UNIT 2 INTRODUCTION TO NETWORK ARCHITECTURES

Structure **Page No.**

2.0 INTRODUCTION

In the simplest form, data transfer can take place between two devices which are directly connected by some form of communication medium. But it is not practical for two devices to be directly point to point connected, because of two reasons (i) the devices are very far apart and (ii) there is a set of devices, each of whom may require to connect to others at various times. Solution to this problem is to connect each device to a communication network. As you know computer networks means interconnected set of autonomous computers, in order to meet the needs of various applications, networks are available with different interconnection layouts and plans, methods of access, protocols and data carrying capacities. Network architecture is a complete design of a communications network. Primarily we can say that it is a framework for the specification of a network's physical components, their functional organization and configuration. Network architecture also includes the operational principles and procedures. This unit is an introduction to network architecture, in which we will discuss about different network architectures like X.25, Frame Relay, ATM. Further, it covers IPv4 and IPv6 protocol details; we will also discuss the mechanisms for implementing/deploying IPv6.

2.1 OBJECTIVES

After going though this unit, you should be able to:

- Understanding the working of various Network architectures
- differentiate between X.25, Frame Relay and ATM Architecture
- Know the functions of X.25, Frame Relay and ATM layers
- describe how X.25, Frame Relay and ATM protocols works;
- Know the need of IPv6 protocol
- Compare between the IPv4 and IPv6

2.2 X.25 ARCHITECTURE

Before discussing about X.25, we will refresh our knowledge about switching techniques. As you may know following are the basic switching techniques:
Circuit Switching: Circuit switching is used in the telephone networks to transmit voice and data signals. To enable synchronised transmission, circuit switching establishes a dedicated connection between the sender and receiver involved in the data transfer over the network. As a result, the connection consumes network

capacity whether or not there is an active transmission taking place; for example, the network capacity is used even when a caller is put on hold.

Packet Switching: In contrast to circuit switching, packet switching ensures that the network is utilised at all times. Data to be sent is broken down into chunk of bits or packets. Each packet contains data and header information for control. At each node the packet is received, stored briefly and passed on. At each node the packets may be put on a queue for further movement into the network. It does this by sending signals even in the small unused segments of the transmission — for example, between the words of a conversation or when a caller is put on hold. There are two approaches to the above kind of transport:

1. ***Datagram***, where each packet can take any path through the network as long as they all reach the destination.

2. ***Virtual Circuit***, where all the packets are routed through the same path without having the path dedicated. The path segments may carry many virtual circuits. Datagram allows for dynamic handling of congestion and no call setup is necessary. Virtual circuits allow for sequencing, error and flow control.

X.25 is an old standard protocol suite for packet based wide area network. The old networks mainly telecommunications companies and ATM's (automated teller machines) were following X.25 protocols for packet switching based network. These WAN's are having packet-switching exchanges and leased communication channels. At present X.25 protocols has been replaced by other better and less complex protocols of TCP/IP suit however, the service is still in use and functioning in some places and applications. Some student are interested to know that why it is called with such name X.25? The reason is International Telecommunication Union (ITU) publishes some series of technical books, among these technical books; there is a larger set of X-Series specifications on public data networks. The X.25 specification is only a part of that X-Series specification on public data networks.

The common perception for development of X.25 was to develop a universal standard for packet switching network. X.25 does not specify how the network operates internally; it specifies only the interface between public switched networks and the users. As shown below in the figure DTE (data terminal equipment) is a user/subscriber, DCE (data communications equipment) is a device between a network and user, in general it is MODEM device, DSE are nothing but data switching exchanges in a packet switching based WAN.

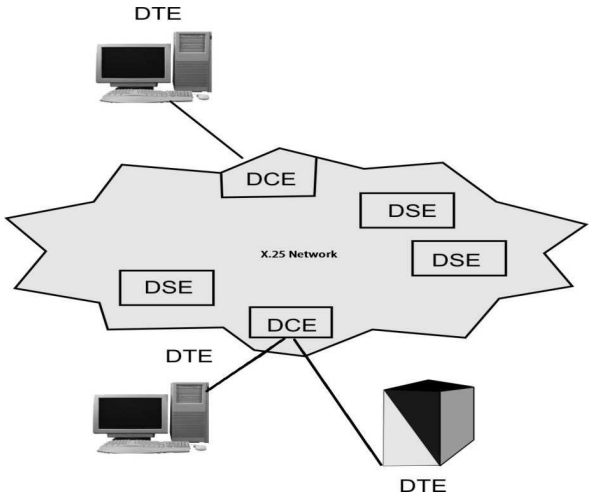

Figure 1: X.25 Network and its components

X.25 is specified on 3 layers:

1. Physical layer
2. Data link layer
3. Network layer

X.25 Network provides the means for these users (DTE) to communicate with each other. In the context of X.25 Data link and Network Layers, an X.25 DCE is the local network node to which the DTE is connected. The X.25 protocol defines the rules for the communication between the DTE and the DCE. You may again note that communication within the WAN may be entirely by some other mechanism. Following are details of each layer of X.25:

- Physical layer: Specify the physical, electrical and interface between host and network. It also specifies functional and procedural characteristics to control the physical link between a DTE and a DCE. Common implementation is X.21protocol.
- Data link layer: Deal with data transmission over an between user equipment and routers. Error control and flow control are its main responsibilities. This layer consists of the link access procedure for data interchange on the link between a DTE and a DCE.
- Network layer: this layer specify a packet-layer protocol for exchanging control and user data packets to form a packet-switching network based on virtual calls. It has main functions like Addressing, Flow control, Delivery confirmation, etc. Also, it allow to established Virtual Circuit and send packet reliably.

X.25 is connection oriented architecture and support switched virtual circuits (SVC) and permanent virtual circuits (PVC). Switched virtual circuits are established on the need basis. SVC is established when a call is made and broken down after the call is completed. On the other hand, permanent virtual circuits are almost leased kind of connections, which provide a dedicated connection between DTE's. X.25 sessions are established when one DTE device contacts another to request a communication session. The DTE device that receives the request can either accept or refuse the connection. If the request is accepted, the two systems begin full-duplex information transfer. Either DTE device can terminate the connection. After the session is terminated, any further communication requires the establishment of a new session.

