Some Topics

Token Ring

- Ring topology is used
- Access control method used is token passing
- Token ring is unidirectional
- Data Rate used is 4mbps & 16mbps
- Piggibacking acknowledgement is used
- Differential Machester encoding is used
- Variable size framing
- Monitor station is used

- Topology – Ring topology
- Transmission – Unidirectional
- Encoding – Differential Manchester encoding
- Access control – Token passing
- Data rates – 4 Mbps, 16 Mbps

Token Ring Frame format: (IEEE 802.4)

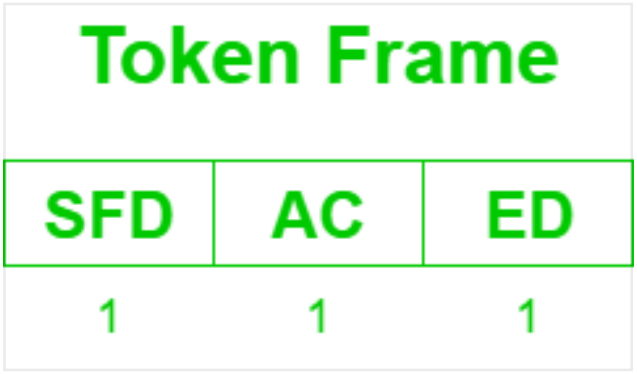
Data Frame

SFD	AC	FC	DA	SA	Data	CRC	ED	FS
1	1	1	6	6	>= 0	1	1	1

Ethernet (IEEE 802.3) Frame Format

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

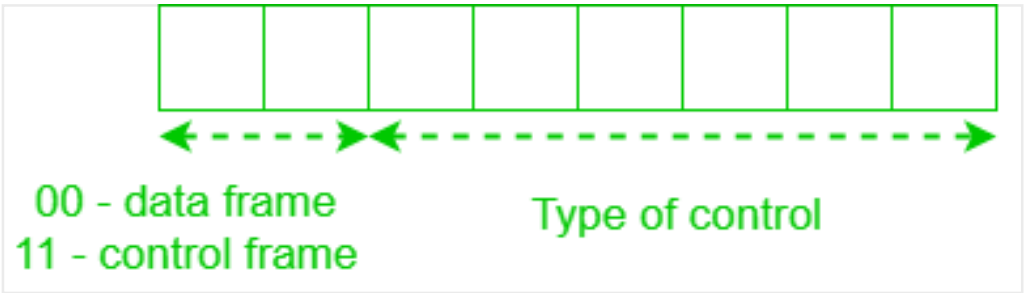
IEEE 802.3 ETHERNET Frame Format



- Start frame delimiter (SFD) – Alerts each station for the arrival of token(or data frame) or start of the frame. It is used to synchronize clocks.

- Access control (AC) –
  Priority bits and reservation bits help in implementing priority. Priority bits = reservation bits = 3. Eg:- server is given priority = 7 and client is given priority = 0.
  Token bit is used to indicate presence of token frame. If token bit = 1 –> token frame and if token bit = 0 –> not a token frame.
  Monitor bit helps in solving orphan packet problem. It is covered by CRC as monitor are powerful machines which can recalculate CRC when modifying monitor bit. If monitor bit = 1 –> stamped by monitor and if monitor bit = 0 –> not yet stamped by monitor.

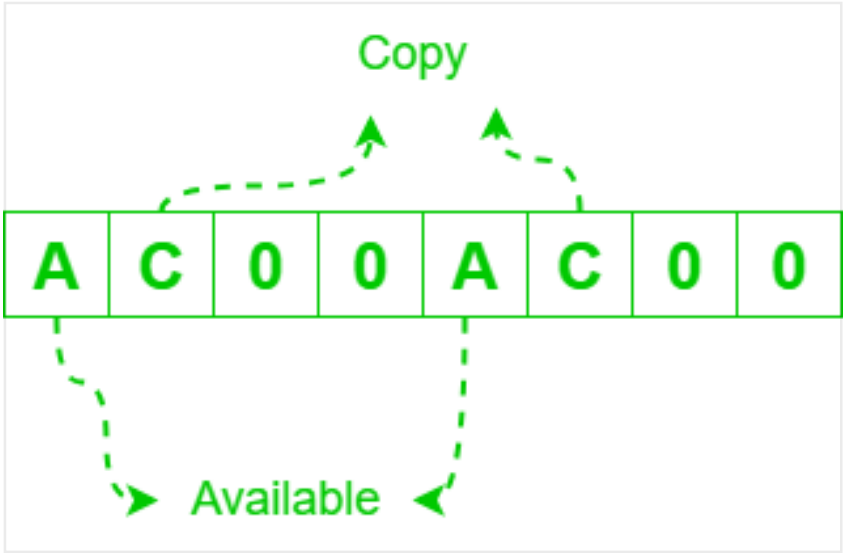
- Frame control (FC) – First 2 bits indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

