SRI VENKATESHWARAA COLLEGE OF ENGINEERING & TECHNOLOGY
(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry.)
13-A, Villupuram – Pondy Main road, Ariyur, Puducherry – 605 102.
Phone: 0413-2644426, Fax: 2644424 / Website: www.svcetpondy.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(JUNE 2014-NOV 2014)

NETWORK PROTOCOL

VII SEMESTER

SYLLABUS

CS E77 NETWORK PROTOCOL

UNIT I

Network Architectures: Introduction – OSI Model – TCP/IP Model – ATM Model.

Application Layer Protocols: BOOTP – DHCP – DHCP – DNS – FTP – HTTP – SMTP – NNTP – Telnet – RMON – SNMP.

UNIT II

Presentation Layer Protocol: LPP.

Session Layer protocols: RPC, SDP, SIP.

Transport Layer protocols: TCP, UDP, RDP, and RUDP.

UNIT III

Network Layer Protocols: IP, IPv6, ICMP, ICMPv6, MobileIP, OSPF, RIP, Multicasting protocols – BGMP, DVMRP, IGMP, and MPLS protocols.

UNIT IV

Data Link Layer Protocols: ARP, IPCP, RARP, SLIP, IEEE 802.3, IEEE 802.5, IEEE 802.11, FDDI, ISDN, xDSL, PPP, LCP, HDLC, PNNI – LANE – SONET/SDH Protocols..

UNIT V

Network Security Protocols: SSH, RADIUS, SSL, Kerberos, TLS, IPSec, Voice over IP.

TEXT BOOKS

1. A. Leon-Garcia and Indra Widjaja, “Communication Networks”, Tata McGraw-Hill, 2000.
2. Willian Stallings, “Data and Computer Communications”, Prentice-Hall of India, Seventh edition, 2005.
3. Andrew S. Tanenbaum, “Computer Networks”, Prentice-Hall of India, Fourth edition, 2003.
4. W. Richard Stevens, “TCP/IP Illustrated Vol. I: The Protocols”, Pearson Education, Asia, 2000.
5. Douglas Comer, “Intenetworking with TCP/IP Vol. I: Principles, Protocols and Architecture, Prentice Hall, Fourth edition, 2000.

REFERENCES

1. Behrouz A. Forouzan, "TCP/IP Protocol Suite", Tata McGraw-Hill, Second edition, 2004.
2. Charles M. Kozierok, "The TCP/IP Guide: A Comprehensice, Illustratead Internet Protocols Reference", No Starch Press, 2005.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Subject: NETWORK PROTOCOL **Subject Code: CS E77**

Verified by: **Approved by:**

UNIT I

Network Architectures: Introduction – OSI Model – TCP/IP Model – ATM Model.

Application Layer Protocols: BOOTP – DHCP – DHCP – DNS – FTP – HTTP – SMTP – NNTP – Telnet – RMON – SNMP.

---

2 Marks

1. What is Networks?

A network is a set of devices connected by communication links. A device can be a computer, printer, or any other device capable of sending and/or receiving data.

2. What is the need for networking?

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet. The following are the important benefits of a computer network.

File sharing: Networking of computers helps the users to share data files.

Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc.

Application sharing: Applications can be shared over the network, and this allows to implement client/server applications

User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

3. Where we can use networks?

1.Data Security and Management

2.Performance Enhancement and Balancing

3. Hardware Sharing

4.Data Sharing

5.Connectivity and communiction

4. What is meant by protocols?

A uniform set of rules that enable two devices to connect and transmit data to one another. Protocols determine how data are transmitted between computing devices and over networks. They define issues such as error control and data compression methods. The protocol determines the following: type of error checking to be used, data compression method (if any), how the sending device will indicate that it has finished a message and how the receiving device will indicate that it has received the message.

5. Name some Internet protocols?

The most common Internet protocols are TCP/IP (Transfer Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

6. What is meant by OSI?

Open Systems Interconnection (OSI) network architecture, developed by International Organization for Standardization, is an open standard for communication in the network across different equipment and applications by different vendors. Though not widely deployed, the OSI 7 layer model is considered the primary network architectural model for inter-computing and inter-networking communications

7. Describe the characteristics of OSI layer?

The OSI 7 layers model has clear characteristics at each layer. Basically, layers 7 through 4 deals with end to end communications between data source and destinations, while layers 3 to 1 deal with communications between network devices. On the other hand, the seven layers of the OSI model can be divided into two groups:

1. Upper layers (layers 7, 6 & 5) and
2. Lower layers (layers 4, 3, 2, 1).

The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software.

The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

8. What is the purpose of OSI Model? (NOV 2013)

The purpose of the OSI reference model is to make networks more manageable and to aid the problem of moving data between computers. The main objectives of the ISO OSI reference model were

a. allow manufactures of different systems to interconnect their equipment through standard interfaces.
b. Allow software and hardware to integration well and be portable on differing systems.
c. Create a model which all the countries of the world use.

9. What is meant by PDU?

In an OSI layer the packages of data passed between layers are called **PDUs** (**Protocol Data Units**). These PDUs have specific names when referring the four lower layers:

Layer	PDU Name

Transport	Segments
Network	Packets
Data Link	Frames
Physical	Bits

10. How the OSI Layers are grouped?

The layers of the OSI model can be grouped into two layers The **Media layers**, consisting of the physical layer and the data link layer, and the **Host layers**, consisting of the application, presentation, session and transport layers. The Media layers so called because it controls delivery of data over the network, and the Host layers so called because they provide for accurate delivery of data between computers, or hosts, on the network.

11. Define Application Layer?

- Defines interface to user processes for communication and data transfer in network
- Provides standardized services such as virtual terminal, file and job transfer and operations

12. Define Presentation Layer?

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; encrypts and decrypts data; compresses and decompresses data

13. Define Session Layer?

- Manages user sessions and dialogues
- Controls establishment and termination of logic links between users
- Reports upper layer errors

14. Define Transport Layer?

- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms• Provides connectionless oriented packet delivery

15. Define Network Layer?

- Determines how data are transferred between network devices

- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion

16. Define Data Link Layer?

- Defines procedures for operating the communication links
- Frames packets
- Detects and corrects packets transmit errors

17. Define Physical Layer

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics

18. List the Various Function of Data Link Layer? (April 13)

1. Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

2. Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

3. Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

4. Error control: Error control is normally achieved through a trailer added to the end of the frame.

5. Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

19. What is meant by TCP/IP Model?

The **Transmission Control Protocol** (**TCP**) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.

20. Name the TCP/IP 4-layer model?

- Application Layer
- Transport Layer
- Network Access Layer
- Network Layer

21. What is the purpose we can use TCP/IP Model?

1) Multi-Vendor Support.
2) Interoperability.
3) Logical Addressing.
4) Rout ability.
5) Name Resolution
6) Error Control and Flow Control
7) Multiplexing/De-multiplexing.

22. Define (ATM) protocol architecture

The **Asynchronous Transfer Mode (ATM)** protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.

23. Define ATM adaptation layer

The basic function of the ATM adaptation layer is to convert the user data supplied by higher layers into 48-byte blocks of data. The ATM adaptation layer is divided into two sub-layers –

- the convergence sub-layer, and
- the segmentation and re-assembly sub-layer.

The convergence sub-layer provides services to higher layers through a set of protocols, but I do not need to describe these here.

The segmentation and re-assembly sub-layer separates the messages from the convergence sub-layer into ATM cells.

24. Define BOOTP: Bootstrap Protocol?

The Bootstrap Protocol (BOOTP) is a UDP/IP-based protocol which allows a booting host to configure itself dynamically and without user supervision.

BOOTP provides a means to notify a host of its assigned IP address, the IP address of a boot server host and the name of a file to be loaded into memory and executed. Other configuration information such as the local subnet mask, the local time offset, the addresses of default routers and the addresses of various Internet servers, can also be communicated to a host using BOOTP.

BOOTP uses two different well-known port numbers. UDP port number 67 is used for the server and UDP port number 68 is used for the BOOTP client.

25. Define DHCP?(April 2013)(NOV 2013)

Dynamic Host Configuration Protocol (DHCP) is a communications protocol enabling network administrators manage centrally and to automate the assignment of IP addresses in a network. In an IP network, each device connecting to the Internet needs a unique IP address. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

26. Define Data Link Switching Client Access Protocol?

The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol used between workstations and routers to transport SNA/NetBIOS traffic over TCP sessions.

27. Define DNS?

Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

28. Define FTP?

File Transfer Protocol (FTP) enables file sharing between hosts. FTP uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfers. The control connection uses an image of the TELNET protocol to exchange commands and messages between hosts.

29. Define HTTP?

The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a connection with a server. The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

30. Define SMTP?

Simple Mail Transfer Protocol (SMTP) is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and provides notification regarding incoming mail.

31. Define Network News Transfer Protocol?

Network News Transfer Protocol (NNTP) specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream (such as TCP port 119) server-client model. NNTP is designed so that news articles need only be stored on one (presumably central) server host, and subscribers on other hosts attached to the network may read news articles using stream connections to the news host. The Network News Transfer Protocol (NNTP) established the technical foundation for the widely used Newsgroups.

NNTP is modeled after the USENET news system. However, NNTP makes few demands upon the structure, content or storage of news articles and thus it can easily be adapted to other non-USENET news systems. Using NNTP, hosts exchanging news articles have an interactive mechanism for deciding which articles are to be transmitted.

32. Define Terminal emulation protocol of TCP/IP?

TELNET is the terminal emulation protocol in a TCP/IP environment.TELNET uses the TCP as the transport protocol to establish connection between server and client. After connecting, TELNET server and client enter a phase of option negotiation that determines the options that each side can support for the connection. Each connected system can negotiate new options or renegotiate old options at any time. In general, each end of the TELNET connection attempts to implement all options that maximize performance for the systems involved.

33. Define RMON?

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

34. Define Simple Network Management Protocol?

SNMP, an application layer protocol, is the standard protocol developed to manage nodes (servers, workstations, routers, switches and hubs, etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

11 Marks

1. Explain in detail about Network Architectures (11 marks)

A network architecture is a blueprint of the complete computer communication network, which provides a framework and technology foundation for designing, building and managing a communication network. It typically has a layered structure.

Layering is a modern network design principle which divides the communication tasks into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts in a small number of well-defined ways. Layering allows the parts of a communication to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple.

If network architecture is open, no single vendor owns the technology and controls its definition and development. Anyone is free to design hardware and software based on the network architecture. The TCP/IP network architecture, which the Internet is based on, is such a open network architecture and it is adopted as a worldwide network standard and widely deployed in local area network (LAN), wide area network (WAN), small and large enterprises, and last but not the least, the Internet.

Open Systems Interconnection (OSI) network architecture, developed by International Organization for Standardization, is an open standard for communication in the network across different equipment and applications by different vendors. Though not widely deployed, the OSI 7 layer model is considered the primary network architectural model for inter-computing and inter-networking communications.

In addition to the OSI network architecture model, there exist other network architecture models by many vendors, such as IBM SNA (Systems Network Architecture), Digital Equipment Corporation (DEC; now part of HP) DNA (Digital Network Architecture), Apple computer's AppleTalk, and Novell's NetWare. Actually, the TCP/IP architecture does not exactly match the OSI model. Unfortunately, there is no universal agreement regarding how to describe TCP/IP with a layered model. It is generally agreed that TCP/IP has fewer levels (from three to five layers) than the seven layers of the OSI model.

Network architecture provides only a conceptual framework for communications between computers. The model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols.

2. Explain in detail about OSI Network Architecture (11 marks)

Open Systems Interconnection (OSI) model is a reference model developed by ISO (International Organization for Standardization) in 1984, as a conceptual framework of standards for communication

in the network across different equipment and applications by different vendors. It is now considered the primary architectural model for inter-computing and internetworking communications. Most of the network communication protocols used today have a structure based on the OSI model. The OSI model defines the communications process into 7 layers, dividing the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The OSI 7 layers model has clear characteristics at each layer. Basically, layers 7 through 4 deals with end to end communications between data source and destinations, while layers 3 to 1 deal with communications between network devices. On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

The specific description for each layer is as follows:

Layer 7: Application Layer

- Defines interface to user processes for communication and data transfer in network
- Provides standardized services such as virtual terminal, file and job transfer and operations

Layer 6: Presentation Layer

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; encrypts and decrypts data; compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logic links between users
- Reports upper layer errors

Layer 4: Transport Layer

- Manages end-to-end message delivery in network

• Provides reliable and sequential packet delivery through error recovery and flow control mechanisms

• Provides connectionless oriented packet delivery

Layer 3: Network Layer

• Determines how data are transferred between network devices

• Routes packets according to unique network device addresses

• Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer

• Defines procedures for operating the communication links

• Frames packets

• Detects and corrects packets transmit errors

Layer 1: Physical Layer

• Defines physical means of sending data over network devices

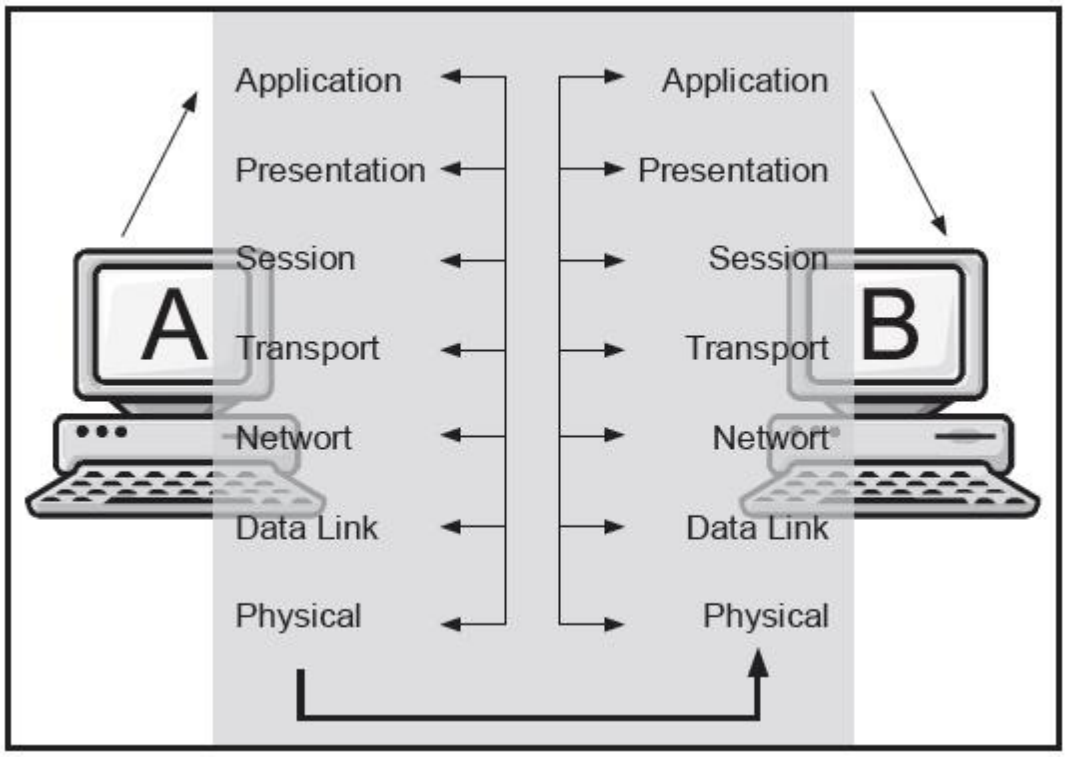
• Interfaces between network medium and devices

• Defines optical, electrical and mechanical characteristics

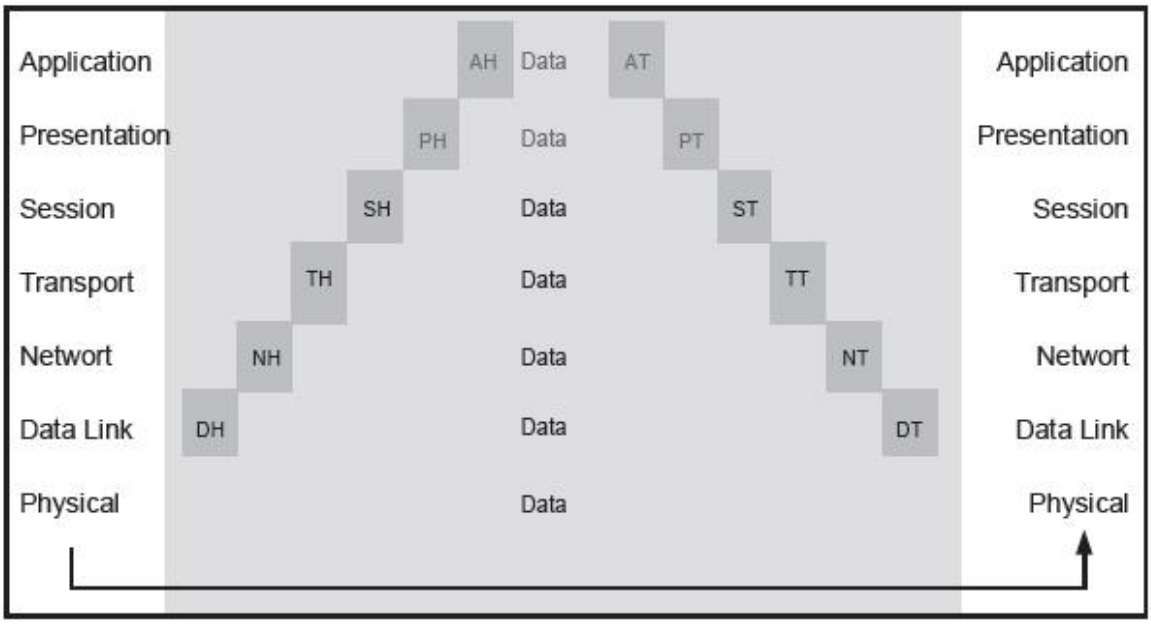
Information being transferred from a software application in one computer to an application in another proceeds through the OSI layers. For example, if a software application in computer A has information to pass to a software application in computer B, the application program in computer A need to pass the information to the application layer (Layer 7) of computer A, which then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on all the way down to the physical layer (Layer 1). At the physical layer, the data is placed on the physical network medium and is sent across the medium to computer B. The physical layer of computer B receives the data from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which relays it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of computer B. Finally, the application layer of computer B passes the information to the recipient application program to complete the communication process.