2.3 FRAME RELAY

Frame Relay is a virtual-circuit based WAN that was designed to provide more efficient transmission scheme than X.25. It provides connection oriented services at reasonable speed and low cost. Interestingly in Frame relay, the packets are now of variable length (called as frame, which is a reason such architecture is named FRAME RELAY) with less overheads. Some of the main drawbacks of X.25 are as follow:

1. X.25 has a low 64 kbps data rate, [In 1990 It was very less]
2. X.25 has extensive flow Central and error central at both the data link and network layer (Because in 1970-80 available media was more prone of these errors and an objective of X.25 was to develop a global system which may have more possibility of errors). It creates large overhead and slow transmission.
3. X.25 was designed for private use, not for Internet (public use). It has its awn network layer and Internet has its awn hence packet is encapsulated in X.25 and than Internet, which increase overheads.

Frame relay overcome from the above drawbacks. It is a wide Area Network (WAN) with following features:

1. It operates a higher speed (1.5 mbps, and 44.376 mpbs)
2. Frame relay operates in only physical and data link layer. (so it can easily be used as backbone network to other protocols have network layer with less overheads)
3. Frame Relay allows bursty data. It means if at some point large amount of data is sent by someone than network should able to handle it properly.
4. Frame relay allow a Frame size of 9000 bytes, which can accommodates all LAN Frame sizes
5. It is less expensive than previous WANs, particularly with X.25.
6. It has error detection at data link layer only.
    - No Flow control, No error control, No re-transmission policy.
    - If frame is damaged, it is dropped.

Now can you answer why Frame Relay is faster than X.25? The answer is given above because it has fewer overheads of error control and flow control.

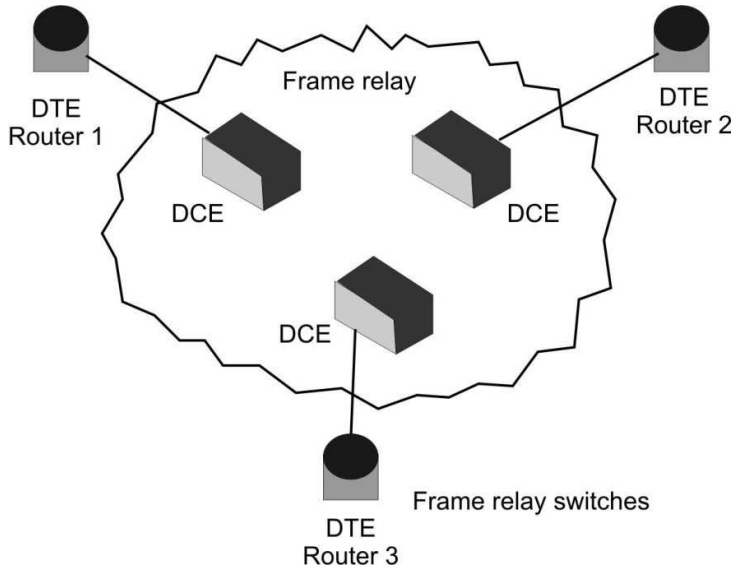

Figure 2: Network Architecture of Frame Relay

In Frame Relay each user/subscriber gets a leased line to a Frame Relay node, however the transmission paths are changed frequently and this is totally transparent to the users. Frame Relay is used for both voice and data transmission. Here, the data is packed in variable-size units called "frames" and necessary error-correction left for the end units. In Frame relay most of the services are based on permanent virtual circuit (PVC), which gives a feel good factor that they have a leased line connection at very low cost. As we discussed earlier, Frame relay operate in only physical and data link layer, so that it can easily be used as backbone-network to other protocols have network layer. Frame Relay layers are:

1. Physical Layer: The role of physical layer is similar with other architectures. However in frame relay no specific protocol is defined for physical layer to give

flexibility and better connectivity with other architectures. It supports any of the protocol recognized by ANSI. (American National Standard Institute)

2. Data Link Layer: Frame Relay uses simple protocol that does not support Flow Control, error Control, only it has error detection mechanism. However, the error correction is left for the end-user machines.

Format of Frame

Each Frame Relay Protocol data unit (PDU) consists of the following fields:

8	16	variable	16	8
Flag	**Address**	**Information …..**	**FCS**	**Flag**

Start and End Flag: Flag Field is 8 bit size, used to perform "synchronization" which indicates the beginning and end of the frame. Please refer to the unit 1 of block 1, where we have given similar example of start and end bits used for asynchronous communication. But what will happen if the flag bit pattern which we are using for end or start a communication occurs in between the flags. To avoid it we use bit stuffing and de-stuffing procedures at the source and destination respectively.

Frame Check Sequence (FCS): This is a 16 bits Field, which carries 16 bits of cyclic redundancy check (CRC) used at each switching node in the network for error detection.

Information: This field is a variable size field because user can send any data bits in this field. This is the actual data which network will pass on to receiver.

Address: This is a 16 bit or 2 bytes field having following fields inside of address:

DLCI	C/R	EA	DLCI	FECN	BECN	DE	EA
6	1	1	4	1	1	1	1

DLCI: Data link connection identifier used to identify virtual circuit in the Frame Relay.

DLCI field is of 10 bit size placed at two positions in the address field as given below:

i) The 1st DLCI is the 6 bits of first Bytes of address field

ii) The 2nd DLCI is the first 4 bits of second Bytes of address field

Command/Response (C/R): This is a 1 bit field. It is provided for upper layers to identify whether "a frame" is a command or a response. (This is not for Frame Relay)
Extended Address: This is 1 bit field, which inform the protocols about the address, such as:

- If, EA = 0 : Another address byte is to follow.(extended address can be 24 bit or 32 bit)
- If, EA = 1 : Current byte is the final address

FECN (Forward Explicit Congestion Notification): FECN bit can be set ("1") by any switch of the network to indicate that traffic is congested in the frames travelling towards the destination machine. This bit informs the destination that congestion has occurred, so destination should is ready for delay or packet loss.