- 

- Destination address (DA) and Source address (SA) – consist

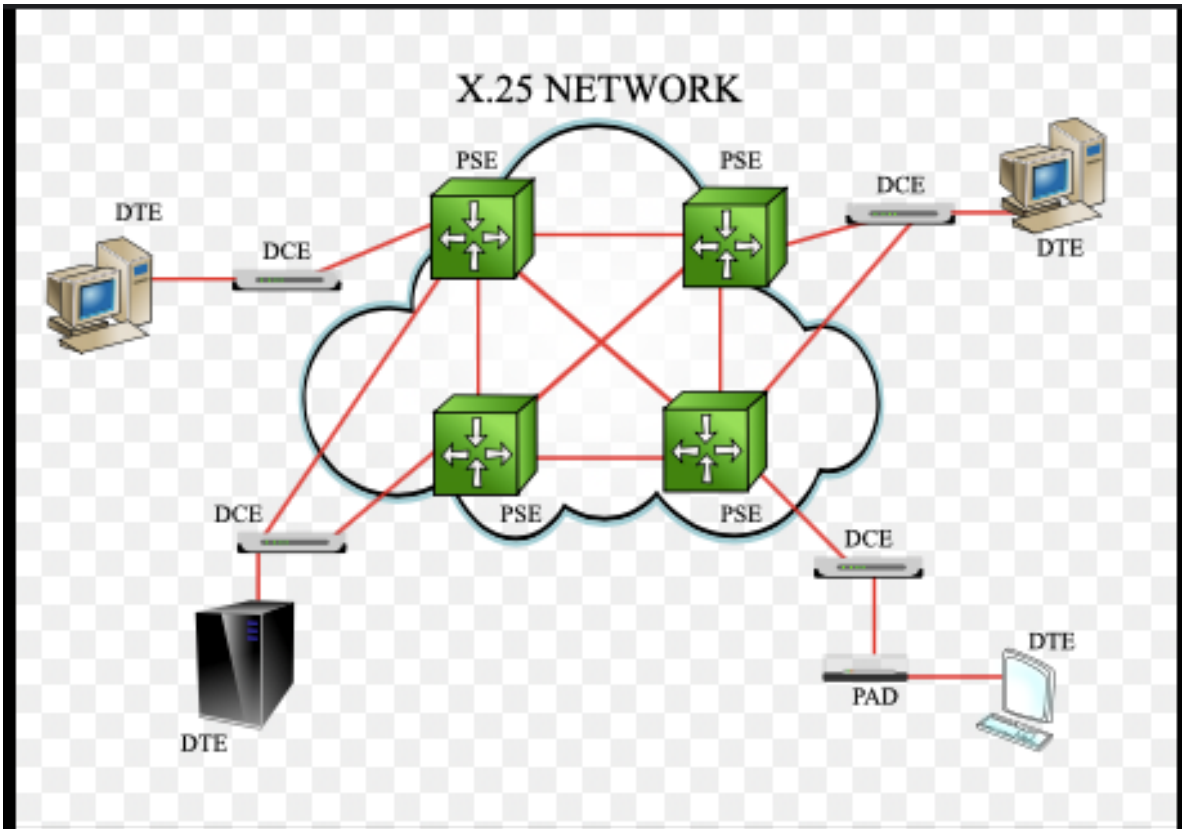
of two 6-byte fields which is used to indicate MAC address of source and destination.

- Data – Data length can vary from 0 to maximum token holding time (THT) according to token reservation strategy adopted. Token ring imposes no lower bound on size of data i.e. an advantage over Ethernet.