The following diagram illustrated this process.

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer OSI layers. Headers and Trailers of data at each layer are the two basic forms to carry the control information.



Headers are prep ended000000 to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers. An OSI layer is not required to attach a header or a trailer to data from upper layers. Each layer may add a Header and a Trailer to its Data, which consists of the upper layer's Header, Trailer and Data as it proceeds through the layers. The Headers contain information that specifically addresses layer-to-layer communication. Headers, trailers and data are relative concepts, depending on the layer that analyzes the information unit. For example, the Transport Header (TH) contains information that only the Transport layer sees. All other layers below the Transport layer pass the Transport Header as part of their Data. At the network layer, an information unit consists of a Layer 3 header (NH) and data.

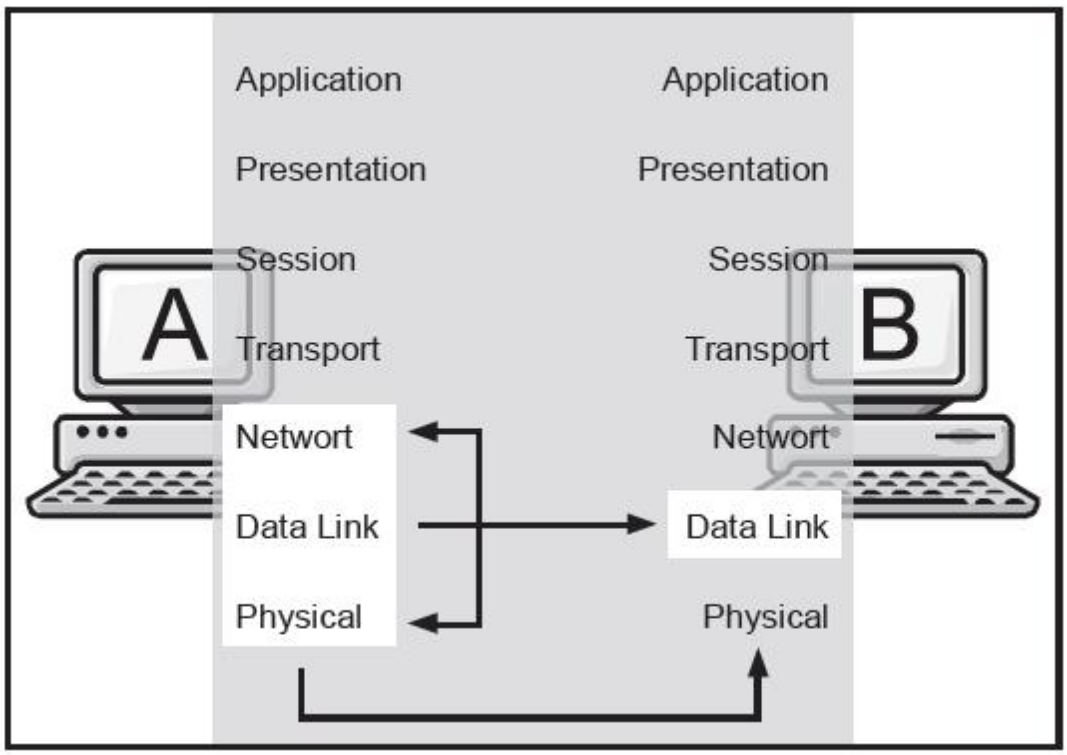


At the data link layer, however, all the information passed down by the network layer (the Layer 3 header and the data) is treated as data. In other words, the data portion of an information unit at a given OSI layer potentially can contain headers, trailers, and data from all the higher layers. This is known as encapsulation.

For example, if computer A has data from software application to send to computer B, the data is passed to the application layer. The application layer in computer A then communicates any control information required by the application layer in computer B by prepending a header to the data. The resulting message unit, which includes a header, the data and maybe a trailer, is passed to the presentation layer, which prepends its own header containing control information intended for the presentation layer in computer B. The message unit grows in size as each layer prepends its own header and trailer containing control information to be used by its peer layer in computer B. At the physical layer, the entire information unit is transmitted through the network medium.

The physical layer in computer B receives the information unit and passes it to the data link layer. The data link layer in computer B then reads the control information contained in the header prepended by the data link layer in computer A. The header and the trailer are then removed, and the remainder of the information unit is passed to the network layer. Each layer performs the same actions: The layer reads the header and trailer from its peer layer, strips it off, and passes the remaining information unit to the next higher layer. After the application layer performs these actions, the data is passed to the recipient software application in computer B, in exactly the form in which it was transmitted by the application in computer A.

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems. A given layer in the OSI model generally communicates with three other OSI layers: the layer directly above it, the layer directly below it and its peer layer in other networked computer systems. The data link layer in computer A, for example, communicates with the network layer of computer A, the physical layer of computer A and the data link layer in computer B. The following chart illustrates this example.



3. Discuss in detailed about OSI ISO layered function in details? (APRIL 2013)

Group	#	Layer Name	Key Responsibilities	Data Type Handled	Scope	Common Protocols and Technologies
Lower Layer	**1**	**Physical**	Encoding and Signaling; Physical Data Transmission; Hardware Specifications; Topology and Design	Bits	Electrical or light signals sent between local devices	(Physical layers of most of the technologies listed for the data link layer)
	2	**Data Link**	Logical Link Control; Media Access Control; Data Framing; Addressing; Error Detection and Handling; Defining Requirements of Physical Layer	Frames	Low-level data messages between local devices	IEEE 802.2 LLC, Ethernet Family; Token Ring; FDDI and CDDI; IEEE 802.11 (WLAN, Wi-Fi); HomePNA; HomeRF; ATM; SLIP and PPP
	3	**Network**	Logical Addressing; Routing; Datagram Encapsulation; Fragmentation and Reassembly; Error Handling and Diagnostics	Datagrams / Packets	Messages between local or remote devices	IP; IPv6; IP NAT; IPsec; Mobile IP; ICMP; IPX; DLC; PLP; Routing protocols such as RIP and BGP
	4	**Transport**	Process-Level Addressing; Multiplexing/Demultiplexing; Connections; Segmentation and Reassembly; Acknowledgments and Retransmissions;	Datagrams / Segments	Communication between software processes	TCP and UDP; SPX; NetBEUI/NBF

			Flow Control			
Upper Layer	**5**	**Session**	Session Establishment, Management and Termination	Sessions	Sessions between local or remote devices	NetBIOS, Sockets, Named Pipes, RPC
	6	**Presentation**	Data Translation; Compression and Encryption	Encoded User Data	Application data representations	SSL; Shells and Redirectors; MIME
	7	**Application**	User Application Services	User Data	Application data	DNS; NFS; BOOTP; DHCP; SNMP; RMON; FTP; TFTP; SMTP; POP3; IMAP; NNTP; HTTP; Telnet

5. Explain in detail about TCP/IP Four Layers Architecture Model (11 marks)(NOV 2013)

TCP/IP architecture does not exactly follow the OSI model. Unfortunately, there is no universal agreement regarding how to describe TCP/IP with a layered model. It is generally agreed that TCP/IP has fewer levels (from three to five layers) than the seven layers of the OSI model. We adopt a four layers model for the TCP/IP architecture.

TCP/IP architecture omits some features found under the OSI model, combines the features of some adjacent OSI layers and splits other layers apart. The 4-layer structure of TCP/IP is built as information is passed down from applications to the physical network layer. When data is sent, each layer treats all of the information it receives from the upper layer as data, adds control information (header) to the front of that data and then pass it to the lower layer. When data is received, the opposite procedure takes place as each layer processes and removes its header before passing the data to the upper layer.

The TCP/IP 4-layer model and the key functions of each layer is described below:

Application Layer

The Application Layer in TCP/IP groups the functions of OSI Application, Presentation Layer and Session Layer. Therefore any process above the transport layer is called an Application in the TCP/IP architecture. In TCP/IP socket and port are used to describe the path over which applications communicate. Most application level protocols are associated with one or more port number.

Transport Layer

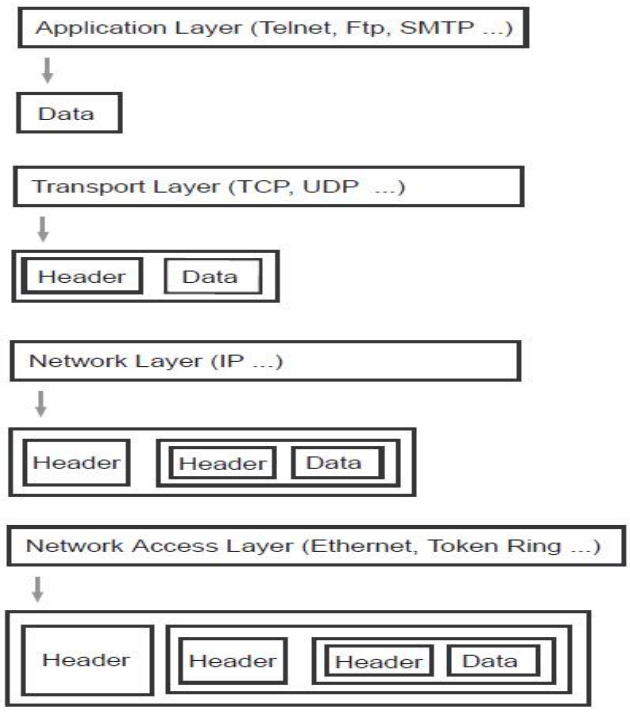
In TCP/IP architecture, there are two Transport Layer protocols. The Transmission Control Protocol (TCP) guarantees information transmission. The User Datagram Protocol (UDP) transports datagram without end-to-end reliability checking. Both protocols are useful for different applications.

Network Layer

The Internet Protocol (IP) is the primary protocol in the TCP/IP Network Layer. All upper and lower layer communications must travel through IP as they are passed through the TCP/IP protocol stack. In addition, there are many supporting protocols in the Network Layer, such as ICMP, to facilitate and manage the routing process.

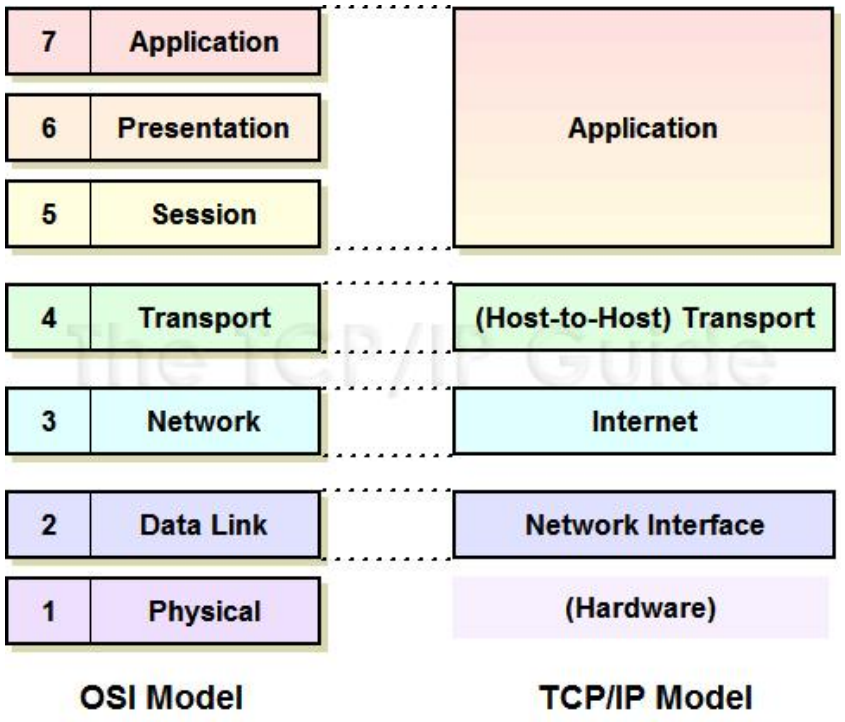
Network Access Layer

In the TCP/IP architecture, the Data Link Layer and Physical Layer are normally grouped together to become the Network Access layer. TCP/IP makes use of existing Data Link and Physical Layer standards rather than defining its own. Many RFCs describe how IP utilizes and interfaces with the existing data link protocols such as Ethernet, Token Ring, FDDI, HSSI, and ATM. The physical layer, which defines the hardware communication properties, is not often directly interfaced with the TCP/IP protocols in the network layer and above.



6.What is the difference between OSI layer and TCP/IP Protocol layer?

OSI network model, TCP/IP also has a network model. TCP/IP was on the path of development when the OSI standard was published and there was interaction between the designers of OSI and TCP/IP standards. The TCP/IP model is not same as OSI model. OSI is a seven-layered standard, but TCP/IP is a four layered standard. The OSI model has been very influential in the growth and development of TCP/IP standard, and that is why much OSI terminology is applied to TCP/IP. The following figure compares the TCP/IP and OSI network models.



As we can see from the above figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functions of Data link Layer and Physical Layer.

Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Interface Layer

This layer represents the place where the actual TCP/IP protocols running at higher layers interface to the local network. This layer is somewhat “controversial” in that some people don't even consider it a “legitimate” part of TCP/IP. This is usually because none of the core IP protocols run at this layer. Despite this, the network interface layer is part of the architecture. It is equivalent to the data link layer (layer two) in the OSI Reference Model and is also sometimes called **the link layer**.

On many TCP/IP networks, there is no TCP/IP protocol running at all on this layer, because it is simply not needed. For example, if you run TCP/IP over an Ethernet, then Ethernet handles layer two (and layer one) functions. However, the TCP/IP standards do define protocols for TCP/IP networks that do not have their own layer two implementation. These protocols, the Serial Line Internet Protocol (SLIP) and the Point-to-Point Protocol (PPP), serve to fill the gap between the network layer and the

physical layer. They are commonly used to facilitate TCP/IP over direct serial line connections (such as dial-up telephone networking) and other technologies that operate directly at the physical layer.

7. Explain some features of TCP/IP Model?

1) Multi-Vendor Support: TCP/IP is implemented by many hardware and software vendors. It is an industry standard and not limited to any specific vendor.

2) Interoperability: Today we can work in a heterogeneous network because of TCP/IP. A user who is sitting on a Windows box can download files from a Linux machine, because both Operating Systems support TCP/IP. TCP/IP eliminates the cross-platform boundaries.

3) Logical Addressing: Every network adapter has a globally unique and permanent physical address, which is known as MAC address (or hardware address). The physical address is burnt into the card while manufacturing. Low-lying hardware-conscious protocols on a LAN deliver data packets using the adapter's physical address. The network adapter of each computer listens to every transmission on the local network to determine whether a message is addressed to its own physical address.