BECN (Backward Explicit Congestion Notification): BECN bit also indicate congestion in a Network. BECN bit can be set ("1") by any switch of the network to indicate that traffic is congested in the frames travelling towards the source machine. This bit informs the sender machine that congestion had occurred in the network, hence slow-down the processing to prevent further delay or packet loss.

Discard Eligibility (DE): This is a 1 bit field, which indicates the priority of a frame. Sometime, switches have to discard frame (like congestion). If DE is set to "1", switch may discard the frame in problematic situation else it is very important frame and should not be discarded.

Frame Relay switching:

Here is an example of switching being done in the frame relay switch:

Table 1: Frame Relay Switching Data

Incoming		Outgoing	
Interface	DLCI	Interface	DLCI
2	78	10	37
2	121	12	147
2			

Interface 2 has received 2 pkts with DLCI values 78 and 121., Table maintained by switch show that a pkt arriving at interface 2 with DLCI = 78 should be souted to interface 10 with DLCI = 37. (Table tells the Frame Relay how to forward Frames from incoming interface to outgoing path)

Congestion Control in Frame Relay

The Frame Relay network is designed to handle busty data, whenever due to the high load and data bursts in some services, frame-relay networks provides some effective mechanisms to control the congestion. Remember, flow control is not performed in data link layer of Frame Relay so congestion avoidance mechanism as given below is used in Frame Relay:

Congestion avoidance is done through sharing information between sender/receiver nodes about backward/forward congestion notification in the network:

- Receiver can send BECN bit as a part of one of the ACK (acknowledgement). Any Frame Relay switch, send a special packet having BECN bit to the sender, so that sender may act accordingly.
- Through FECN bit, we can warn the destination that congestion has occurred, Destination can send ACK with BECN bit Set. Also, delay in sending ACK, may force the sender for deliberate delay in sending further data and consequently reduce congestion.

☞ Check Your Progress 1

1. Differentiate between virtual circuit and datagram.

……

……

……

……

2. Compare between SVC and PVC of X.25?

……

……

……

……

3. Write any four differences between X.25 and Frame Relay.

……

……

……

……

4. Explain the used of FECN and BECN in Frame Relay.

……

……

……

……

2.4 ATM NETWORK

Asynchronous Transfer Mode (ATM) is a form of data transmission that allows voice, video and data to be sent along the same network. In contrast to ATM, in the past, voice, video and data were transferred using separate networks. For example, voice was transmitted over the phone, video over cable networks and data over an internet work. ATM has its similarities with the frame relay, particularly in the term of data unit size, frame replay used a variable lengh data unit called frame. On the contrary, ATM used fixed data unit named as "cell", we can say ATM as Cell-Relay in analogy to frame relay.

ATM was emerged as a viable technology for effective transmission of voice, video and data. Some of its features are:

- ATM is a packet network like X.25, frame relay.
- ATM integrates all different types of traffic into one network.
- ATM supports multiplexing of multiple logical connections over single physical channel.
- ATM does not provide flow Control and error control at data link layer.
- ATM can serve as a LAN or WAN backbone without requiring any network replacement.
- ATM can be used in existing physical channels and networks. Because ATM was developed to have such a wide range of compatibility with existing networks, its implementation does not require replacement or over-building of telephone, data or cable networks. It is also compatible with wireless and satellite communications.

ATM Cell

As we had already discussed that ATM used a fixed size data unit called cell. As packet size is one of the key issues for protocol design, we would like to discuss the reasons for deciding the cell size. First let's assume a situation of using large packet size.

Large packets are better in a sense that they use less number of headers for data transfer. So, large packets may cause less overhead in a network. Another, important point is if a we are using a large size packet, than sometime the system has to wait till the packet is completely filled before sending any data. Remember the data sending requirement are not same at all time. Just to solve this problem, we can use variable size packet for different type of data. For example, Voice traffic can be sent in small packet and data traffic into large packet. But the variable size packet may increase additional Complexity such that variable packet size can leads to starvation problem for small packets.

The team of ATM designer had discarded the idea of both large packet and variable packets, and agreed for a fixed size data unit of 53 bytes (a 5-byte cell header and 48 bytes of data), which can achieve both higher data rate and less transmission delay. What was so special about '48 bytes'? Some people say that US telecommunication organizations wants 64 bytes Cell but the Europeans and Japanese telecommunication organizations want 32 bytes Cell. So as a compromise, 48 byte was decided.

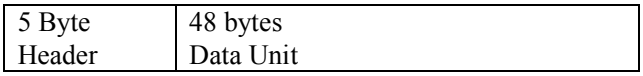

Figure 3: ATM Cell

We have various advantages of using fixed size small Cell, like it reduced queuing delay for a high priority cell. This concept simplifies the implementation of switching mechanism in hardware. The fixed cell size ensures that time-critical information such as voice or video is not adversely affected by long data frames or packets. Also, the cell header is organized for efficient switching, virtual-circuit identifiers and header error checks.

ATM cell has two formats for user to network interface and network to network interface as shown in the Figure 4:

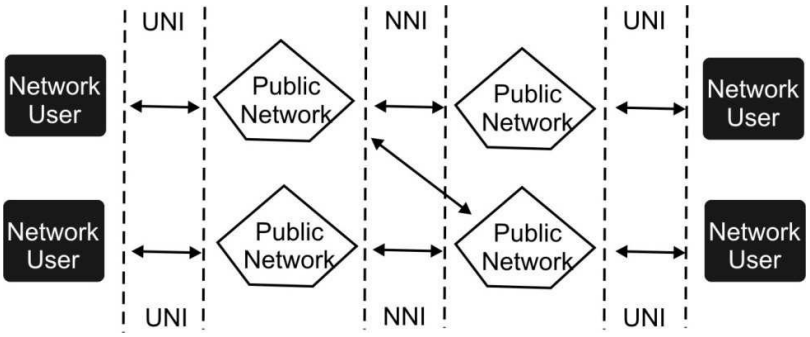

Figure 4: UNI and NNI of ATM

The Header Format

The structure of the header is different in UNI and NNI. In the network-network interface, the virtual path identifier field is expanded from 8 to 12 bits.