- Cyclic redundancy check (CRC) – 32 bit CRC which is used to check for errors in the frame, i.e., whether the frame is corrupted or not. If the frame is corrupted, then its discarded.
- End delimiter (ED) – It is used to mark the end of frame. In Ethernet, length field is used for this purpose. It also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- Frame status (FS) – It Is a 1-byte field terminating a data frame.
- 

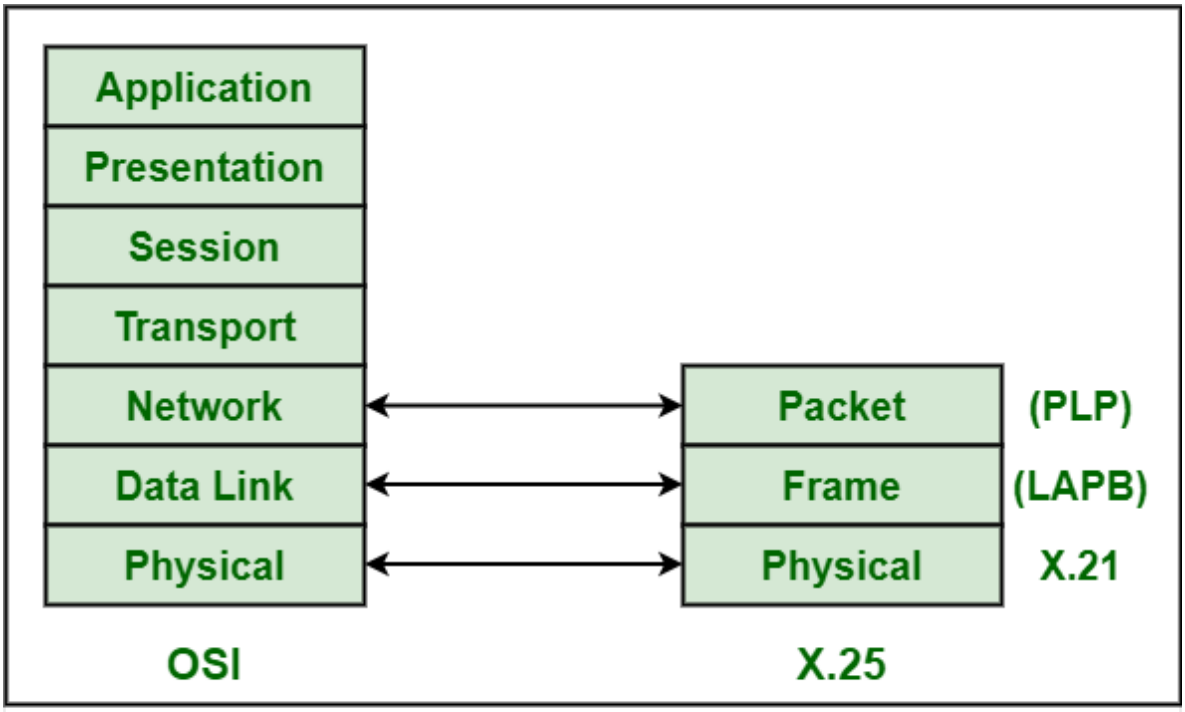
It makes use of 2 copies of AC bits are used as a error detection mechanism (100% redundancy) as CRC does not cover FS byte so that destination does not have to recalculate CRC when modifying AC bits

1) X.25 Structure



X.25 is generally a protocol that was developed by Telecommunication Standardization Sector (ITU-T) of International Telecommunication Union. It usually allows various logical channels to make use of same physical line. It basically defines a series of documents particularly issued by ITU. These documents are also known as X.25 Recommendations. X.25 also supports various conversations by multiplexing packets and also with the help of virtual communication channels. X.25 basically encompasses or suits to the lower three layers of the Open System Interconnection (OSI) reference model for networking. These three protocol layers are :