4) Rout ability: A router is a network infrastructure device which can read logical addressing information and direct data across the network to its destination.TCP/IP is a routable protocol, which means the TCP/IP data packets can be moved from one network segment to another.

5) Name Resolution: IP addresses are designed for the computers and it is difficult for humans to remember many IP addresses. TCP/IP allows us to use human-friendly names, which are very easy to remember (Ex. www.google.com). Name Resolutions servers (DNS Servers) are used to resolve a human readable name (also known as Fully Qualified Domain Names (FQDN)) to an IP address and vice versa.

6) Error Control and Flow Control: The TCP/IP protocol has features that ensure the reliable delivery of data from source computer to the destination computer. TCP (Transmission Control Protocol) defines many of these error-checking, flow-control, and acknowledgement functions.

7) Multiplexing/De-multiplexing: Multiplexing means accepting data from different applications and directing that data to different applications listening on different receiving computers. On the receiving side the data need to be directed to the correct application, for that data was meant for. This is called De-multiplexing. We can run many network applications on the same computer. By using logical channels called ports, TCP/IP provides means for delivering packets to the correct application. In TCP/IP, ports are identified by using TCP or UDP port numbers.

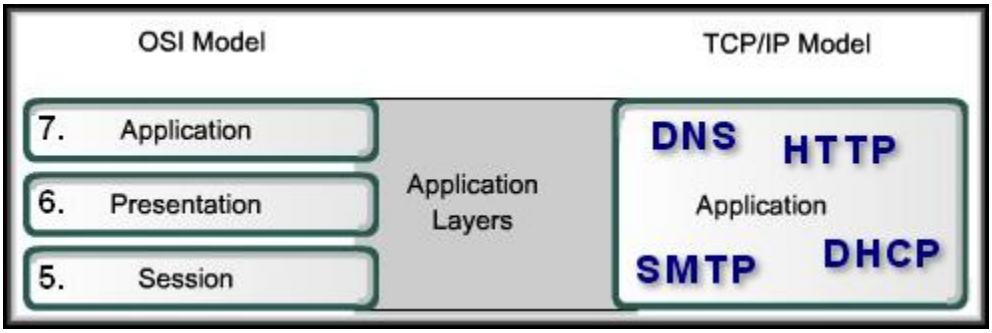
8. Explain various application layer protocols and its functions? (APRIL 2013)

Application Layer can be used in Both OSI and TCP /IP reference models. In an OSI Model the application layer can be used for to defines interface to user processes for communication and data transfer in network, Provides standardized services such as virtual terminal, file and job transfer and operations.

In Application Layer the two important basics concept can be used

1. Application Layer: The first step for getting data on to the network.

2. Application Software: The programs used to communicate over the network. For example: When displaying a web page the Application Layer uses the HTTP Protocol. The Application Software is your browser.



Functionality of the TCP/IP Application Layer protocols it roughly into the top three layers of the OSI Model.

Most TCP/IP application layer protocols were developed before PCs, GUIs and multimedia objects. They implement very little of the Presentation and Session layer functionality.

Session Layer Functionality is used to Create and maintain dialogs between source and destination applications. Handles the exchange of information to initiate dialogs, keep them active and restart sessions. Incorporated by most applications (e.g. Web Browser).

The Application Layer uses protocols that are implemented within applications and services Applications **provide** people a way to create messages. Application layer **services** establish an interface to the network. **Protocols** provide the rules and formats that govern how data is treated.

Presentation Layer Functionality include Coding and conversion of application layer data, Compression, Coding and compression formats: GIF, JPG, TIF, Encryption.

In an Application Layer services Application layer protocols are used by both the source and destination devices during a communication session. The application layer protocols implemented on the source and destination host must match.

The followings are the Application Layer Services and its Ports number

DNS (Domain Name System): Resolves Internet names (URLs) to IP Addresses, port 53

Telnet, SSH (Terminal emulation, Secure shell): access to servers and network devices, port 23, 22

SMTP (Simple Mail Transfer Protocol): Transfer of mail messages and attachments (outgoing), port 25

POP3, POP3S (Post Office Protocol): Transfer of mail messages and attachments (incoming), port 110, 995

IMAP: Internet Message Access Protocol, port 143

DHCP (Dynamic Host Configuration Protocol): Assigns IP Addresses (IP, subnet mask) and other parameters (DNS, Gateway,) to hosts, port 67, 68

HTTP(s) (Hypertext Transfer Protocol): Transfer less that make up web pages, port 80, 443

FTP(S) ((Secure) File Transfer Protocol): Interactive less transfer between systems, port control: 21,data:21 and 3713, data:989,990

9. Explain in detail about ATM protocol architecture model (11 marks)

The *asynchronous transfer mode* (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.

Figure shows the reference model for ATM. The first thing to notice is that, as well as layers, the model has planes. The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes.

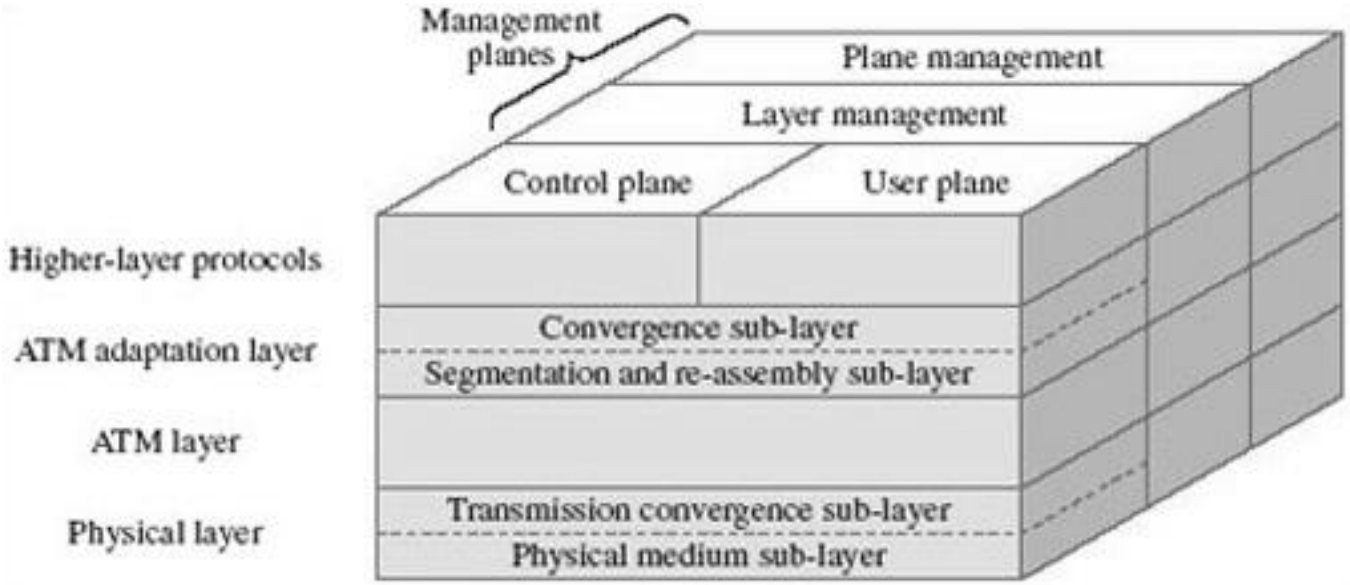


Figure ATM reference model

The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. The horizontal layers indicate the encapsulation of protocols through levels of abstraction as one layer is built on top of another, whereas the vertical planes indicate the functions that require co-ordination of the actions taken by different layers. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane).

The protocols in the ATM layer provide communication between ATM switches while the protocols in the ATM adaptation layer (AAL) operate end-to-end between users. This is illustrated in the example ATM network in Figure.

Two types of interface are identified in Figure 24: one between the users and the network (user-network interface), and the other between the nodes (switches) within the network (network-node interface).

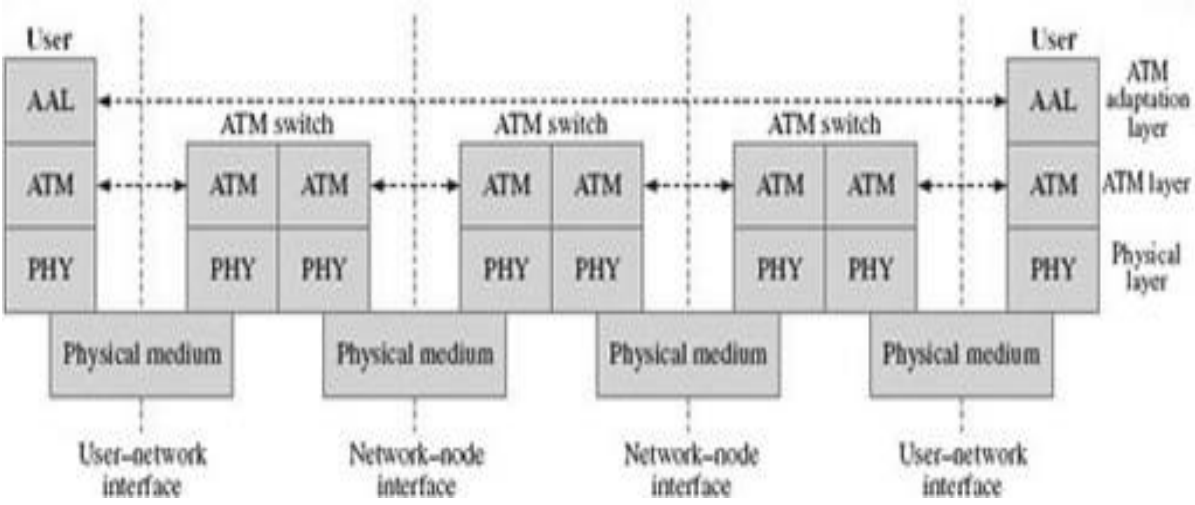
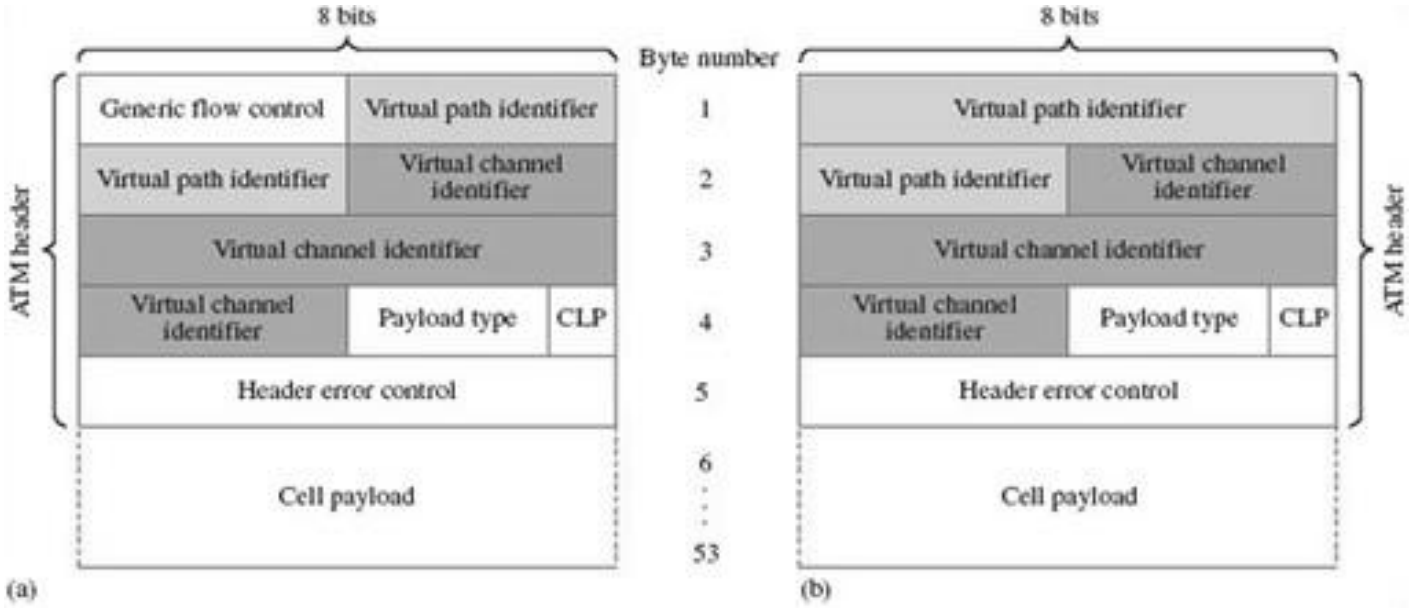


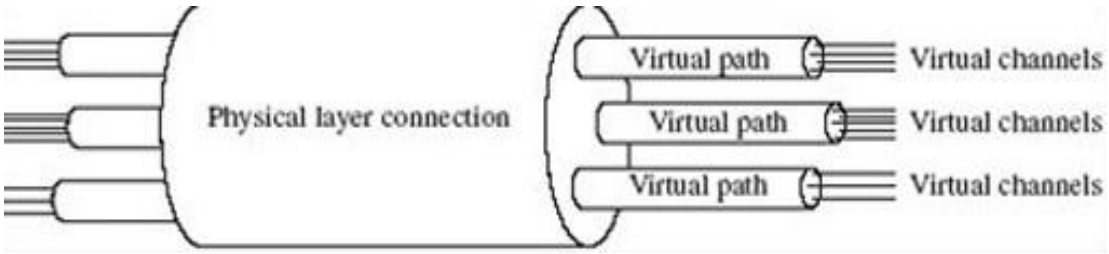
Figure ATM network

Before describing the functions of the three layers in the ATM reference model, describe the format of ATM cells. Figure shows the two basic types of cell.



Each ATM cell consists of 53 bytes: the header is five bytes long and the remaining 48 bytes (the cell payload) carry information from higher layers. The only difference between the two types of ATM cell is that the cells at the user-network interface carry a data field for the flow control of data from users. This means that only eight bits are available for virtual path identifiers, rather than 12 bits at the network-node interface.

The virtual connections set up in ATM networks are identified by the combination of the *virtual path identifier* and *virtual channel identifier* fields shown in Figure 26. These two fields provide a hierarchy in the numbering of virtual connections, whereby a virtual path contains a number of virtual channels as is illustrated in Figure below. An advantage of this hierarchy is that in some cases the switching of ATM cells may be based on the virtual path identifier alone.



The payload type field identifies the type of cell. I do not intend to describe the specific types of ATM cell, but there are types for carrying user information, signaling information for controlling virtual connections, and management information. There are two basic types of user information cell: one in which congestion has been identified and one in which it has not.

The cell loss priority (CLP) field is a single bit; if the bit is 0 that cell has a high priority, and if the bit is 1 the cell has a low priority. This information may influence the decision whether to discard cells if a network becomes congested.

The header error control field contains a cyclic redundancy check on the other bytes in the header.

ATM layers

ATM physical layer

The ATM physical layer is divided into two sub-layers: the transmission convergence sub-layer and the physical medium sub-layer.

Functions of the transmission convergence sub-layer include generating and receiving cells, and generating and verifying the cyclic redundancy check in the header error control field. For correct interpretation of ATM cells it is important to identify the beginning of a cell. In theory, if ATM cells are transmitted as a continuous stream of bits, once a receiver has found the start of one cell, the start of the next cell starts 53 × 8 = 424 bits later. However, this still leaves the problem of identifying the start of the first ATM cell. The sending device inserts a cyclic redundancy check word in the header error control field in each ATM cell. A receiving device performs cyclic redundancy checks on 40 consecutive bits (five bytes) of the bit stream, so valid headers will pass this test. Of course, it is possible that any 40 bits may pass a cyclic redundancy check by chance. To avoid the possibility of misinterpretation, a receiver will check the header error control bytes of the next few cells before assuming that it has managed to synchronize with the arrival of ATM cells over a link. Unfortunately, because of mismatches in the timing of senders and receivers, it is possible to lose bits. Therefore, the receiver should still monitor the header error control field. If several consecutive cells fail the cyclic redundancy check, the receiver assumes that it has lost synchronization over that link and starts again to look for ATM headers by examining 40 consecutive bits. This process is shown as a state diagram in Figure 28. The number of correct header error control checks that should occur before the receiver assumes synchronization is expressed as δ α and the number of incorrect checks that can occur before it assumes loss of synchronization is expressed as $\alpha\alpha$.