8	7	6	5	4	3	2	1
Generic Flow Control*				Virtual Path Identifier			
Virtual Path Identifier				Virtual Channel Identifier			
Virtual Channel Identifier							
Virtual Channel Identifier				Payload Type ID			CLP
Header Error Control							

Figure 3: User-network Interface

8	7	6	5	4	3	2	1
Virtual Path Identifier							
Virtual Path Identifier				Virtual Channel Identifier			
Virtual Channel Identifier							
Virtual Channel Identifier				Payload Type ID CLP			
Header Error Control							
INFORMATION PAYLOAD (48 Bytes)							

Figure 4: Network-network interface

Let's now look at the characteristics of each of the fields of the header format of an ATM cell.

Generic Flow Control (GFC)

The GFC field of the header is only defined across the UNI and does not appear in the NNI.

Function

- It controls the traffic flow across the UNI.

Virtual Path Identifier (VPI)

The VPI is an 8-bit field for the UNI and a 12-bit field for the NNI.

Function

- It constitutes a routing field for the network and is used to identify virtual paths. In an idle cell, the VPI is set to all 0's.
- Together with the Virtual Channel Identifier, the VPI provides a unique local identification for the transmission.

Virtual Channel Identifier (VCI)

It is a 16-bit field used to identify a virtual channel. For idle cells, the VCI is set to all 0's.

Function

- It functions as a service access point and it is used for routing to and from the end user.
- Together with the Virtual Path Identifier, the VCI provides a unique local identification for the transmission.

Payload Type Identifier (PTI)

The PTI field indicates the type of information in the information field. The value in each of the three bits of PTI indicate different conditions.

- Bit 1 is set to 1 to identify operation, administration, or maintenance cells (i.e. anything other than data cells).
- Bit 2 is set to 1 to indicate that congestion was experienced by a data cell in transmission and is only valid when bit 4 is set to 0.
- Bit 3 is used to convey information between end-users.

Cell Loss Priority (CLP)

The 1-bit CLP field is used for indication of the priority of the cell. It is used to provide guidance to the network in the event of congestion. When set to value 1, it indicates that the cell may be discarded within the network when congestion occurs. When the CLP value is set to 0, it indicates that the cell is of relatively high priority and should be discarded only in situations when no alternative is available.

Header Error Control (HEC)

Each ATM cell includes an 8-bit HEC that is calculated based on the remaining 32 bits of the header.

Function

- It detects all single-bit errors and some multiple-bit errors. As an ATM cell is received at a switch, the HEC of the cell is compared and all cells with HEC discrepancies (errors) are discarded. Cells with single-bit errors may be subject to error correction if supported or discarded. When a cell is passed through the switch and the VPI/VCI values are altered, the HEC is recalculated for the cell prior to being passed out to the port.

ATM Layers

ATM is a connection-invented protocol. ATM has a layered structure that is similar to the 7-layerd OSI model. However, ATM only addresses the functionality of the two lowest layers of the OSI model, i.e.

- The physical layer and
- The data link layer.

Apart from these two layers, all other layers of the OSI model are irrelevant in ATM, as these layers are only part of the encapsulated information portion of the cell which is not used by the ATM network. In ATM, three layers handle the functionality of the two lower OSI layers.

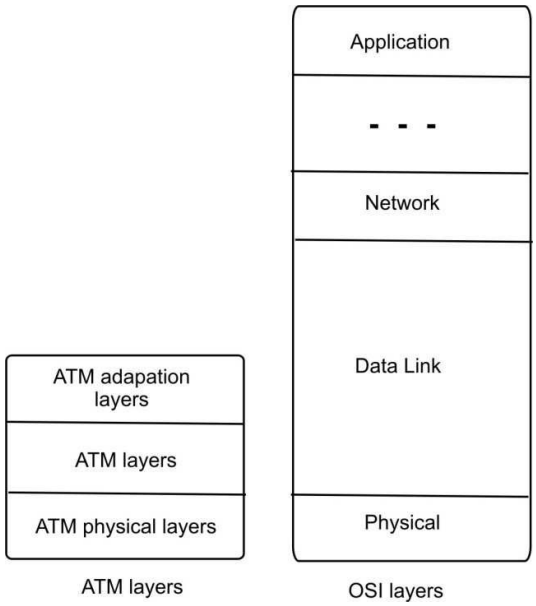

Figure 5: ATM and OSI Model

i) **Physical Layer:** The physical layer defines the specification of a transmission medium (copper, fiber optic, coaxial, HFC, wireless) and a signal encoding scheme and electrical to optical transformation. It provides convergence with physical transport protocols such as SONET as well as the mechanism for transforming the flow of cells into a flow of bits. The ATM form has left most of the specification for this level to the implementer.

ii) **The ATM Layer:** The ATM layer deals with cells and cell transport. It defines the layout of a cell and tells what the header fields mean. The size of a cell is 53 bytes (5 bytes of header and 48 bytes of payload). Because each cell is the same size and all are relatively small, delay and other problems with multiplexing different sized packets are avoided.

It also deals with establishment and release of virtual circuits. Congestion control is also located here. It resembles the network layer of the OSI model as it has got the characteristics of the network layer protocol of OSI model like Routing, Switching, End to end virtual circuit set up and Traffic management.

Switches in ATM provide both switching and multiplexing. A Cell format of ATM Layer are distinguished as,UNI (User Network Interface) and NNI (Network-Network Interface)

In both cases the cell consists of a 5 byte header followed by a 48 bytes pay-load but the two headers are slightly different.

iii) **ATM Adaptation Layer:** The ATM Adaptation Layer (AAL) maps the higher-level data into ATM cells to be transported over the ATM network, i.e. this layer segments the data and adds appropriate error control information as necessary. It is dependent on the type of services (voice, data etc.) being transported by the higher layer.