1. Physical Layer
2. Frame Layer
3. Packet Layer



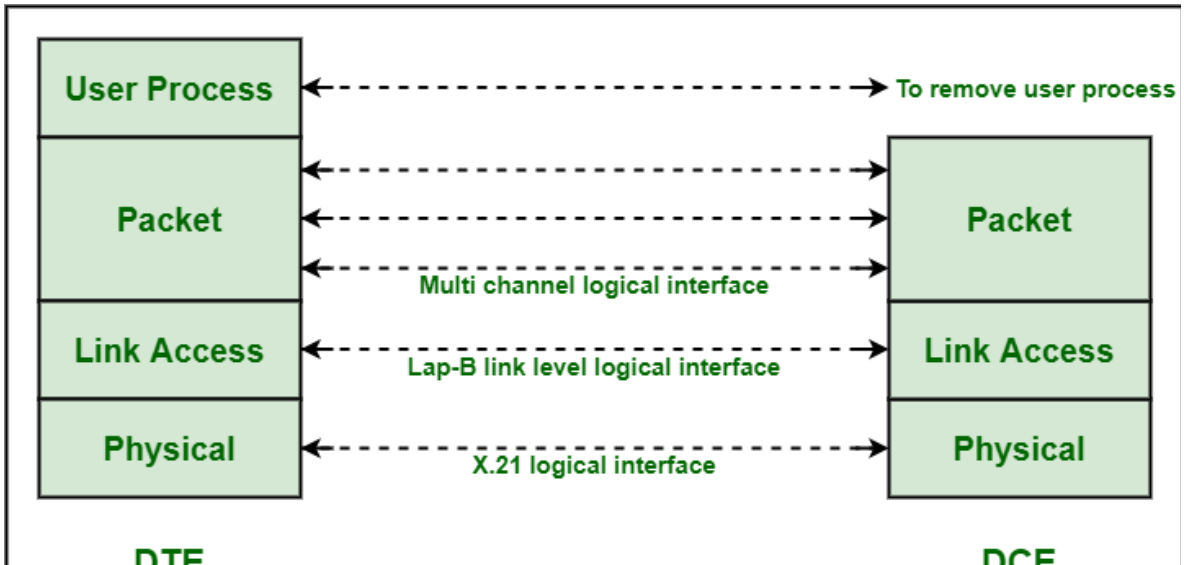
X.25 Layer Mapping with OSI Model

These are explained as following below.

1. **Physical Layer :** This layer is basically concerned with electrical or signaling. The physical layer interface of X.25 also known as X.21 bis was basically derived from RS-232 interface for serial transmission. This layer provides various communication lines that transmit or transfer some electrical signals. X.21 implementer is usually required for linking.
2. **Data Link Layer :** Data link layer is also known as Frame Layer. This layer is an implementation or development of ISO High-Level Data Link Layer (HDLC) standard which is known as LAPB (Link Access Procedure Balanced). It also provides a communication link and transmission that is error-free among any two physically connected nodes or X.25 nodes. LAPB also allows DTE (Data Terminal Equipment) or DCE (Data Circuit-Terminating Equipment) simply to start or end a communication session or start data transmission. This layer is one of the most important and essential parts of X.25 Protocol. This layer also provides a mechanism for checking in each hop during the transmission. This service also ensures a bit-oriented, error-free, and also sequenced and ordered delivery of data frames or packets. There are many protocols that can be used in frame-level as given below :

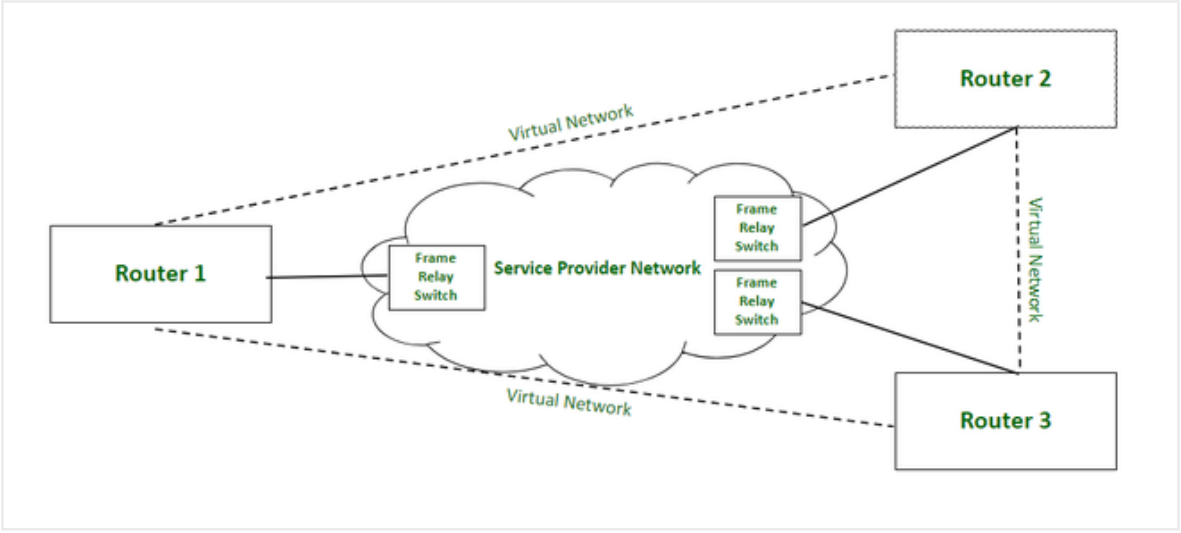
- **Link Access Procedure Balanced (LAPB) –** It is specified by ITU-T Recommendation X usually derived from HDLC. It is the most commonly used protocol that allows establishing a logical connection.
- **Link Access Protocol (LAP) –** This protocol is very rarely used. This is usually used for framing and transferring data packets across point-to-point links.
- **Link Access Procedure D-channel (LAPD) –** It is used to convey or transfer data over D-channel. It also enables and allows transmission of data among DTEs through D channel especially among a DTE and an ISDN node.
- **Logical Link Control (LLC) –** It is used to manage and ensure the integrity of transmissions of data. It also allows transmission of X.25 data packets or frames through a LAN (Local Area Network) channel.