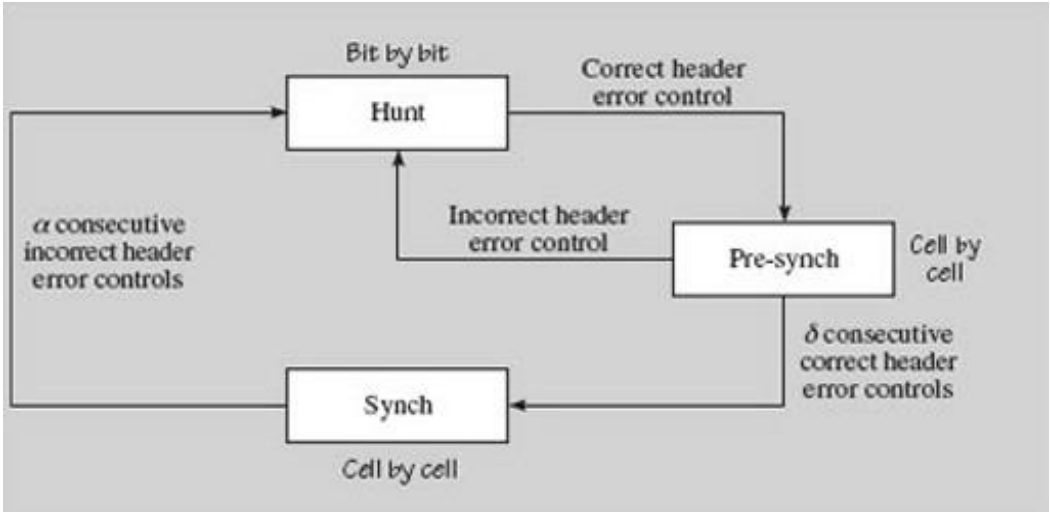


Figure ATM cell synchronization

ATM layer

The primary functions of the ATM layer are associated with the routing and switching of ATM cells. Because ATM cells are packets, the switches are packet switches and the switching operation can be called forwarding, but by convention, because the ATM layer provides a connection-oriented service, the term 'forwarding' is generally not used.

The path cells take and the resources allocated to them depend on their service category. This is determined when a virtual connection is established. The following service categories are recognized by the ATM layer:

- Constant bit rate – a constant data rate is allocated and is continuously available for the duration of a connection.
- Real-time variable bit rate – there are some commitments about the data rate to be made available, and the delay and variation in delay are tightly controlled.
- Non-real-time variable bit rate – there are some commitments about the data rate to be made available, but no delay limits are placed on the delivery of cells.
- Unspecified bit rate – there are no commitments about the data rate to be made available.
- Available bit rate – the data rate made available may be changed during the time a connection is maintained.
- Guaranteed frame rate – there is a commitment about the minimum data rate of a connection.

There are two types of virtual circuit – switched virtual circuits and permanent virtual circuits. The two types are similar in that they must be established before user data can be transferred; the difference is how they are set up. Switched virtual circuits are set up in response to user requests to transfer data and are released once that exchange has been completed.

Permanent virtual circuits are set up by management activities in response to contracts established between users and are expected to last much longer than switched virtual circuits. The word 'permanent' may be misleading because permanent virtual circuits do change in a network, but they change relatively infrequently, and from the point of view of users they are always available. Both types of virtual circuit are controlled by functions in the control plane of the ATM reference model and are very important for the routing and switching of ATM cells.

In an ATM virtual connections, similar to TCP connections, but they take place at a lower level of abstraction. ATM switches examine the destination address in a set-up message and decide the best path to take for the service category intended for that connection. Each link in the path is identified by a virtual path identifier and a virtual channel identifier. Once a virtual circuit has been established, ATM

cells carrying user data are switched according to their virtual path and virtual channel identifiers. For the purposes of switching, permanent virtual circuits are treated identically to switched virtual circuits.

ATM adaptation layer

The basic function of the ATM adaptation layer is to convert the user data supplied by higher layers into 48-byte blocks of data. The ATM adaptation layer is divided into two sub-layers – the convergence sub-layer, and the segmentation and re-assembly sub-layer. The *convergence sub-layer* provides services to higher layers through a set of protocols, but I do not need to describe these here. The segmentation and re-assembly sub-layer separates the messages from the convergence sub-layer into ATM cells. Each of the two sub-layers adds some protocol information, which is transported in the payload of ATM cells as illustrated in Figure 29.

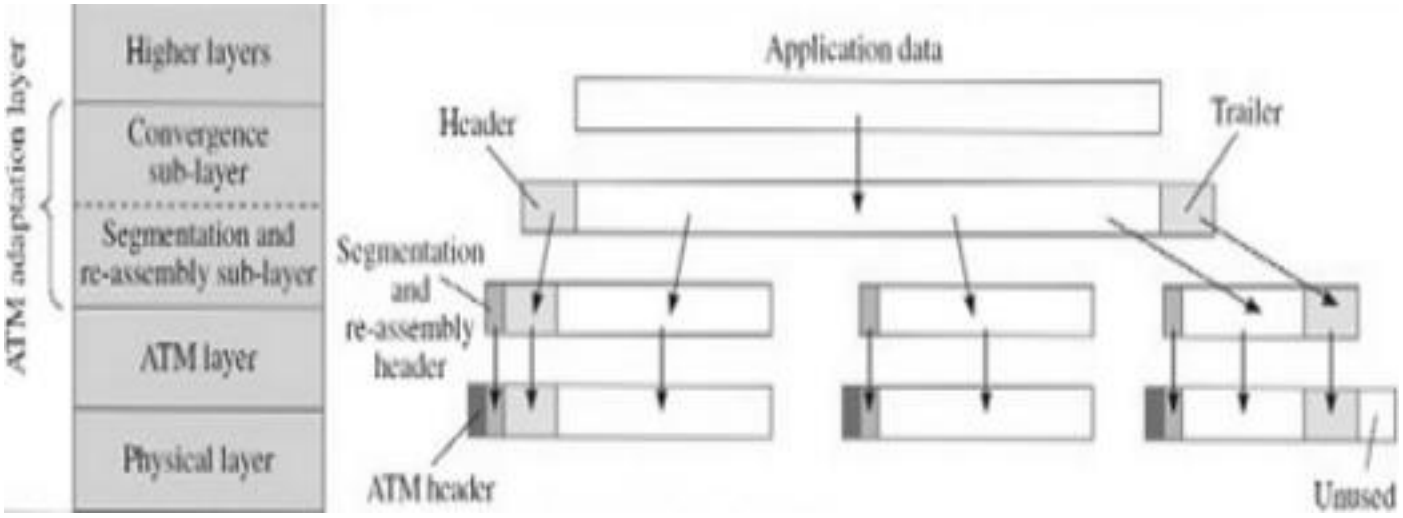


Figure 29 ATM adaptation layer functions

10. Explain in detail about Bootstrap Protocol(11 marks)

Protocol Description

The Bootstrap Protocol (BOOTP) is a UDP/IP-based protocol which allows a booting host to configure itself dynamically and without user supervision. BOOTP provides a means to notify a host of its assigned IP address, the IP address of a boot server host and the name of a file to be loaded into memory and executed. Other configuration information such as the local subnet mask, the local time offset, the addresses of default routers and the addresses of various Internet servers, can also be communicated to a host using BOOTP.

BOOTP uses two different well-known port numbers. UDP port number 67 is used for the server and UDP port number 68 is used for the BOOTP client. The BOOTP client broadcasts a single packet called a BOOTREQUEST packet that contains the client's physical network address and optionally, its IP address if known. The client could send the broadcast using the address 255.255.255.255, which is a

special address called the limited broadcast address. The client waits for a response from the server. If a response is not received within a specified time interval, the client retransmits the request.

The server responds to the client's request with a BOOTREPLY packet. The request can (optionally) contain the 'generic' filename to be booted, for example, 'unix' or 'ethertip'. When the server sends the bootreply, it replaces this field with the fully qualified path name of the appropriate boot file. In determining this name, the server may consult its own database correlating the client's address and filename request, with a particular boot file customized for that client. If the bootrequest filename is a null string, then the server returns a filename field indicating the 'default' files to be loaded for that client.

In the case of clients who do not know their IP addresses, the server must also have a database relating hardware address to IP address. This client IP address is then placed into a field in the bootreply.

BOOTP is an alternative to RARP, which operates at the Data Link Layer for LAN only. BOOTP, a UDP/IP based configuration protocol, provides much more configuration information and allows dynamic configuration for an entire IP network. BOOTP and its extensions became the basis for the Dynamic Host Configuration Protocol (DHCP).

Protocol structure

Op	The message operation code. Messages can be either BOOTREQUEST or BOOTREPLY.
Htype	The hardware address type.
Hlen	The hardware address length.
Xid	The transaction ID.
Secs	The seconds elapsed since the client began the address acquisition or renewal process.
Flags	The flags.
Ciaddr	The client IP address.
Yiaddr	The "Your" (client) IP address.
Siaddr	The IP address of the next server to use in bootstrap.
Giaddr	The relay agent IP address used in booting via a relay agent.
Chaddr	The client hardware address.
Sname	Optional server host name, null terminated string
File	Boot file name, null terminated string; generic name or null in DHCPDISCOVER, fully qualified directory path name in DHCPOFFER.
Options	Optional parameters field.

11. Explain in detail about Data Link Switching Client Access Protocol(6 marks)

Protocol Description

The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol used between workstations and routers to transport SNA/NetBIOS traffic over TCP sessions.

DCAP was introduced to address a few deficiencies in the Data Link Switching Protocol (DLSw). The implementation of the Data Link Switching Protocol (DLSw) on a large number of workstations raises the important issues of scalability and efficiency. Since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP addresses these issues. It introduces a hierarchical structure to resolve the scalability problems. All workstations are clients to the router (server) rather than peers to the router. This creates a client/server model. It also provides a more efficient protocol between the workstation (client) and the router (server).

In a DLSw network, each workstation needs a MAC address to communicate with an FEP attached to a LAN. When DLSw is implemented on a workstation, it does not always have a MAC address defined. For example, when a workstation connects to a router through a modem via PPP, it

only consists of an IP address. In this case, the user must define a virtual MAC address. This is administratively intensive since each workstation must have a unique MAC address. DCAP uses the Dynamic Address Resolution protocol to solve this problem. The Dynamic Address Resolution protocol permits the server to dynamically assign a MAC address to a client without complex configuration.

Protocol structure

4	8	16bit
Protocol ID	Version Number	Message Type
Packet Length		

Protocol description

Protocol ID: It consists of 4 bits. The value can be set to 8.

Version Number: It consists of 4 bits. The value can be set to 1.

Message Type :It consists of 8 bits. The message type can be DCAP message.

Packet Length: It consists of 16 bits. Size of the packet including the DCAP header, DCAP data and user data. The minimum size of the packet is 4 bytes.

12. Explain about Dynamic Host Configuration Protocol (6 marks)

Protocol Description

Dynamic Host Configuration Protocol (DHCP) is a communications protocol enabling network administrators manage centrally and to automate the assignment of IP addresses in a network. In an IP network, each device connecting to the Internet needs a unique IP address. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DHCP is an alternative to another network IP management protocol,
Bootstrap Protocol (BOOTP). DHCP is a more advanced protocol but both configuration management protocols are commonly used. Some operating systems, including Windows

NT/2000, come with DHCP servers. A DHCP or BOOTP client is a program that is located in each computer so that it can be configured.

Protocol Structure

8	16	24	32bit
Op	Htype	Hlen	Hops
Xid			
Secs		Flags	
Ciaddr			
Yiaddr			
Siaddr			
Giaddr			
Chaddr (16 bytes)			
Sname (64 bytes)			
File (128 bytes)			
Option (variable)			

Op	The message operation code. Messages can be either BOOTREQUEST or BOOTREPLY.
Htype	The hardware address type.
Hlen	The hardware address length.
Xid	The transaction ID.
Secs	The seconds elapsed since the client began the address acquisition or renewal process.
Flags	The flags.
Ciaddr	The client IP address.
Yiaddr	The “Your” (client) IP address.
Siaddr	The IP address of the next server to use in bootstrap.
Giaddr	The relay agent IP address used in booting via a relay agent.
Chaddr	The client hardware address.
Sname	Optional server host name, null terminated string
File	Boot file name, null terminated string; generic name or null in DHCPDISCOVER, fully qualified directory path name in DHCPOFFER.
Options	Optional parameters field. See the options documents for a list of defined options.

13. Explain about Domain Name System (Service) protocol(6 marks) (NOV 2013)

Protocol Description

Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

DNS has two independent aspects:

1. It specifies the name syntax and rules for delegating authority over names. The basic syntax is local.group.site

2. It specifies the implementation of a distributed computing system that efficiently maps names to addresses.

In theory, the domain name standard in DNS protocol specifies an abstract hierarchical namespace with arbitrary values for labels. Any group can build an instance of the domain system to choose labels for all parts of its hierarchy. However most users of the DNS protocols follow the hierarchical labels used by the official Internet domain system. Some of the top level domains are: COM, EDU, GOV, NET, ORG, BIZ ... plus many country codes.

The distributed scheme of DNS allows efficient and reliable mapping of names to IP addresses. Most names can be mapped locally and a set of servers operating at multiple sites cooperatively solve the mapping problem of a large network. Because of the distributing nature, no single machine failure will prevent the DNS from operating correctly.

Protocol Structure

<table>
<tr><td>16</td><td colspan="2">21</td><td colspan="3"></td><td colspan="2">28</td><td colspan="2">32bit</td></tr>
<tr><td>ID</td><td>Q</td><td>Query</td><td>A</td><td>T</td><td>R</td><td>V</td><td>B</td><td>Rcode</td></tr>
<tr><td>Question count</td><td colspan="8">Answer count</td></tr>
<tr><td>Authority count</td><td colspan="8">Additional count</td></tr>
</table>

ID	16bit field used to correlate queries and responses.
Q	1 bit field that identifies the message as a query or response.
Query	4bit field that describes the type of message: 0 Standard query (name to address); 1 Inverse query; 2 Server status request.
A	Authoritative Answer. 1bit field. When set to 1, identifies the response

	as one made by an authoritative name server.
T	Truncation. 1bit field. When set to 1, indicates the message has been truncated.
R	1bit field. Set to 1 by the resolve to request recursive service by the name server.
V	1bit field. Signals the availability of recursive service by the name server.
B	3bit field. Reserved for future use. Must be set to 0.
Rcode	Response Code. 4bit field that is set by the name server to identify the status of the query.
Question count	16bit field that defines the number of entries in the question section.
Answer count	16bit field that defines the number of resource records in the answer section.
Authority count	16bit field that defines the number of name server resource records in the authority section.
Additional count	16bit field that defines the number of resource records in the additional records section.

14. Write in detail File Transfer Protocol (6 marks)

File Transfer Protocol (FTP) enables file sharing between hosts. FTP uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfers. The control connection uses an image of the TELNET protocol to exchange commands and messages between hosts.

The key functions of FTP are:

1) To promote sharing of files (computer programs and/or data);
2) To encourage indirect or implicit (via programs) use of remote computers;
3) To shield a user from variations in file storage systems among hosts; and
4) To transfer data reliably and efficiently.

FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. FTP control frames are TELNET exchanges and can contain TELNET commands and option negotiation. However, most FTP control frames are simple ASCII text and can be classified as FTP commands or FTP

messages. FTP messages are responses to FTP commands and consist of a response code followed by explanatory text.

Command Description

ABOR	Abort data connection process.
ACCT <account>	Account for system privileges.
ALLO <bytes>	Allocate bytes for file storage on server.
APPE <filename>	Append file to file of same name on server.
CDUP <dir path>	Change to parent directory on server.
CWD <dir path>	Change working directory on server.
DELE <filename>	Delete specified file on server.
HELP <command>	Return information on specified command.
LIST <name>	List information if name is a file or list files if name is a directory.
MODE <mode>	Transfer mode (S=stream, B=block, C=compressed).
MKD <directory>	Create specified directory on server.
NLST <directory>	List contents of specified directory.
NOOP	Cause no action other than acknowledgement from server.
PASS <password>	Password for system login.
PASV	Request server wait for data connection.
PORT <address>	IP address and 2byte system port ID.
PWD	Display current working directory.
QUIT	Log off from the FTP server.
REIN	Reinitialize connection to login status.
REST <offset>	Restart file transfer from given offset.
RETR <filename>	Retrieve (copy) file from server.
RMD <directory>	Remove specified directory on server.
RNFR <old path>	Rename from old path.
RNTO <new path>	Rename to new path.
SITE <params>	Site specific parameters provided by server.
SMNT <pathname>	Mount the specified file structure.

