchronization Of processes
② Synchronization of data

Process Synchronization refers to the idea that multiple processes are to join up ~~&~~ or handshake at a certain point so as to reach Certain Sequence of action.

Data Synchronization refers to idea of istore multiple copies of data set ine: ~~clo~~ coherance with another of to maintain data integrity.