ATM is connection oriented and allows the user to specify the resources required on a per-connection basis (per SVC) dynamically. There are the five classes of service defined for ATM (as per ATM Forum UNI 4.0 specification).

ATM Service Classes

Service Class	Quality of Service Parameter
Constant bit rate (CBR)	CBR class is used for emulating circuit switching. The cell rate is constant with time. CBR applications are sensitive to cell-delay variation. Examples of applications that can use CBR are telephone traffic (i.e. nx64 kbps), video conferencing and television.
Variable bit rate–non-real time (VBR–NRT)	VBR-NRT class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR–NRT.
Variable bit rate–real time (VBR–RT)	This class is similar to VBR–NRT but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.
Available bit rate (ABR)	ABR class provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail. Although the standard does not require the cell transfer delay and cell-loss ratio to be guaranteed or minimized, it is desirable for switches to minimize delay and loss as much as possible. Depending upon the state of congestion in the network, the source is required to control its rate. The users are allowed to declare a minimum cell rate, which is guaranteed to the connection by the network.
Unspecified bit rate (UBR)	UBR class is widely used today for TCP/IP.

The ATM Forum has identified certain technical parameters to be associated with a connection.

Depending on the type of data, several types of AAL layers have been defined. However, no AAL is restricted to a specific data class or type; all types of data could conceivably be handled by any of the AALs. The various AAL protocols defined are:

1. AAL 1
2. AAL 2
3. AAL 3/4 (layer 3 and 4 were merged to avoid function overlapping)
4. AAL 5

Each layer of ATM is further divided into two sublayers

- SAR (Segmentation and Reassembly)
- CS (Convergence Sublayer).

Segmentation & Reassembly: This is the lower part of the AAL. The SAR sublayer breaks packets up into cells on the transmission side and puts them back together again at the destination. It can add headers and trailers to the data units given to it by the CS to form payloads. It is basically concerned with cells.

Convergence Sublayer: The CS sublayer makes it possible to have ATM systems offer different kind of services to different applications. The CS is responsible for accepting bit streams or arbitrary length messages from the application and breaking them into units of 44 or 48 bytes for transmission.

Working of ATM

When a user sends data over the ATM network, the higher-level data unit is passed down to the Convergence Sublayer of the AAL Layer, which prepares the data for the ATM Layer according to the designated AAL protocol. The data is then passed down to the Segmentation and Reassembly Sublayer of the AAL Layer, which divides the data unit into appropriately sized segments.

These segments are then passed down to the ATM Layer, which defines an appropriate cell header for each segment and encapsulates the header and payload segment into a 53-byte ATM cell. The cells are then passed down to the Physical Layer, which streams the cells at an appropriate pace for the transmission medium being used, adding empty cells as needed.
ATM circuit connections are of two types:

1. Virtual Paths and

2. Virtual Channels.

A virtual channel is a unidirectional pipe made up from the concatenation of a sequence of connection elements. A virtual path **consists of a set of these virtual channels.** Each virtual channel and virtual path has an identifier associated with it. Virtual path is identified by Virtual Path Identifiers (VPI) and a virtual channel is identified by a Virtual Channel Identifier (VCI). All channels within a single path must have distinct channel identifiers but may have the same channel identifier as channels in different virtual paths.

An individual channel can therefore be uniquely identified by its virtual channel and virtual path number. Cell sequence is maintained through a virtual channel connection.
ATM connections can be categorised into two types:

i) ***Point-to-point connections:*** These are the connections which connect two ATM end-systems. Such connections can be unidirectional or bidirectional.

ii) ***Point-to-multipoint connections:*** These are the connections which connects a single source end-system known as the root node) to multiple destination end-systems (known as leaves).

The basic operation of an ATM switch is very simple to understand.

1. The ATM switch receives a cell across a link on a known VCI or VPI value.

2. The ATM switch looks up the connection value in a local translation table to determine the outgoing port (or ports) of the connection and the new VPI/VCI value of the connection on that link.

3. The ATM switch then retransmits the cell on that outgoing link with the appropriate connection identifiers.

The manner in which the local translation tables are set up determine the two fundamental types of ATM connections:

- ***Permanent Virtual Connections (PVC):*** A PVC is a connection set up by some external mechanism, typically network management, in which a set of switches between an ATM source and destination ATM system are programmed with the appropriate VPI/VCI values.
- ***Switched Virtual Connections (SVC):*** An SVC is a connection that is set up automatically through a signalling protocol. SVCs do not require the manual interaction needed to set up PVCs and as such, are likely to be much more widely used.

Traffic Control

An ATM network needs efficient Traffic Control mechanisms to allocate network resources in such a way as to separate traffic flows according to the various service classes and to cope with potential errors within the network at any time.
Network Resource Management: Network Resource management deals with allocation of network resources in such a way that traffic is separated on the basis of the service characteristics. A tool of network resource management which can be used for Traffic Control is the **virtual path technique**. A virtual path connection (VPC) groups several virtual channel connections (VCC)s together such that only the collective traffic of an entire virtual path has to be handled. In this type of setup, priority control can be supported by reaggregating traffic types requiring different qualities of service through virtual paths. Messages for the operation of traffic control can be more easily distributed, a single message referring to all the virtual channels within a virtual path will do.

Connection Admission Control: Connection Admission Control is the set of actions taken by the network in protecting itself from excessive input loads. When a user requests a new virtual path connection or virtual channel connection, the user needs to specify the traffic characteristics in both directions for that connection. The network establishes such a connection only if sufficient network resources are available to establish the end-to-end connection with the required quality of service. The agreed quality of service for any of the existing channels must not be affected by the new connection.

Usage Parameter Control and Network Parameter Control: After a connection is accepted by the Connection Admission Control function, the UPC function of network monitors the connection to check whether the traffic conforms to the traffic contract.
The main purpose of UPC/NPC is to protect the network resources from an overload on one connection that would affect the quality of service of other already established connections. Usage Parameter Control (UPC) and Network Parameter Control (NPC) do the same job at different interfaces. The UPC function is performed at the UNI, while the NPC function is performed at the NNI.