STAT <directory>	Return information on current process or directory.
STOR <filename>	Store (copy) file to server.
STOU <filename>	Store file to server name.
STRU <type>	Data structure (F=file, R=record, P=page).
SYST	Return operating system used by server.
TYPE <data type>	Data type (A=ASCII, E=EBCDIC, I=binary).
USER <username>	User name for system login.

Standard FTP messages are as follows:

Response Code	**Explanatory Text**
110	Restart marker at MARK yyyy=mmmm (new file pointers).
120	Service ready in nnn minutes.
125	Data connection open, transfer starting.
150	Open connection.
200	OK.
202	Command not implemented.
211	(System status reply).
212	(Directory status reply).
213	(File status reply).
214	(Help message reply).
215	(System type reply).
220	Service ready.
221	Log off network.
225	Data connection open.
226	Close data connection.
227	Enter passive mode (IP address, port ID).
230	Log on network.
250	File action completed.
257	Path name created.
331	Password required.
332	Account name required.

350	File action pending.
421	Service shutting down.
425	Cannot open data connection.
426	Connection closed.
450	File unavailable.
451	Local error encountered.
452	Insufficient disk space.
500	Invalid command.
501	Bad parameter.
502	Command not implemented.
503	Bad command sequence.
504	Parameter invalid for command.
530	Not logged onto network.
532	Need account for storing files.
550	File unavailable.
551	Page type unknown.
552	Storage allocation exceeded.
553	File name not allowed.

15. Write in detail Hypertext Transfer Protocol?

Protocol Description

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990.

HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. It builds on the discipline of reference provided by the Uniform Resource Identifier (URI), as a location (URL) or name (URN), for indicating the resource on which a method is to be applied. Messages are passed in a format similar to that used by Internet Mail and the Multipurpose Internet Mail Extensions (MIME).

HTTP is also used as a generic protocol for communication between user agents and proxies/gateways to other Internet protocols, such as SMTP, NNTP, FTP, Gopher and WAIS, allowing

basic hypermedia access to resources available from diverse applications and simplifying the implementation of user agents.

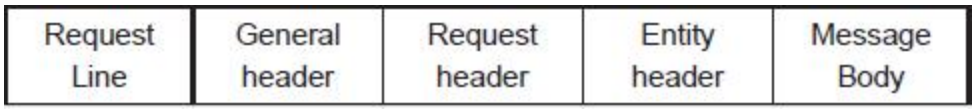
The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a connection with a server. The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet. HTTP/1.0, as defined by RFC 1945, improved the protocol by allowing messages to be in the format of MIME-like messages, containing meta information about the data transferred and modifiers on the request/response semantics. However, HTTP/1.0 does not sufficiently take into consideration the effects of hierarchical proxies, caching, the need for persistent connections, or virtual hosts. "HTTP/1.1" includes more stringent requirements than HTTP/1.0 in order to ensure reliable implementation of its features. There is a secure version of HTTP (S-HTTP) specification, which will be discussed in a separate document.

Protocol Structure

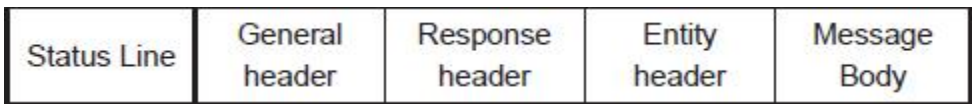
HTTP messages consist of requests from client to server and responses from server to client.

The request message has the following format:



The Request-Line begins with a method token, followed by the Request-URI and the protocol version, and ends with CRLF. The elements are separated by SP characters. No CR or LF is allowed except in the final CRLF sequence. The details of the general header, request header and entity header can be found in the reference documents.

The response message has the following format:



The Status-Code element is a 3-digit integer result code of the attempt to understand and satisfy the request. The Reason-Phrase is intended to give a short textual description of the Status-Code. The

Status-Code is intended for use by automata and the Reason-Phrase is intended for the human user. The client is not required to examine or display the Reason-Phrase. The details of the general header, response header and entity header could be found in the reference documents.

16. Explain about Simple Mail Transfer Protocol (11 marks)

Protocol Description

Simple Mail Transfer Protocol (SMTP) is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and provides notification regarding incoming mail.

SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. An important feature of SMTP is its capability to transport mail across networks, usually referred to as "SMTP mail relaying". A network consists of the mutually-TCP-accessible hosts on the public Internet, the mutually-TCP-accessible hosts on a firewall-isolated TCP/IP Intranet, or hosts in some other LAN or WAN environment utilizing a non-TCP transport-level protocol. Using SMTP, a process can transfer mail to another process on the same network or to some other network via a relay or gateway process accessible to both networks.

In this way, a mail message may pass through a number of intermediate relay or gateway hosts on its path from sender to ultimate recipient. The Mail eXchanger mechanisms of the domain name system are used to identify the appropriate next-hop destination for a message being transported.

Protocol Structure

SMTP commands are ASCII messages sent between SMTP hosts. Possible commands are as follows:

Command	Description
DATA	Begins message composition.
EXPN <string>	Returns names on the specified mail list.
HELO <domain>	Returns identity of mail server.
HELP <command>	Returns information on the specified command.
MAIL FROM <host>	Initiates a mail session from host.
NOOP	Causes no action, except acknowledgement from server.
QUIT	Terminates the mail session.
RCPT TO <user>	Designates who receives mail.

RSET	Resets mail connection.
SAML FROM <host>	Sends mail to user terminal and mailbox.
SEND FROM <host>	Sends mail to user terminal.
SOML FROM <host>	Sends mail to user terminal or mailbox.
TURN	Switches role of receiver and sender.
VRFY <user>	Verifies the identity of a user.

17. Explain about Network News Transfer Protocol (11 marks)

Protocol Description

Network News Transfer Protocol (NNTP) specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream (such as TCP port 119) server-client model. NNTP is designed so that news articles need only be stored on one (presumably central) server host, and subscribers on other hosts attached to the network may read news articles using stream connections to the news host. The Network News Transfer Protocol (NNTP) established the technical foundation for the widely used Newsgroups.

NNTP is modeled after the USENET news system. However, NNTP makes few demands upon the structure, content or storage of news articles and thus it can easily be adapted to other non-USENET news systems. Using NNTP, hosts exchanging news articles have an interactive mechanism for deciding which articles are to be transmitted.

Host desiring new news, or which has new news to send, will typically contact one or more of its neighbors using NNTP. The client host will then inquire as to which new articles have arrived in all or some of the newsgroups that it desires to receive, using the NEWNEWS command. It will receive a list of new articles from the server, and can request transmission of those articles that it desires and does not already have. Finally, the client can advise the server of those new articles which the client has recently received. The server will indicate those articles that it has already obtained copies of and which articles should be sent to add to its collection. In this manner, only those articles which are not duplicates and which are desired are transferred.

Protocol Structure

NNTP uses commands and responses for communications. Commands consist of a command word, which in some cases may be followed by a parameter. NNTP has many commands.

The following are the key commands:

Article <message ID> Displays the header, a blank line, then the body (text) of the specified article.

Message-id Optional field, is the message id of an article as shown in that article's header. If it is blank, the current article is assumed.

Head Identical to the ARTICLE command except that it returns only the header lines.

Status Similar to the ARTICLE command except that no text is returned.

Group <ggg> The required parameter ggg is the name of the newsgroup to be selected. A list of valid newsgroups may be obtained from the LIST command. The successful selection response will return the article numbers of the first and last articles in the group, and an estimate of the number of articles on file in the group.

Body Identical to the ARTICLE command except that it returns only the text body of the article.

List Returns a list of valid newsgroups and associated information.

NewsGroups A list of newsgroups created since <date and time> will be listed in the same format as the LIST command.

NewNews A list of message-ids of articles posted to or received by the specified newsgroup since "date" will be listed.

Next The internally maintained "current article pointer" is advanced to the next article in the current newsgroup.

Post If posting is allowed, response code 340 is returned to indicate that the article to be posted should be sent.

Quit The server process acknowledges the QUIT command and then closes the connection to the client.

18. Explain about Terminal emulation protocol of TCP/IP (11 marks)

Protocol Description

TELNET is the terminal emulation protocol in a TCP/IP environment.TELNET uses the TCP as the transport protocol to establish connection between server and client. After connecting, TELNET server and client enter a phase of option negotiation that determines the options that each side can support for the connection. Each connected system can negotiate new options or renegotiate old options at any time. In general, each end of the TELNET connection attempts to implement all options that maximize performance for the systems involved.

When a TELNET connection is first established, each end is assumed to originate and terminate at a "Network Virtual Terminal", or NVT. An NVT is an imaginary device which provides a standard,

network-wide, intermediate representation of a canonical terminal. This eliminates the need for "server" and "user" hosts to keep information about the characteristics of each other's terminals and terminal handling conventions.

The principle of negotiated options takes cognizance of the fact that many hosts will wish to provide additional services over and above those available within an NVT and many users will have sophisticated terminals and would like to have elegant, rather than minimal, services.

Option requests are likely to flurry back and forth when a TELNET connection is first established, as each party attempts to get the best possible service from the other party. Beyond that, however, options can be used to dynamically modify the characteristics of the connection to suit changing local conditions.

Modern Telnet is a versatile terminal emulation due to the many options that have evolved over the past twenty years. Options give TELNET the ability to transfer binary data, support byte macros, emulate graphics terminals, and convey information to support centralized terminal management.

Protocol Structure

TELNET commands are ASCII text. The following are the TELNET commands:

Commands	Code No.		Description
	Dec	Hex	
Data			All terminal input/output data.
End subNeg	240	FO	End of option subnegotiation command.
No Operation	241	F1	No operation command.
Data Mark	242	F2	End of urgent data stream.
Break	243	F3	Operator pressed the Break key or the Attention key.
Int process	244	F4	Interrupt current process.
Abort output	245	F5	Cancel output from current process.
You there?	246	F6	Request acknowledgment.
Erase char	247	F7	Request that operator erase the previous character.
Erase line	248	F8	Request that operator erase the previous line.
Go ahead!	249	F9	End of input for half - duplex connections.
SubNegotiate	230	FA	Begin option subnegotiation.
Will Use	231	FB	Agreement to use the specified option.
Won't Use	232	FC	Reject the proposed option.

Start use	233	FD	Request to start using specified option.
Stop Use	234	FE	Demand to stop using specified option.
LAC	235	FF	Interpret as command.

19. Explain about Remote Monitoring MIBs (11 marks)

Protocol Description

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

RMON was originally developed to address the problem of managing LAN segments and remote sites from a central location. The RMON is an extension of the SNMP MIB. Within an RMON network monitoring data is defined by a set of statistics and functions and exchanged between various different monitors and console systems. Resultant data is used to monitor network utilization for network planning and performance-tuning, as well as assisting in network fault diagnosis.

There are 2 versions of RMON: RMONv1 and RMONv2. RMONv1, which can now be found on most modern network hardware, defined 9 MIB groups for basic network monitoring.

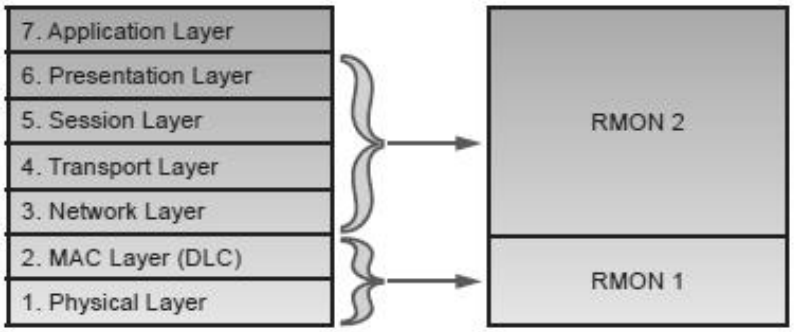
RMON2 is an extension of RMON that focuses on higher layers of traffic above the medium access-control(MAC) layer. RMON2 has an emphasis on IP traffic and application-level traffic.

RMON2 allows network management applications to monitor packets on all network layers. This is different from RMONv1, which only allows network monitoring at MAC layer or below.

RMON solutions are comprised of two components: a probe (or an agent or a monitor), and a management station. Agents store network information within their RMON MIB and are normally found as embedded software on network hardware such as routers and switches although they can be a program running on a PC. Agents can only see the traffic that flows through them so they must be placed on each LAN segment or WAN link that is to be monitored. Clients, or management stations, communicate with the RMON agent or probe, using SNMP to obtain and correlate RMON data. There are a number of variations to the RMON MIB. For example, the Token Ring RMON MIB provides objects specific to managing Token Ring networks. The SMON MIB extends RMON by providing RMON analysis for switched networks.

Protocol Structure

The monitoring focus of RMON1 and RMON 2 in the network layers:



RMON Monitoring Layers

RMON 1 MIB Group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores for retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples and compares them with set thresholds for events generation.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the top hosts.	Statistics, host(s), sample start and stop periods, rate base,duration.
Matrix	Stores and retrieves statistics for	Source and destination address pairs

	conversations between sets of two addresses.	and packets, bytes, and errors for each pair.
Filters	Enables packets to be matched by a filter equation for capturing or events.	Bit filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), number of captured packets.
Events	Controls the generation and notification of events from this device.	Event type, description, last time event sent.
Token Ring	Support of Token Ring	(not used often)

RMON 2 MIB Group	Functions
Protocol Directory	The Protocol Directory is a simple and interoperable way for an RMON2 application to establish which protocols a particular RMON2 agent implements. This is especially important when the application and the agent are from different vendors .
Protocol Distribution	Mapping the data collected by a probe to the correct protocol name that can then be displayed to the network manager.
Address mapping	Address translation between MAC layer addresses and network layer addresses which are much easier to read and remember. Address translation not only helps the network manager, it supports the SNMP management platform and will lead to improved topology maps.
Network Layer host	Network host (IP layer) statistics
Network layer matrix	Stores and retrieves network layer (IP layer) statistics for conversations between sets of two addresses.
Application layer host	Application host statistic
Application layer	Stores and retrieves application layer statistics for conversations

matrix	between sets of two addresses.
User history	This feature enables the network manager to configure history studies of any counter in the system, such as a specific history on a particular file server or a router to router Connection.
Probe configuration	This RMON2 feature enables one vendor's RMON application to remotely configure another vendor's RMON probe.

20. Write in detail Simple Network Management Protocol (11 marks)

Protocol Description

SNMP, an application layer protocol, is the standard protocol developed to manage nodes (servers, workstations, routers, switches and hubs, etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

An SNMP managed network consists of three key components: managed devices, agents, and network-management systems (NMSs). A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers. An agent is a network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

Currently, there are three versions of SNMP defined: SNMP v1, SNMP v2 and SNMP v3. Both versions 1 and 2 have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations. SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to the previous versions. To solve the incompatible issues among different versions of SNMP, RFC 3584 defines the coexistence strategies.

SNMP also includes a group of extensions as defined by RMON, RMON 2, MIB, MIB2,SMI, OIDs, and Enterprise OIDs.

Protocol Structure

SNMP is an application protocol, which is encapsulated in UDP. The general SNMP message format for all versions is shown below:

Version	Community	PDU

• Version -- SNMP version number. Both the manager and agent must use the same version of SNMP. Messages containing different version numbers are discarded without further processing.

• Community -- Community name used for authenticating the manager before allowing access to the agent.

• PDU (Protocol Data Unit) -- The PDU types and formats for SNMPv1, v2 and v3 will be explained in the corresponding sections.

Pondicherry University Questions

2 Marks

1. What is the purpose of OSI Model? (UQ NOV '13) (Ref.Pg.No.05 Qn.No.08)
2. List the Various Function of Data Link Layer? (UQ APRIL'13) (Ref.Pg.No.07Qn.No.18)
3. Define DHCP? (UQ APRIL'13 & NOV'13) (Ref.Pg.No.09Qn.No.25)

11 Marks

(Regular)

3. 2. Explain in detail about TCP/IP Four Layers Architecture Model? (UQ NOV'13)(Ref.Pg.No.19 Qn.No.05)

(Arrear)

1. Discuss in detailed about OSI ISO layered function in details? (UQ APRIL '13) (Ref.Pg.No.18 Qn.No.03)
2. Explain various application layer protocols and its functions? (UQ APRIL'13)(Ref.Pg.No.24 Qn.No.08)
3. Explain about Domain Name System (Service) protocol??(UQ APRIL '13)(Ref.Pg.No.36 Qn.No.13)

SRI VENKATESHWARAA COLLEGE OF ENGINEERING & TECHNOLOGY

(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry.)
13-A, Villupuram – Pondy Main road, Ariyur, Puducherry – 605 102.
Phone: 0413-2644426, Fax: 2644424 / Website: www.svcetpondy.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Subject: NETWORK PROTOCOL **Subject Code: CS E77**

UNIT II

Presentation Layer Protocol: LPP.
Session Layer protocols: RPC, SDP, SIP.
Transport Layer protocols: TCP, UDP, RDP, and RUDP.