3. **Packet Layer :** Packet layer is also known as Network Layer protocol of X.25. This layer generally governs the end-to-end communications among various DTE devices. It also defines how to address and deliver X.25 packets among end nodes and switches on a network with the help of PVCs (Permanent Virtual Circuits) or SVCs (Switched Virtual Circuits). This layer also governs and manages set-up and teardown and also flow control among DTE devices as well as various routing functions along with multiplexing multiple logical or virtual connections. This layer also defines and explains the format of data packets and also the procedures for control and transmission of data frames. This layer is also responsible for establishing a connection, transmitting data frames or packets, ending or terminating a connection, error and flow control, transmitting data packets over external virtual circuits.



2.) How does Frame Relay Work?

Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation. Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.



Frame Relay Network

Working:

Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network. It supports communication with multiple LANs over the shared physical links or private lines.

Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks. Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch. The access link is the private physical link used for communication with other LAN networks over WAN. The frame relay switch is responsible for terminating the access link and providing frame relay services.

For data transmission, LAN's router (or other border device linked

with access link) sends the data packets over the access link. The packet sent by LAN is examined by a frame relay switch to get the Data Link Connection Identifier (DLCI) which indicates the destination of the packet. Frame relay switch already has the information about addresses of the LANs connected to the network hence it identifies the destination LAN by looking at DLCI of the data packet. DLCI basically identifies the virtual circuit (i.e. logical path between nodes that doesn't really exist) between source and destination network. It configures and transmits the packet to frame relay switch of destination LAN which in turn transfers the data packet to destination LAN by sending it over its respective access link. Hence, in this way, a LAN is connected with multiple other LANs by sharing a single physical link for data transmission.
Frame relay also deals with congestion within a network. Following methods are used to identify congestion within a network:

1. **Forward Explicit Congestion Network (FECN) –**
   FECN is a part of the frame header that is used to notify the destination about the congestion in the network. Whenever a frame experiences congestion while transmission, the frame relay switch of the destination network sets the FECN bit of the packet that allows the destination to identify that packet has experienced some congestion while transmission.
2. **Backward Explicit Congestion Network (BECN) –**
   BECN is a part of the frame header that is used to notify the source about the congestion in the network. Whenever a frame experiences congestion while transmission, the destination sends a frame back to the source with a set BECN bit that allows the source to identify that packet that was transmitted had experienced some congestion while reaching out to the destination. Once, source identifies congestion in the virtual circuit, it slows down to transmission to avoid network overhead.
3. **Discard Eligibility (DE) –**
   DE is a part of the frame header that is used to indicate the priority for discarding the packets. If the source is generating a huge amount of traffic on the certain virtual network then it can set DE bits of less significant packets to indicate the high priority for discarding the packets in case of network overhead. Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion within a network.

Types:

1. **Permanent Virtual Circuit (PVC) –**
   These are the permanent connections between frame relay nodes that exist for long durations. They are always available for communication even if they are not in use. These connections are static and do not change with time.
2. **Switched Virtual Circuit (SVC) –**
   These are the temporary connections between frame relay nodes that exist for the duration for which nodes are communicating with each other and are closed/ discarded after the communication. These connections are dynamically established as per the requirements.

Advantages:

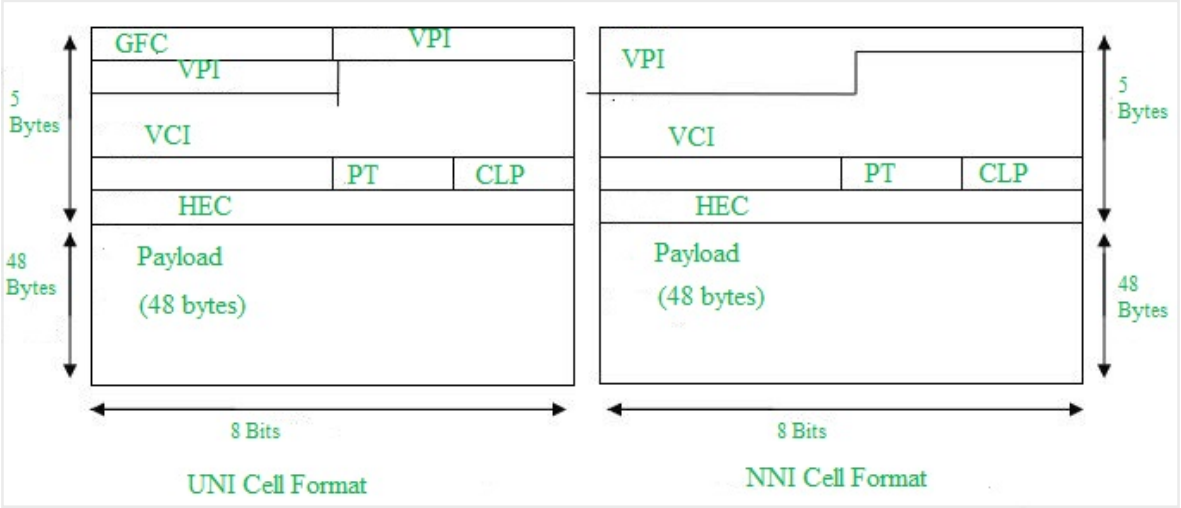
1. High speed
2. Scalable
3. Reduced network congestion
4. Cost-efficient
5. Secured connection

Disadvantages:

1. Lacks error control mechanism
2. Delay in packet transfer
3. Less reliable

Asynchronous Transfer Mode (ATM) in Computer Network

-> It usually used in multimedia transfer in televisions etc
-> It has 32 bit local header and 20bytes global NASP header
-> It established a connection before transferring the data
-> It sends packets in a sequence one by one.
-> It also have pic (permamnent virtual connection) w can use that too for data transfer.
-> Its packets are of fixed or small size
-> It packets are transferred in form of cell of total size 53 bytes
-> 4 header bytes & 48 data bytes .
-> It can transmit videos and images data
-> Cause it uses asynchronous time division multiplexing that why we called it asynchronous transfer mode.



1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).

2. Telephone networks support a single quality of service and are expensive to boot.

3. Internet supports no quality of service but is flexible and cheap.

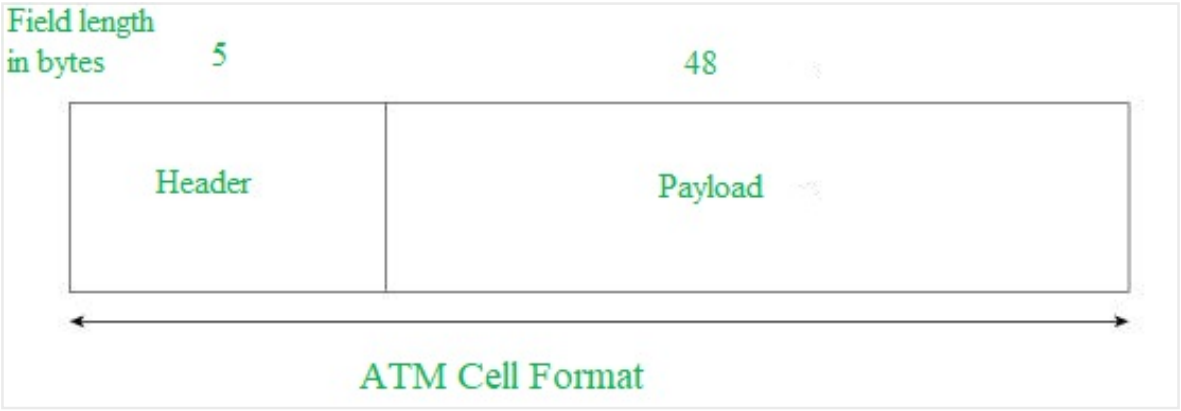
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM):
It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.
ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.
Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with **end-to-end** quality of service.
ATM is independent of a transmission medium, they may be sent on a

wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use “Packet” or “cell” Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

ATM Cell Format –

As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



Asynchronous Transfer Mode can be of two format types which are as follows:

1. **UNI Header:** This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving

the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

ATM vs DATA Networks (Internet) –

- ATM is a “virtual circuit” based: the path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.
- ATM Cells: Fixed or small size and Tradeoff is between voice or data. While IP packets are of variable size.
- Addressing: ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.