Functions performed by the Usage parameter control include:

- Checking the validity of VPI/VCI values.

- Monitoring the traffic volume entering the network from all active VP and VC connections to ensure that the agreed parameters are not violated.
- Monitoring the total volume of the accepted traffic on the access link.
- Detecting violations of contracted (agreed) parameter values and taking appropriate actions.

Priority Control: Priority control is an important function as its main objective is to discard lower priority cells in order to protect the performance of higher-priority cells.

Congestion Control: Congestion is a state of network wherein the network resources are overloaded. This situation indicates that the network is not able to guarantee the negotiated quality of service to the established connections and to the new connection requests. ATM Congestion control refers to the measures taken by the network to minimize the intensity, spread and duration of network congestion.

1. As a high-bandwidth medium with low delay and the capability to be switched or routed to a specific destination, ATM provides a uniformity that meets the needs of the telephone, cable television, video and data industries. This universal compatibility makes it possible to interconnect the networks — something that is not currently possible because of the various transmission standards used by each industry.

2. One of the key advantages of ATM is its ability to transmit video without creating a jittery picture or losing the synchronisation of the sound and picture. This is possible due to proper resource allocation and admission control.

3. ATM also provides dynamic bandwidth for bursty traffic.

4. Telephone networks connect each telephone to every other telephone using a dedicated path, but carry narrow bandwidth signals. Cable networks carry broadband signals, but only connect subscribers to centralised locations. To build a network that would provide a dedicated connection between sender and receiver for broadband communications would be prohibitively expensive. For this reason, ATM seems to be the best hope since it can use existing networks to deliver simple voice and data as well as complex and time-sensitive television signals. ATM can also handle bi-directional communications easily.

5. Unlike packet switching, ATM is designed for high-performance multimedia networking.

☞ Check Your Progress 2

1. What are VPI and VCI in ATM network? Write the importance of each.

   ……

   ……

   ……

   ……

2. Explain how ATM layers are divided into sub-layers.

   ……

   ……

   ……

2.5 IPv4 AND IPv6 OVERVIEW

The primary goal of the Internet is to provide an abstract view of the complexities involved in it. Internet must appear as single network of computers. At the same time network administrators or users must be free to choose hardware or various internetworking technologies like Ethernet, Token ring etc. Different networking technologies have different physical addressing mechanisms. Therefore, identifying a computer on Internet is a challenge. To have uniform addressing for computers over the Internet, IP software defines an IP address which is a logical address. Now, when a computer wants to communicate to another computer on the Internet, it can use logical address and is not bothered with the physical address of the destination and hence the format and size of data packet.

2.5.1 Classes of IP Address

Internet addresses are 32 bits long, written as four bytes separated by periods (full stops). They can range from 0.0. 0.0 to 223. 255. 255. 255. It's worth noting that IP addresses are stored in big-endian format, with the most significant byte first, read left to right. This contrasts with the little-endian format used on Intel- based systems for storing 32- bit numbers. This minor point can cause a lot of trouble for PC programmers and others working with raw IP data if they forget.
IP addresses comprise two parts, the network ID and the host ID. An IP address can identify a network (if the host part is all zero) or an individual host. The dividing line between the network ID and the host ID is not constant. Instead, IP addresses are split into five classes, which allow for a small number of very large networks, a medium number of medium- sized networks and a large number of small networks. The classes of IP address are briefly explained below, the structure of these classes are also shown in.

IP Address Class	High Order Bit(s)	Format	Range	No. of Network Bits	No. of Host Bits	Max. Hosts	Purpose
A	0	N.H.H.H	1.0.0.0 to 126.0.0.0	7	24	2^{24}-2	Few large organisations
B	1,0	N.N.H.H	128.1.0.0 to 191.254.0.0	14	16	2^{16}-2	Medium-size organisations
C	1,1,0	N.N.N.H	192.0.1.0 to 223.255.254.0	21	8	2^{8}-2	Relatively small organisations
D	1,1,1,0	N/A	224.0.0.0 to 239.255.255.255	N/A	N/A	N/A	Multicast groups (RFC 1112)
E	1,1,1,1	N/A	240.0.0.0 to 254.255.255.255	N/A	N/A	N/A	Future Use (Experimental)

Figure 4: Classes of IPv4 address

IP follows these rules to determine the address class:

- **Class A:** If the first bit of an IP address is 0, it is the address of a class A network. The first bit of a class A address identifies the address class. The next 7 bits identify the network, and the last 24 bits identify the host. There are fewer than 128 classes a network numbers, but each class A network can be composed of millions of hosts.

- **Class B:** If the first 2 bits of the address are 1 0, it is a class B network address. The first 2 bits identify class; the next 14 bits identify the network, and the last 16 bits identify the host. There are thousands of class B network numbers and each class B network can contain thousands of hosts.
- **Class C:** If the first 3 bits of the address are 1 1 0, it is a class C network address. In a class C address, the first 3 bits are class identifiers; the next 21 bits are the network address, and the last 8 bits identify the host. There are millions of class C network numbers, but each class C network is composed of fewer than 254 hosts.
- **Class D:** If the first 4 bits of the address are 1 1 1 0, it is a multicast address. These addresses are sometimes called class D addresses, but they don't really refer to specific networks. Multicast addresses are used to address groups of computers all at one time. Multicast addresses identify a group of computers that share a common application, such as a video conference, as opposed to a group of computers that share a common network.
- **Class E:** If the first four bits of the address are 1 1 1 1, it is a special reserved address. These addresses are called class E addresses, but they don't really refer to specific networks. No numbers are currently assigned in this range.

IP addresses are usually written as four decimal numbers separated by dots (periods). Each of the four numbers is in the range 0-255 (the decimal values possible for a single byte). Because the bits that identify class are contiguous with the network bits of the address, we can lump them together and look at the address as composed of full bytes of network address and full bytes of host address. If the value of the first byte is:

- Less than 128, the address is class A; the first byte is the network number, and the next three bytes are the host address.
- From 128 to 191, the address is class B; the first two bytes identify the network, and the last two bytes identify the host.
- From 192 to 223, the address is class C; the first three bytes are the network address, and the last byte is the host number.
- From 224 to 239, the address is multicast. There is no network part. The entire address identifies a specific multicast group.
- Greater than 239, the address is reserved.