Faculty Incharge **HOD** **PRINCIPAL**

2 Marks

1. What is the use of LPP?

Lightweight Presentation Protocol (LPP) describes an approach for providing "stream-lined" support of OSI application services on top of TCP/IP-based network for some constrained environments. LPP was initially derived from a requirement to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks.

2. What is the use of RPC?

Remote Procedure Call (RPC) is a protocol for requesting a service from a program located in a remote computer through a network, without having to understand the under layer network technologies. RPC presumes the existence of a low-level transport protocol, such as TCP or UDP, for carrying the message data between communicating p

rograms.

3. What is meant by SIP? (APRIL 2013)

The **Session Initiation Protocol** (**SIP**) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.

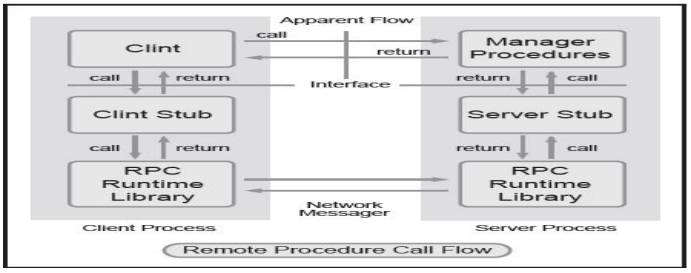
The protocol defines the messages that are sent between endpoints which govern establishment, termination and other essential elements of a call. SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams. SIP can be used for two-party (unicast) or multiparty (multicast) sessions. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games

4. What is meant by Stub?

- Stubs are generated automatically from interface specifications.
- Stubs hide details of (un)marshalling from application programmer & library code developer.
- Client Stubs perform marshalling into request messages and unmarshalling from reply messages

- Server Stubs perform unmarshalling from request messages and marshalling into reply messages
- Stubs also take care of communication & invocation

5. Draw remote procedure call flow.



6. What is the purpose of SDP?

The Session Description Protocol (SDP) describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

7. Write the names included in the text messages.

The SDP text messages include:

- Session name and purpose
- Time the session is active
- Media comprising the session
- Information to receive the media (address etc.)

8. Write the use SIP in application layer.

Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session.

9. Write about the SIP supports.

SIP supports five facets of establishing and terminating multimedia communications:

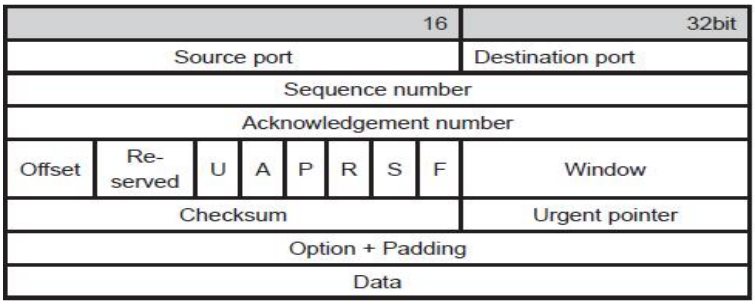
- User location: determination of the end system to be used for communication;
- User availability: determination of the willingness of the called party to engage in communications;

- User capabilities: determination of the media and media parameters to be used;
- Session setup: "ringing", establishment of session parameters at both called and calling party;
- Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

10. What is TCP?

Transmission Control Protocol (TCP) is the transport layer protocol in the TCP/IP suite, which provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgment with retransmission of packets when necessary. Along with the Internet Protocol (IP), TCP represents the heart of the Internet protocols.

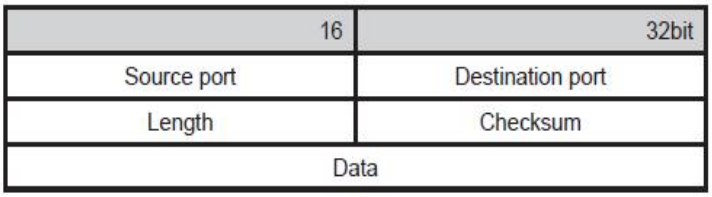
11. Draw TCP protocol structure.



12. What is UDP? (NOV 2013)

UDP is a connectionless transport layer (layer 4) protocol in the OSI model which provides a simple and unreliable message service for transaction-oriented services. UDP is basically an interface between IP and upper-layer processes.

13. Draw UDP protocol structure.



14. Compare TCP and UDP? (APRIL 2013)

TCP or **Transmission Control Protocol** and **UDP** or **User Datagram Protocol**. TCP is connection oriented once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

15. What is RDP? (NOV 2013)

RDP is a connection-oriented transport protocol designed to efficiently support the bulk transfer of data for such host monitoring and control applications as loading/dumping and remote debugging. It attempts to provide only those services necessary, in order to be efficient in operation and small in size.

16. Draw RDP protocol structure.

1	2	3	4	5	6	8	16bit
SYN	ACK	EAK	RST	NUL	0	Ver No	Header Length
Source Port							
Destination Port							
Data Length							
Sequence Number							
Acknowledgement Number							
Checksum							
Variable header area …							

17. What is RUDP?

Reliable UDP (RUDP) is a simple packet based transport protocol, based on RFCs 908 (version 1) and 1151 (version 2), which was intended as a reliable transport protocol to transport telephony signaling across IP networks.

18. Draw RUDP protocol structure.

1	2	3	4	5	6	7	8	16bit
SYN	ACK	EAK	RST	NUL	CHK	TCS	0	Header Length
Sequence number								Ack number
Checksum								

19. Write the functions of RDP control flags.

SYN	The SYN bit indicates a synchronization segment is present.

ACK	The ACK bit indicates the acknowledgment number in the header is valid.
EACK	The EACK bit indicates an extended acknowledge segment is present.
RST	The RST bit indicates the packet is a reset segment.
NUL	The NUL bit indicates the packet is a null segment.
0	The value of this field must be zero.
Ver no	version number; current version is 2.

20. Write the features of RUDP.

Reliable UDP features include:

- Client acknowledgment of packets sent by the server to the client
- Windowing and congestion control so the server does not exceed the currently available bandwidth
- Server retransmission to the client in the event of packet loss
- Faster than real-time streaming known as “over buffering”.

11 Marks

1. Write in detail Lightweight Presentation Protocol (11 marks)(NOV 2013)(APRIL 2013)

Protocol Description

Lightweight Presentation Protocol (LPP) describes an approach for providing "stream-lined" support of OSI application services on top of TCP/IP-based network for some constrained environments. LPP was initially derived from a requirement to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks.

LPP is designed for a particular class of OSI applications, namely those entities whose application context contains only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). In addition, a Directory Services Element (DSE) is assumed for use by the application entity, but only in a very limited sense. LPP is not applicable to entities whose application context is more extensive (e.g., contains a Reliable Transfer Service Element).

If one wants to implement ISO applications in a TCP/IP based network without constrains, the ITOT mechanisms (specified in RFC 2126) should be used.

Protocol Structure

The service provider is in one of the following states:
IDLE, WAIT1, WAIT2, DATA, WAIT3 or WAIT4
The possible events are:
PS-user P-CONNECT.REQUEST
P-CONNECT.RESPONSE
P-RELEASE.REQUEST
P-RELEASE.RESPONSE
P-DATA.REQUEST
P-U-ABORT.REQUEST
Network TCP closed or errored(*)
receive ConnectRequest PDU
receive ConnectResponse PDU
receive ReleaseRequest PDU
receive ReleaseResponse PDU
receive UserData(*) or CL-UserData(**) PDU
receive user-initiated Abort PDU
receive provider-initiated Abort PDU
timer expires(**)
The possible actions are:
PS-user P-CONNECT.INDICATION
P-CONNECT.CONFIRMATION
P-RELEASE.INDICATION
P-RELEASE.CONFIRMATION
P-DATA.INDICATION

P-U-ABORT.INDICATION
P-P-ABORT.INDICATION
network open TCP(*)
close TCP(*)
send ConnectRequest PDU
send ConnectResponse PDU
send ReleaseRequest PDU
send ReleaseResponse PDU
send UserData(*) or CL-UserData(**) PDU
send user-initiated Abort PDU
send provider-initiated Abort PDU
set timer(**)
(*) tcp-based service only
(**) udp-based service only

2. Explain in detail about Remote Procedure Call protocol (11 marks)

Protocol Description

Remote Procedure Call (RPC) is a protocol for requesting a service from a program located in a remote computer through a network, without having to understand the under layer network technologies. RPC presumes the existence of a low-level transport protocol, such as TCP or UDP, for carrying the message data between communicating programs. RPC spans the
Transport layer and the Application layer in the Open Systems Interconnection (OSI) model of network communication. RPC makes it easier to develop an application that includes multiple
programs distributed in a network.

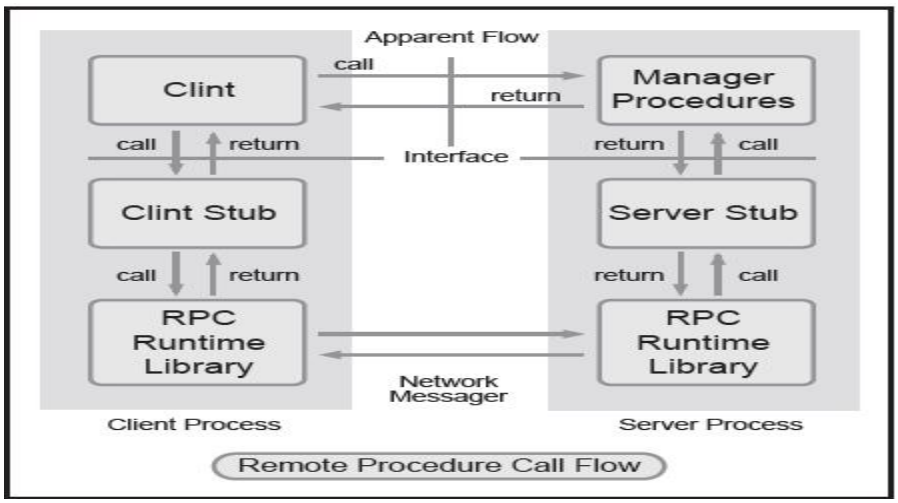
RPC uses the client/server model. The requesting program is a client and the service-providing program is the server. First, the caller process sends a call message that includes the procedure parameters to the server process. Then, the caller process waits for a reply message (blocks). Next, a process on the server side, which is dormant until the arrival of the call message, extracts the procedure parameters, computes the results, and sends a reply message. The server waits for the next call message. Finally, a process on the caller receives the reply message, extracts the results of the procedure, and the caller resumes execution.

There are several RPC models and implementations. Sun Microsystem originally introduced the RPC. IETF ONC charter modified the Sun version and made the ONC PRC protocol, an IETF standard protocol. A popular model and implementation is the Open Software Foundation's Distributed Computing Environment (DCE).

Protocol Structure

The Remote Procedure Call (RPC) message protocol consists of two distinct structures: the call message and the reply message.

The message flows are displayed as follows:



RPC Call Message: Each remote procedure call message contains the following unsigned integer fields to uniquely identify the remote procedure:

- Program number
- Program version number
- Procedure number

The body of an RPC call message takes the following form:

```
struct call_body {
    unsigned int rpcvers;
    unsigned int prog;
    unsigned int vers;
    unsigned int proc;
    opaque_auth cred;
    opaque_auth verf;
    1 parameter
    2 parameter . . .
};
```

RPC Reply Message: The RPC protocol for a reply message varies depending on whether the call message is accepted or rejected by the network server. The reply message to a request contains information to distinguish the following conditions:

- RPC executed the call message successfully.

• The remote implementation of RPC is not protocol version 2. The lowest and highest supported RPC version numbers are returned.

• The remote program is not available on the remote system.

• The remote program does not support the requested version number. The lowest and highest supported remote program version numbers are returned.

• The requested procedure number does not exist. This is usually a caller-side protocol or programming error.

The RPC reply message takes the following form:

```
enum reply stat stat {
    MSG_ACCEPTED = 0,
    MSG_DENIED = 1
};
```

3. Explain in detail about Session Description Protocol (11 marks)

Protocol Description

The Session Description Protocol (SDP) describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

Session directories assist the advertisement of conference sessions and communicate the relevant conference setup information to prospective participants. SDP is designed to convey such information to recipients. SDP is purely a format for session description - it does not incorporate a transport protocol, and is intended to use different transport protocols as appropriate including the Session Announcement Protocol (SAP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), electronic mail using the MIME extensions, and the Hypertext Transport Protocol (HTTP).

SDP is intended to be general purpose so that it can be used for a wider range of network environments and applications than just multicast session directories. However, it is not intended to support negotiation of session content or media encodings.

On Internet Multicast backbone (Mbone) a session directory tool is used to advertise multimedia conferences and communicate the conference addresses and conference tool-specific information necessary for participation. The SDP does this. It communicates the existence of a session and conveys sufficient information to enable participation in the session. Many of the SDP messages are sent by periodically multicasting an announcement packet to a well-known multicast address and port using SAP (Session Announcement Protocol). These messages are

UDP packets with a SAP header and a text payload. The text payload is the SDP session description. Messages can also be sent using email or the WWW (World Wide Web).

The SDP text messages include:

- Session name and purpose
- Time the session is active
- Media comprising the session
- Information to receive the media (address etc.)

Protocol Structure

SDP messages are text messages using the ISO 10646 character set in UTF-8 encoding. SDP Session description (optional fields have an *) is:

v= (protocol version)

o= (owner/creator and session identifier).

s= (session name)

i=* (session information)

u=* (URI of description)

e=* (email address)

p=* (phone number)

c=* (connection information - not required if included in all media)

b=* (bandwidth information)

One or more time descriptions (see below)

z=* (time zone adjustments)

k=* (encryption key)

a=* (zero or more session attribute lines)

Zero or more media descriptions (see below)

Time description

t= (time the session is active)

r=* (zero or more repeat times)

Media description

m= (media name and transport address)

i=* (media title)

c=* (connection information - optional if included at session-level)

b=* (bandwidth information)

k=* (encryption key)

a=* (zero or more media attribute lines)

4. Explain in detail about Session Initiation Protocol (11 marks)

Protocol Description

Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and
redirection services, which supports personal mobility – users can maintain a single externally visible identifier regardless of their network location.

SIP supports five facets of establishing and terminating multimedia communications:
User location: determination of the end system to be used for communication;
User availability: determination of the willingness of the called party to engage in communications;
User capabilities: determination of the media and media parameters to be used;
Session setup: "ringing", establishment of session parameters at both called and calling party;
Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

SIP is a component that can be used with other IETF protocols to build a complete multimedia architecture, such as the Real-time Transport Protocol (RTP) for transporting real-time data and providing QoS feedback, the Real-Time streaming protocol (RTSP) for controlling delivery of streaming media, the Media Gateway Control Protocol (MEGACO) for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP) for describing multimedia sessions. Therefore, SIP should be used in conjunction with other protocols in order to provide complete services to the users. However, the basic functionality and operation of SIP does not depend on any of these protocols.

SIP provides a suite of security services, which include denial- of-service prevention, authentication (both user to user and proxy to user), integrity protection, and encryption and privacy services.

SIP works with both IPv4 and IPv6. For Internet telephony sessions, SIP works as follows: Callers and callees are identified by SIP addresses. When making a SIP call, a caller first locates the appropriate server and then sends a SIP request. The most common SIP operation is the invitation. Instead of directly reaching the intended callee, a SIP request may be redirected or may trigger a chain

of new SIP requests by proxies. Users can register their location(s) with SIP servers. SIP addresses (URLs) can be embedded in Web pages and therefore can be integrated as part of such powerful implementations as Click to talk.

Protocol Structure

SIP messages can be transmitted either over TCP or UDP SIP messages are text based and use the ISO 10646 character set in UTF-8 encoding. Lines must be terminated with CRLF. Much of the message syntax and header field are similar to HTTP. Messages can be request messages or response messages.

A request message has the following format:

Method	Request URI	SIP version

• Method – The method to be performed on the resource. Possible methods are Invite, Ack, Options, Bye, Cancel, Register.

• Request-URI - A SIP URL or a general Uniform Resource Identifier; this is the user or service to which this request is being addressed.

• SIP version - The SIP version being used.

The format of the Response message header is shown in the following illustration:

SIP version	Status code	Reason phrase

• SIP version - The SIP version being used.

• Status-code – A 3-digit integer result code of the attempt to understand and satisfy the request.

• Reason-phrase – A textual description of the status code.

5. Explain in detail about Transmission Control Protocol (11 marks)

Protocol Description

Transmission Control Protocol (TCP) is the transport layer protocol in the TCP/IP suite, which provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgment with retransmission of packets when necessary. Along with the Internet Protocol (IP), TCP represents the heart of the Internet protocols.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine and some way to make sure replies get routed to the correct

application on the source computer. This is accomplished through the use of the TCP "port numbers". The combination of IP address of a network station and its port number is known as a "socket" or an "endpoint". TCP establishes connections or virtual circuits between two "endpoints" for reliable communications.

Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because the application does not have to chop data into blocks before handing it off to TCP. TCP can group bytes into segments and pass them to IP for delivery.

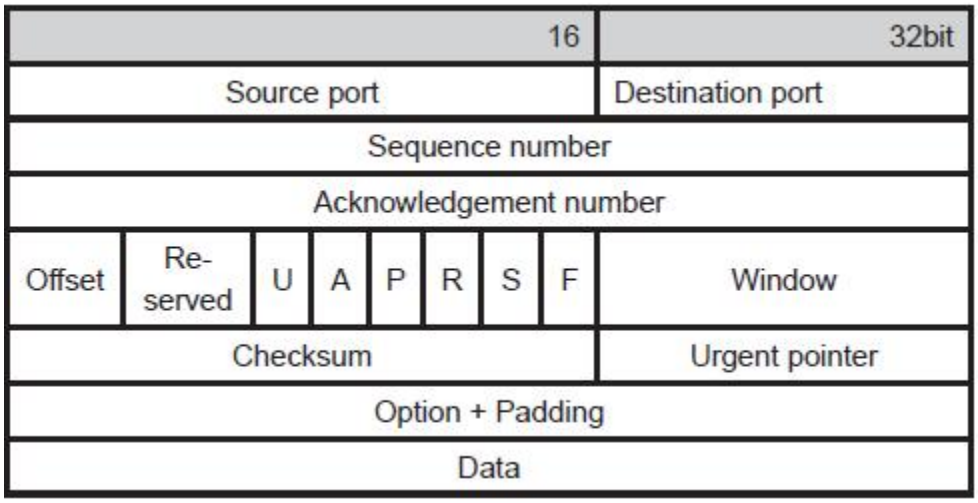
TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

TCP offers efficient flow control - When sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers.

Full-duplex operation: TCP processes can both send and receive packets at the same time.

Multiplexing in TCP: Numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

Protocol Structure



• Source port -- Identifies points at which upper-layer source process receives TCP services.

• Destination port -- Identifies points at which upper-layer Destination process receives TCP services.

• Sequence number -- Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.

• Acknowledgment number – Contains the sequence number of the next byte of data the sender of the packet expects to receive. Once a connection is established, this value is always sent.

• Data offset -- 4 bits. The number of 32-bit words in the TCP header indicates where the data begins.

• Reserved -- 6 bits. Reserved for future use. Must be zero.

• Control bits (Flags) -- 6 bits. Carry a variety of control information. The control bits may be:

U (URG) Urgent pointer field significant.

A (ACK) Acknowledgment field significant.

P (PSH) Push function.

R (RST) Reset the connection.

S (SYN) Synchronize sequence numbers.

F (FIN) No more data from sender.

• Window -- 16 bits. Specifies the size of the sender's receive window, that is, the buffer space available in octets for incoming data.

• Checksum -- 16 bits. Indicates whether the header was damaged in transit.

• Urgent Pointer -- 16 bits. Points to the first urgent data byte in the packet.

• Option + Paddling – Specifies various TCP options. There are two possible formats for an option: a single octet of option type; an octet of option type, an octet of option length and the actual option data octets.

• Data – contains upper-layer information.

6. Explain about User Datagram Protocol (11 marks)

Protocol Description

UDP is a connectionless transport layer (layer 4) protocol in the OSI model which provides a simple and unreliable message service for transaction-oriented services. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine and some way to make sure replies get routed to the correct application on the source computer. This is accomplished through the use of the UDP "port numbers". For example, if a station wished to use a Domain Name System (DNS) on the station 128.1.123.1, it would address the packet to station 128.1.123.1 and insert destination

port number 53 in the UDP header. The source port number identifies the application on the local station that requested domain name server, and all response packets generated by the destination station should be addressed to that port number on the source station. Details of UDP port numbers can be found in the reference.

Unlike TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP.

UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol or application might provide error and flow control.

UDP is the transport protocol for several well-known application layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

Protocol Structure

16	32bit
Source port	Destination port
Length	Checksum
Data	

• Source port – 16 bits. Source port is an optional field. When used, it indicates the port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

• Destination port – 16 bits. Destination port has a meaning within the context of a particular Internet destination address.

• Length – 16 bits. The length in octets of this user datagram, including this header and the data. The minimum value of the length is eight.

• Checksum -- 16-bits The sum of a pseudo header of information from the IP header, the UDP header and the data, padded with zero octets at the end, if necessary, to make a multiple of two octets.

• Data – Contains upper-level data information.

7. Explain by the services offered by TCP? (NOV 2013)

1. Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

2. Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

3. Connection control: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

4. Flow control: Flow control at this layer is performed end to end rather than across a single link.

5. Error control: Error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

8. Write the difference between TCP and UDP?

	TCP	**UDP**
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is	UDP is also a protocol used in message transport or transfer. This is not connection based

	connection based.	which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Examples	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a

	reliability and congestion control.	small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking	UDP does error checking, but no recovery options.
Fields	1. Sequence Number, 2. AcK number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port	1. Length, 2. Source port, 3. Destination port, 4. Check Sum
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)
Checksum	checksum	to detect errors

9. Explain about Reliable Data Protocol (11 marks)

Protocol Description

RDP is a connection-oriented transport protocol designed to efficiently support the bulk transfer of data for such host monitoring and control applications as loading/dumping and remote debugging. It attempts to provide only those services necessary, in order to be efficient in operation and small in size. The key functions of RDP are as follows:

RDP will provide a full-duplex communications channel between the two ports of each transport connection.

RDP will attempt to reliably deliver all user messages and will report a failure to the user if it cannot deliver a message. RDP extends the datagram service of IP to include reliable delivery.

RDP will attempt to detect and discard all damaged and duplicate segments. It will use a checksum and sequence number in each segment header to achieve this goal.

RDP will optionally provide sequenced delivery of segments. Sequenced delivery of segments must be specified when the connection is established.

RDP will acknowledge segments received out of sequence, as they arrive. This will free up resources on the sending side.

RDP supports a much simpler set of functions than TCP. The flow control, buffering, and connection management schemes of RDP are considerably simpler. The goal is a protocol that can be easily and efficiently implemented and that will serve a range of applications.

RDP functions can also be subset to further reduce the size of a particular implementation. For example, a target processor requiring down-loading from another host might implement an RDP module supporting only the passive Open function and a single connection. The module might also choose not to implement out-of-sequence acknowledgements.

Protocol Structure

1	2	3	4	5	6	8	16bit
SYN	ACK	EAK	RST	NUL	0	Ver No	Header Length
Source Port							
Destination Port							
Data Length							
Sequence Number							
Acknowledgement Number							
Checksum							
Variable header area …							

Control flags

The 8 control bits are divided as follows:

SYN	The SYN bit indicates a synchronization segment is present.
ACK	The ACK bit indicates the acknowledgment number in the header is valid.
EACK	The EACK bit indicates an extended acknowledge segment is present.
RST	The RST bit indicates the packet is a reset segment.
NUL	The NUL bit indicates the packet is a null segment.
0	The value of this field must be zero.
Ver no	version number; current version is 2.

Header length -The length of the RDP header.

Source Ports - Source address to identify the processes that originated the communication. The combination of the port identifiers with the source and destination addresses in the network access protocol header serves to fully qualify the connection and constitutes the connection identifier. This permits RDP to distinguish multiple connections between two hosts.

Destination Ports - Destination address to identify the processes targeted in the communication.

Data Length - The length in octets of the data in this segment. The data length does not include the RDP header.

Sequence number - The sequence number of this segment.

Acknowledgement number - If the ACK bit is set in the header, this is the sequence number of the segment that the sender of this segment last received correctly and in sequence. Once a connection is established this should always be sent.

Checksum - The checksum to ensure integrity

Variable Header Area - This area is used to transmit parameters for the SYN and EACK segments.

10. Explain about Reliable User Datagram Protocol (11 marks)

Protocol Description

Reliable UDP (RUDP) is a simple packet based transport protocol, based on RFCs 908 (version 1) and 1151 (version 2), which was intended as a reliable transport protocol to transport telephony signalling across IP networks. RUDP is designed to allow characteristics of each connection to be individually configured so that a number of protocols with different transport requirement can be implemented simultaneously not on the same platform. It is layered on the UDP/IP protocols and provides reliable in-order delivery (up to a maximum number of retransmissions) for virtual connections. RUDP has a very flexible design that makes it suitable for a variety of transport uses. One such use would be to transport telecommunication-signaling protocols.

Reliable UDP is a set of quality of service enhancements, such as congestion control tuning improvements, retransmit, and thinning server algorithms, that improves the ability to present a good quality RTP stream to RTP clients even in the presence of packet loss and network congestion. Reliable UDP's congestion control mechanisms allow streams to behave in a TCP-friendly fashion without disturbing the real-time nature of the protocol.

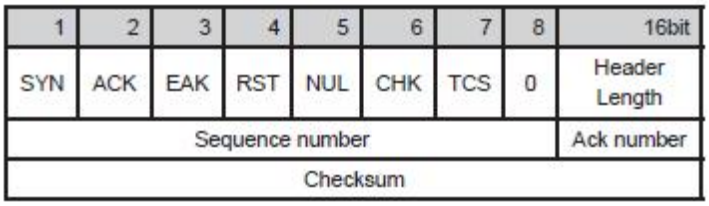
To work well with TCP traffic on the Internet, Reliable UDP uses retransmission and congestion control algorithms similar to the algorithms used by TCP. Additionally, these algorithms are time-tested to utilize available bandwidth optimally.

Reliable UDP features include:

- Client acknowledgment of packets sent by the server to the client
- Windowing and congestion control so the server does not exceed the currently available bandwidth
- Server retransmission to the client in the event of packet loss
- Faster than real-time streaming known as "over buffering".

Protocol Structure

The basic TFTP header structure:



1	2	3	4	5	6	7	8	16bit
SYN	ACK	EAK	RST	NUL	CHK	TCS	0	Header Length
Sequence number								Ack number
Checksum								

Control bits

Indicate what is present in the packet. Details as follows:

SYN	The SYN bit indicates a synchronization segment is present.
ACK	The ACK bit indicates the acknowledgment number in the header is valid.
EACK	The EACK bit indicates an extended acknowledge segment is present.
RST	The RST bit indicates the packet is a reset segment.
NUL	The NUL bit indicates the packet is a null segment.
CHK	The CHK bit indicates whether the Checksum field contains the checksum of just the header or the header and the body (data).
TCS	The TCS bit indicates the packet is a transfer connection state segment.
0	The value of this field must be zero.

Header length - Indicates where user data begins in the packet.

Sequence number - When a connection is first opened, each peer randomly picks an initial sequence number. This sequence number is used in the SYN segments to open the connection.

Each transmitter increments the sequence number before sending a data, null, or reset segment.

Acknowledgement number - This field indicates to a transmitter the last in- sequence packet the receiver has received.

Checksum - The checksum is always calculated on the RUDP header to ensure integrity. The checksum here is the same algorithm used in UDP and TCP headers.

11. Explain the various phases of TCP connection? (7 Marks)(APRIL 2013)

TCP is a heavy weight connection requiring three packets for a socket connection and handles congestion control and reliability. **UDP** is a lightweight transport layer designed atop an IP. There are no tracking connections or ordering of messages.

Method of transfer

TCP reads data as a byte stream and message is transmitted to segment boundaries. **UDP** messages are packets which are sent individually and on arrival are checked for their integrity. Packets have defined boundaries while data stream has none.

A TCP connection is established via a three way handshake, which is a process of initiating and acknowledging a connection. Once the connection is established data transfer can begin. After transmission, the connection is terminated by closing of all established virtual circuits.

UDP uses a simple transmission model without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Unlike TCP, UDP is compatible with packet broadcasts (sending to all on local network) and multicasting (send to all subscribers).

Pondicherry University Questions

2 Marks

1. What is mean by SIP? (UQ APRIL'13) (Ref.Pg.No.2 Qn.No.3)
2. What is UDP**?** (UQ NOV'13) (Ref.Pg.No.4 Qn.No.12)
3. Compare TCP and UDP? (UQ APRIL'13) (Ref.Pg.No.4 Qn.No.14)
4. What is meant by RDP? (UQ NOV'13) (Ref.Pg.No.4 Qn.No.15)

11 Marks

(Regular & Arrear)

1. Write in detail Lightweight Presentation Protocol? (UQ APRIL'13 & NOV '13) (Ref.Pg.No.7 Qn.No.1)

(Regular)

2. Explain by the services offered by TCP? (UQ NOV '13) (Ref.Pg.No.17 Qn.No.7)
3. Explain the various phases of TCP connection? (UQ NOV '13) (Ref.Pg.No.22 Qn.No.11)

SRI VENKATESHWARAA COLLEGE OF ENGINEERING & TECHNOLOGY

(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry.)
13-A, Villupuram – Pondy Main road, Ariyur, Puducherry – 605 102.
Phone: 0413-2644426, Fax: 2644424 / Website: www.svcetpondy.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Subject: NETWORK PROTOCOL **Subject Code: CS E77**

UNIT III

Network Layer Protocols: IP, IPv6, ICMP, ICMPv6, Mobile IP, OSPF, RIP, Multicasting protocols – BGMP, DVMRP, IGMP, and MPLS protocols.

Faculty Incharge **HOD** **PRINCIPAL**

2 MARKS

1. Write about IP

The Internet Protocol (IP) is a network-layer (Layer 3 in the OSI model) protocol that contains addressing information and some control information to enable packets to be routed in a network. IP is the primary network-layer protocol in the TCP/IP protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is equally well suited for both LAN and WAN communications.

2. Write down the responsibilities of IP

IP has two primary responsibilities: providing connectionless, best-effort delivery of datagram's through a network; and providing fragmentation and reassembly of datagram's to support data links with different maximum-transmission unit (MTU) sizes.

3. Draw the Protocol Structure of IP

4	8	16	32bit	
Version	IHL	Type of service	Total length	
Identification			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Option + Padding				
Data				

4. Write about IPv6

IPv6 is the new version of Internet Protocol (IP) based on IPv4, a network-layer (Layer 3) protocol that contains addressing information and some control information enabling packets to be routed in the network. There are two basic IP versions: IPv4 and IPv6. IPv6 is also called next generation IP or IPng. IPv4 and IPv6 are de-multiplexed at the media layer. For example, IPv6 packets are carried over Ethernet with the content type 86DD (hexadecimal) instead of IPv4's 0800. This document describes the IPv6 details. The IPv4 is described in a separate document.