To learn further about IP address and CIDR you can see the course material of BCS-061: TCP/IP programme which you will study in your next semester.

IPv6 Overview

With the advancement in the technologies, mobile-handheld devices and emerging applications, it is quite evident that soon the IP addresses provided by IPv4 are not sufficient. In the recent future we can operate and use various smart deices (like TV, Fridges, cameras, ACs, phone, mobiles, etc). Each of such devices will require a unique IP address, which will increase the demand of IP addresses exponentially.

The number of IPv4 unique addresses is not that large in relation to the current rate of expansion of the Internet. Consequently, a new addressing system has been devised which is a part of Internet Protocol version 6 (IPv6), which uses 128-bit addresses, means total addresses will be 2^{128} . IPv4 uses 32-bit addresses, means total addresses will be 2^{32} around 4,294,967,296 unique addresses. IPv6 has almost 7.9×10^{28} times more addresses than IPv4.

It is possible that IPv6 would not be used or implemented completely in the coming couple of years. This IPv6 (Internet Protocol version 6) is a revision of the earlier

Internet Protocol (IP) version 4. As you know IPv4 address is 32 bit and divided into four octets separated by dot for example 192.186.12.10, on the other hand IPv6 addresses are consist of eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:0000:8a2e:0370:7334. IPv6 is designed to swap the existing IPv4, which is the main communications protocol for most Internet traffic as of today. IPv6 was developed to deal with the long-anticipated problem of IPv4 running out of addresses, some of the reasons and need for implementing IPv6 are following:

- The short term solutions like sub-netting, classless addressing cannot fulfill the massive future demand of address space.
- The internet must accommodate the real-time audio and video transmission with best quality of services.
- Internet protocol must provide the necessary security implementation for some applications.
- There is a need of multicasting in current IPv4, where the transmission of a packet to multiple destinations can be sent in a single send operation.
- IPv4 need a major revision in various issues like privacy, mobility, routing, QoS (quality of services), extendibility and addressing.

Address format

As we discussed before, IPv6 addresses are consist of eight groups of four hexadecimal digits separated by colons (:), for example 2001:0db8:85a3:0042:0000:8a2e:0370:7334. Lets see the bit composition of an IPv6 address, as we know each hexadecimal should be of 4 bits each, in a group we have four hexadecimal bits hence a group has 16 bits. Now we have 8 groups so 16 multiple with 8 is 128 bits. Any IPv6 address may be reduced and interpreted using the following rules:

- First thing is leading zeroes from the groups of hexadecimal digits can be removed, similar to the currency where leading zeros are nothing. For example, convert the group 0036 to 36.
- Always remember that hexadecimal digits in the groups are not case-sensitive just like the c programming; e.g., the groups 08DB and 08db are same.
- Next you may merge successive groups of one or more zeroes, using a double colon (::) to indicate the omitted groups. But, double colon may only be used once in any given address

The initial process and few implementation of IPv6 have been done, but still the transition process of replacing from IPv4 with IPv6 will continue for couple of years. We must consider that at present IPv4 is backbone of Internet, replacing it, is not an easy process. Definitely it will be done slow transition from one stage to another. Following are the approaches being used for replacing from IPv4 with IPv6:

1. Protocol Translation
2. Dual IP Stack
3. Tunneling

Protocol Translation

Like any other protocol both IPv4 and IPv6 are using their own headers. There are different kinds of IPv4 to IPv6 translators possible

- IP header translator: At the IP layer, we replaces IPv4 header by IPv6 header through trnslation. IP header translator is similar to NAT, Network Address Translator.
- TCP relay: At the TCP layer, we can transmit IPv4 TCP connection to IPv6 TCP connection, and vice versa, regardless of the application protocol used over TCP.
- Application gateway: In this technology we works in application protocol layer (such as FTP, HTTP), and uses application protocol-specific mechanism for protocol translation.

Protocol translation may interfere with an objective of end-to-end transparency in network communications. Also, the use of protocol translators cause problems with NAT and limit the use of addressing.

Dual IP stack

In dual IP stack implementation, we will use both IPv4 and IPv6 protocol stacks together at the Internet layer. Dual IP stack seems to be a fair solution for IPv6 implementation, as it avoids many complexities and overheads. Dual-stacked hosts running on a dual-stack network allow applications to migrate one at a time from IPv4 to IPv6. Applications and devices (that are not upgraded according to IPv6 stack) can coexist with upgraded IPv6 applications on the same network system.
In dual stack we will need the devices having capability of handling both IPv4 and IPv6 can use any IPv4 or IPv6, depending on the requirement. Dual stack approach will be costly and in some cases network devices may not support this mplementation.

Tunneling

In tunneling, we mean to encapsulate the packets of one protocol into the packets of another protocol. Something likes keeping one letter envelope into another envelope. Assume a situation as shown in the figure when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4 and communicate (between two IPv6 networks) without updating the inter-mediatory IPv4 network infrastructure.

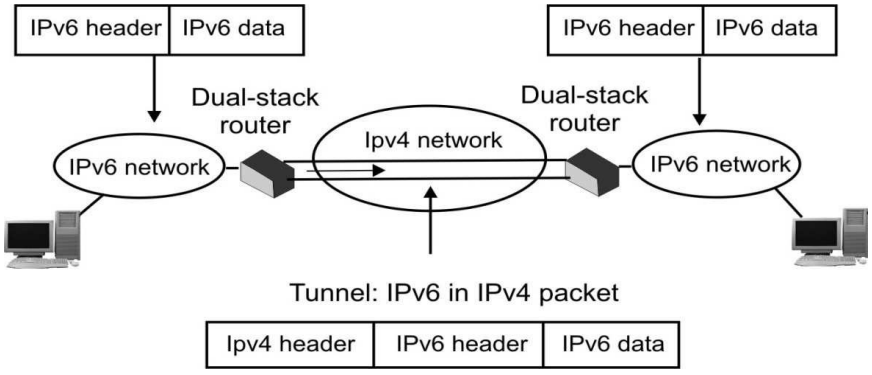

Figure 5: Tunneling Mechanism for IPv6

☞ Check Your Progress 3

1. Discuss the need of IPv6.

……

……

……

2. Explain the dual stack approach for IPv6 implementation.

……

……

……

……

1.5 SUMMARY

Network architecture is a complete design of a communications network. Primarily we can say that it is a framework for the specification of a network's physical components, their functional organization and configuration. In this unit you have learnt about X.25, Frame Relay and ATM Architectures. X.25 is an old standard protocol suite for packet based wide area network. The old networks mainly tele-communications companies and ATM's (automated teller machines) were following X.25 protocols for packet switching based network. Frame Relay is a virtual-circuit based WAN that was designed to provide more efficient transmission scheme than X.25. It provides connection oriented services at reasonable speed and low cost. Asynchronous Transfer Mode (ATM) is a form of data transmission that allows voice, video and data to be sent along the same network. In contrast to ATM, in the past, voice, video and data were transferred using separate networks. In this unit you have also studied about ISP and different address schemes of TCP/IP protocols suits. Now you know that the number of IPv4 unique addresses is not that large in relation to the current rate of expansion of the Internet. Consequently, a new addressing system has been devised which is a part of Internet Protocol version 6 (IPv6), which uses 128-bit addresses, means total addresses will be 2^{128} . In this unit you have also learnt about different approaches, which can be used for replacing from IPv4 with IPv6.

1.6 SOLUTIONS/ANSWERS

☞ Check Your Progress 1

1. Datagram allows for dynamic handling of congestion and no call setup is necessary. Virtual circuits allow for sequencing, error and flow control.

2. X.25 is connection oriented architecture and support switched virtual circuits (SVC) and permanent virtual circuits (PVC). Switched virtual circuits are established on the need basis. SVC is established when a call is made and broken down after the call is completed. On the other hand, permanent virtual circuits are almost leased kind of connections, which provide a dedicated connection between DTE's.

3. Following are the differences between X.25 and Frame Relay:

   - Frame Relay operates a higher speed
   - Frame relay operate in only physical and data link layer. (so it can easily be used as backbone network to other protocols have network layer with less overheads)
   - Frame Relay allows bursty data. It means if at some point large amount of data is sent by someone than network should able to handle it properly.
   - Frame relay allow a Frame size of 9000 bytes, which can accommodates all LAN Frame sizes.
   - It is less expensive than X.25.

- It has error detection at data link layer only.

4. FECN and BECN are used in Frame Relay mainly for congestion control

   FECN (Forward Explicit Congestion Notification): FECN bit can be set ("1") by any switch of the network to indicate that traffic is congested in the frames travelling towards the destination machine. This bit informs the destination that congestion has occurred, so destination should is ready for delay or packet loss.

   BECN (Backward Explicit Congestion Notification): BECN bit also indicate congestion in a Network. BECN bit can be set ("1") by any switch of the network to indicate that traffic is congested in the frames travelling towards the source machine. This bit informs the sender machine that congestion had occurred in the network, hence slow-down the processing to prevent further delay or packet loss.

☞ Check Your Progress 2

1. Virtual Path Identifier (VPI) is an 8-bit field for the UNI and a 12-bit field for the NNI. It constitutes a routing field for the network and is used to identify virtual paths. In an idle cell, the VPI is set to all 0's. Together with the Virtual Channel Identifier, the VPI provides a unique local identification for the transmission.

   Virtual Channel Identifier (VCI) is a 16-bit field used to identify a virtual channel. For idle cells, the VCI is set to all 0's. It functions as a service access point and it is used for routing to and from the end user. **Together with the Virtual Path Identifier, the VCI provides a unique local identification for the transmission.**

2. Each layer of ATM is further divided into two sublayers SAR (Segmentation and Reassembly) and CS (Convergence Sublayer).

   Segmentation & Reassembly: This is the lower part of the AAL. The SAR sublayer breaks packets up into cells on the transmission side and puts them back together again at the destination. It can add headers and trailers to the data units given to it by the CS to form payloads. It is basically concerned with cells.

   Convergence Sublayer: The CS sublayer makes it possible to have ATM systems offer different kind of services to different applications. The CS is responsible for accepting bit streams or arbitrary length messages from the application and breaking them into units of 44 or 48 bytes for transmission.

☞ Check Your Progress 3

1. With the advancement in the technologies, mobile-handheld devices and emerging applications, it is quite evident that soon the IP addresses provided by IPv4 are not sufficient. In the recent future we can operate and use various smart deices (like TV, Fridges, cameras, ACs, phone, mobiles, etc). Each of such devices will require a unique IP address, which will increase the demand of IP addresses exponentially.

   The number of IPv4 unique addresses is not that large in relation to the current rate of expansion of the Internet. Consequently, a new addressing system has been devised which is a part of Internet Protocol version 6 (IPv6), which uses 128-bit addresses, means total addresses will be 2^{128} . IPv4 uses 32-bit

addresses, means total addresses will be 2^{32} around 4,294,967,296 unique addresses. IPv6 has almost $7.9x10^{28}$ times more addresses than IPv4.

2. In dual IP stack implementation, we will use both IPv4 and IPv6 protocol stacks together at the Internet layer. Dual IP stack seems to be a fair solution for IPv6 implementation, as it avoids many complexities and overheads. Dual-stacked hosts running on a dual-stack network allow applications to migrate one at a time from IPv4 to IPv6. Applications and devices (that are not upgraded according to IPv6 stack) can coexist with upgraded IPv6 applications on the same network system.

   In dual stack we will need the devices having capability of handling both IPv4 and IPv6 can use any IPv4 or IPv6, depending on the requirement. Dual stack approach will be costly and in some cases network devices may not support this implementation.