5. Draw the Protocol Structure of IPV6

4	12	16	24	32bit
Version	Priority	Flow label		
Identification			Flags	Fragment offset
Payload length	Next header		Hop limit	
Source address(128 bits)				
Destination address(128 bits)				

6. Write about ICMP & ICMPv6

Internet Control Message Protocol (ICMP) is an integrated part of the IP suite. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-

operation. ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problems. The key ICMP functions are:

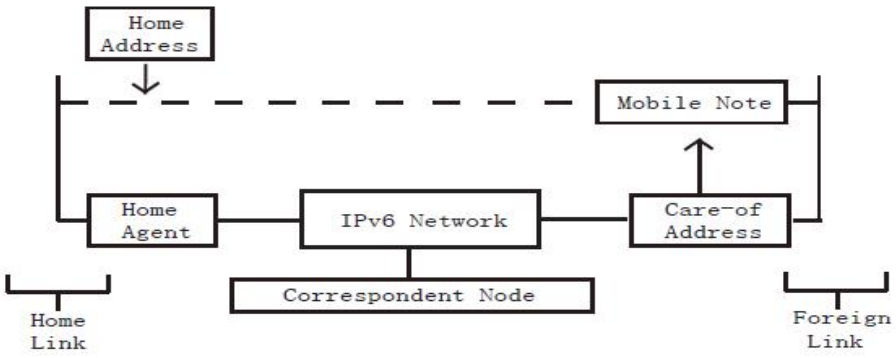
7. Draw the Protocol Structure of ICMP

8	16	32bit
Type	Code	Checksum
Identifier		Sequence number
Address mask		

8. Write about Mobile IP? (NOV 2013)

Mobile IP is the key protocol to enable mobile computing and networking, which brings together two of the world's most powerful technologies, the Internet and mobile communication. In Mobile IP, two IP addresses are provided for each computer: home IP address which is fixed and care-of IP address which is changing as the computer moves. When the mobile moves to a new location, it must send its new address to an agent at home so that the agent can tunnel all communications to its new address timely.

9. Draw the Mobile IP Functional Flow Chart



10. List out the features of mobile IPV4 and Mobile IPV6 (APRIL 2013)

Key Features	Mobile IPv4	Mobile IPv6
Special router as foreign agent –Yes	No	
Support for route optimization	Part of the protocol	In Extensions
Ensure symmetric reachability between mobile nodes and its router at current location	No	Yes
Routing bandwidth overhead	More	Less
Decouple from Link Layer	No	Yes
Need to manage "Tunnel soft state"	Yes	No
Dynamic home agent address discovery	No	Yes

11. Draw the Protocol header Structure of Mobility IPv6

8	16	24	32bit
Next Header	**Length**	**Type**	**Reserved**
Checksum		**Data**	

12. Write about OSPF

Open Shortest Path First (OSPF) is an interior gateway protocol which is used for routing between routers belonging to a single Autonomous System. OSPF uses link-state technology in which routers send each other information about the direct connections and links which they have to other routers. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest- path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multi-path. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated.

13. Draw the Protocol Structure of OSPF

8	16	32bit
Version No.	Packet Type	Packet length
Router ID		
Area ID		
Checksum		AuType
Authentication (64 bits)		

14. Write about RIP

Routing Information Protocol (RIP) is a standard for exchange of routing information among gateways and hosts. This protocol is most useful as an "interior gateway protocol". In a nationwide network such as the current Internet, there are many routing protocols used for the whole network. The network will be organized as a collection of "autonomous systems". Each autonomous system will have its own routing technology, which may well be different for different autonomous systems. The routing protocol used within an autonomous system is referred to as an interior gateway protocol, or "IGP". A separate protocol is used to interface among the autonomous systems. The earliest such protocol, still used in the Internet, is "EGP" (exterior gateway protocol). Such protocols are now usually referred to as inter-AS routing protocols. RIP is designed to work with moderate-size networks using reasonably homogeneous technology. Thus it is suitable as an IGP for many campuses and for regional networks using serial lines whose speeds do not vary widely. It is not intended for use in more complex environments.

15. Draw the Protocol Structure of RIP

8	16	32bit
Command	Version	Unused
Address family identifier		Route tag (only for RIP2; 0 for RIP)
IP address		
Subnet mask (only for RIP2; 0 for RIP)		
Next hop (only for RIP2; 0 for RIP)		
Metric		

16. Write about BGMP

Border Gateway Multicast Protocol (BGMP) is a protocol for inter- domain multicast routing. BGMP natively supports "source specific multicast" (SSM). To also support "any-source multicast" (ASM), BGMP builds shared trees for active multicast groups, and allows domains to build source-specific, inter-domain, distribution branches where needed. Building upon concepts from PIM-SM and CBT, BGMP requires that each global multicast group be associated with a single root. However, in BGMP, the root is an entire exchange or domain, rather than a single router.

17. Draw the Protocol Structure of BGMP

16	24	32bit
Length	Type	Reserved

18. Write about DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is an Internet routing protocol that provides an efficient mechanism for connectionless message multicast to a group of hosts across an internetwork. DVMRP is an "interior gateway protocol" (IGP); suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non-multicast datagram's, so a router that routes both multicast and unicast datagram's must run two separate routing processes.

19. Draw the Protocol Structure of DVMRP

4	8	16	24	32 bit
Version	Type	Sub-type	Checksum	
DVMRP Data stream				

20. Write about IGMP

Internet Group Management Protocol (IGMP), a multicasting protocol in the internet protocols family, is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP messages are encapsulated in IP datagram's, with an IP protocol number of 2. IGMP has versions IGMP v1, v2 and v3.

21. List out the variant protocols of IGMP

- DVMRP: Distance Vector Multicast Routing Protocol.
- IGAP: IGMP for user Authentication Protocol.
- RGMP: Router-port Group Management Protocol.

22. Draw the Protocol Structure of IGMP

8		16		32 bit
Type		Max response time		Checksum
Group address				
RSV	S	QRV	QQIC	Number of source
Source Address (1)				
…				
Source Address (N)				

23. Write about MPLS

Multiprotocol Label Switching (MPLS), architecture for fast packet switching and routing, provides the designation, routing, forwarding and switching of traffic flows through the network. More specifically, it has mechanisms to manage traffic flows of various granularities. It is independent of the layer-2 and layer-3 protocols such as ATM and IP. It provides a means to map IP addresses to simple, fixed-length labels used by different packet forwarding and packet-switching technologies. It interfaces to existing routing and switching protocols, such as IP, ATM, Frame Relay, Resource Reservation Protocol (RSVP) and Open Shortest Path First (OSPF), etc.

24. Draw the MPLS label structure

20	23	24	32 bit
Label	Exp	S	TTL

25. List out the multicast characteristics? (NOV 2013)

- Group Address
- Use of Hardware
- Inter-network Forwarding
- Delivery Semantics
- Membership and Transmission

26. What is multicasting? (APRIL 2013)

Transmission method in which one device communicates with several devices with a single transmission. In contrast to broadcasting (in which a message or signal is sent to all connected devices) a multicast message is transmitted only to the selected device(s). See also narrowcasting and unicasting.

11 MARKS

1. Explain in detail about Internet Protocol in detail?

Protocol Description

The Internet Protocol (IP) is a network-layer (Layer 3 in the OSI model) protocol that contains addressing information and some control information to enable packets to be routed in a network. IP is the primary network-layer protocol in the TCP/IP protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is equally well suited for both LAN and WAN communications.

IP has two primary responsibilities: providing connectionless, best-effort delivery of datagram's through a network; and providing fragmentation and reassembly of datagram's to support data links with different maximum-transmission unit (MTU) sizes. The IP addressing scheme is integral to the process of routing IP datagram's through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks. Each computer (known as a host) on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

All other protocols within the TCP/IP suite, except ARP and RARP, use IP to route frames from host to host. There are two basic IP versions, IPv4 and IPv6. This document describes the IPv4 details. The IPv6 details are described in a separate document.

Protocol Structure

<table>
<tr><td>4</td><td>8</td><td>16</td><td colspan="2">32bit</td></tr>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Option + Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

• Version— 4-bit field indicates the version of IP currently used.

• IP Header Length (IHL) - is the datagram header length in 32-bit words. Points to the beginning of the data. The minimum value for a correct header is 5.

• Type-of-Service— indicates the quality of service desired by specifying how an upper-layer protocol would like a current datagram to be handled, and assigns datagram's various levels of importance. These 8 bits fields are used for the assignment of Precedence, Delay, Throughput and Reliability.

• Total Length—specifies the length, in bytes, of the entire IP packet, including the data and header. The maximum length which can be specified by this field is 65,535 bytes. Typically, hosts are prepared to accept datagram's up to 576 bytes.

• Identification—contains an integer that identifies the current datagram. This field is assigned by sender to help receiver to assemble the datagram fragments.

• Flags - consists of a 3-bit field of which the two low order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

• Fragment Offset - This 13-bits field indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

• Time-to-Live - is a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

• Protocol - indicates which upper-layer protocol receives incoming packets after IP processing is complete.

• Header Checksum—helps ensure IP header integrity. Since some header fields change, e.g., Time to Live, this is recomputed and verified at each point the Internet header is processed.

• Source Address—specifies the sending node.

• Destination Address—specifies the receiving node.

• Options—allows IP to support various options, such as security.

• Data—contains upper-layer information.

2. Explain in detail about Internet Protocol version 6(11 marks)(APRIL 2013)

Protocol Description

IPv6 is the new version of Internet Protocol (IP) based on IPv4, a network-layer (Layer 3) protocol that contains addressing information and some control information enabling packets to be routed in the network. There are two basic IP versions: IPv4 and IPv6. IPv6 is also called next generation IP or IPng. IPv4 and IPv6 are de-multiplexed at the media layer. For example, IPv6 packets are carried over Ethernet with the content type 86DD (hexadecimal) instead of IPv4's 0800. This document describes the IPv6 details. The IPv4 is described in a separate document.

IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes and simpler auto-configuration of addresses. IPv6 addresses are expressed in hexadecimal format (base 16) which allows not only numerals (0-9) but a few characters as well (a-f). A sample ipv6 address looks like:3ffe:ffff:100:f101:210:a4ff:fee3:9566. Scalability of multicast addresses is introduced. A new type of address called an anycast address is also defined, to send a packet to any one of a group of nodes. Two major improvements in IPv6 vs. v4:

• Improved support for extensions and options - IPv6 options are placed in separate headers that are located between the IPv6 header and the transport layer header. Changes in the way IP header options are encoded allow more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future. The extension headers are: Hop-by-Hop Option, Routing (Type 0), Fragment, Destination Option, Authentication, and Encapsulation Payload.

• Flow labeling capability - A new capability has been added to enable the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default Quality of Service or real time service.

Protocol Structure

4	12	16	24	32bit
Version	**Priority**	**Flow label**		
Identification			**Flags**	**Fragment offset**
Payload length	**Next header**		**Hop limit**	
Source address(128 bits)				
Destination address(128 bits)				

• Version – 4-bit Internet Protocol Version number (IPv6 is 6).

• Priority -- 8-bit traffic class field enables a source to identify the desired delivery priority of the packets. Priority values are divided into ranges: traffic where the source provides congestion control and non-congestion control traffic.

• Flow label -- 20-bit flow label is used by a source to label those products for which it requests special handling by the IPv6 router. The flow is uniquely identified by the combination of a source address and a non-zero flow label.

• Payload length -- 16-bit integer in octets is the length of payload including header.

• Next header – 8-bit selector identifies the type of header immediately following the IPv6 header.

• Hop limit -- 8-bit integer that is decremented by one by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero.

• Source address -- 128-bit address of the originator of the packet.

• Destination address -- 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

3. Explain in detail about Internet Message Control Protocol and ICMP version 6(6marks) (NOV 2013)

Protocol Description

Internet Control Message Protocol (ICMP) is an integrated part of the IP suite. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation. ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problems. The key ICMP functions are:

• Announce network errors, such as a host or entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.

• Announce network congestion. When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP Source Quench messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed. Of course, generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.

• Assist Troubleshooting. ICMP supports an Echo function, which just sends a packet on a round--trip between two hosts. Ping, a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round--trip times and computing loss percentages.

• Announce Timeouts. If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact. Trace Route is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements. The Internet Control Message Protocol (ICMP) was revised during the definition of IPv6. In addition, the multicast control functions of the IPv4 Group Membership Protocol (IGMP) are now incorporated in the ICMPv6.

Protocol Structure

8	16	32bit
Type	**Code**	**Checksum**
Identifier		**Sequence number**
Address mask		

• Type -- Messages can be error or informational messages. Error messages can be Destination unreachable, Packet too big, Time exceed, Parameter problem. The possible informational messages are, Echo Request, Echo Reply, Group Membership Query, Group Membership Report, and Group Membership Reduction.

• Code -- For each type of message several different codes are defined. An example of this is the Destination Unreachable message, where possible messages are: no route to destination, communication with destination administratively prohibited, not a neighbor, address unreachable, port unreachable. For further details, refer to the standard.

• Checksum -- The 16-bit one's complement of the one's complement sum of the ICMP message starting with the ICMP Type. For computing the checksum, the checksum field should be zero.

• Identifier -- An identifier to aid in matching requests/ replies; may be zero.

• Sequence number -- Sequence number to aid in matching requests/replies; may be zero.

• Address mask -- A 32-bit mask.

4. Write in detail IP Mobility Support Protocol for IPv4 & IPv6 (6 marks)

Protocol Description

Mobile IP is the key protocol to enable mobile computing and networking, which brings together two of the world's most powerful technologies, the Internet and mobile communication. In Mobile IP, two IP addresses are provided for each computer: home IP address which is fixed and care-of IP address which is changing as the computer moves. When the mobile moves to a new location, it must send its new address to an agent at home so that the agent can tunnel all communications to its new address timely.

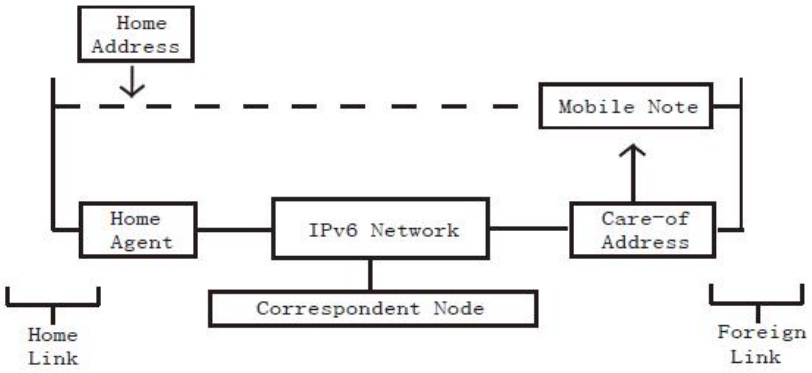
The main components defined in the Mobile IPv6 architecture are shown as follows:

Mobile node – A mobile unit that can change links, and therefore addresses, and maintain reach ability using its home address.

- Home link - The link from which the mobile node originates.
- Home address - An address assigned to the mobile node when it is attached to the home link and through which the mobile node is always reachable, regardless of its location on an IPv6 network.
- Home agent - A router on the home link that maintains registrations of mobile nodes that are away from home and their current addresses.
- Foreign link - A link that is not the mobile node's home link.
- Care-of address - An address used by a mobile node while it is attached to a foreign link. The association of a home address with a care-of address for a mobile node is known as a binding.
- Correspondent node A node that communicates with a mobile node. A correspondent node does not have to be Mobile IPv6-capable.

There are two versions of Mobile IP: Mobile IP for IPv4 and IPv6.

The major differences are summarized as follows:



Mobile IP Functional Flow Chart

Key Features	Mobile IPv4	Mobile IPv6
Special router as foreign agent –Yes	No	
Support for route optimization	Part of the protocol	In Extensions
Ensure symmetric reachability between mobile nodes and its router at current location	No	Yes
Routing bandwidth overhead	More	Less
Decouple from Link Layer	No	Yes
Need to manage "Tunnel soft state"	Yes	No
Dynamic home agent address discovery	No	Yes

Protocol Structure

Mobility IPv6 Protocol header structure:

8	**16**	**24**	**32bit**
Next Header	**Length**	**Type**	**Reserved**
Checksum		**Data**	

Next Header - Identifies the protocol following this header.
Length - 8 bits unsigned. Size of the header in units of 8 bytes excluding the first 8 bytes.
Type - Mobility message types.

Type	Description
0	BRR, Binding Refresh Request.
1	HoTI, Home Test Init.
2	CoTI, Care-of Test Init.
3	HoT, Home Test.
4	CoT, Care-of Test.
5	BU, Binding Update.
6	Binding Acknowledgement.
7	BE, Binding Error.

Reserved - MUST be cleared to zero by the sender and MUST be ignored by the receiver.
Checksum - The 16 bit one's complement checksum of the Mobility Header.

Data - Variable length.

5. Write in detail Open Shortest Path First protocol (11 marks)

Protocol Description

Open Shortest Path First (OSPF) is an interior gateway protocol which is used for routing between routers belonging to a single Autonomous System. OSPF uses link-state technology in which routers send each other information about the direct connections and links which they have to other routers. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest- path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multi-path. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated.

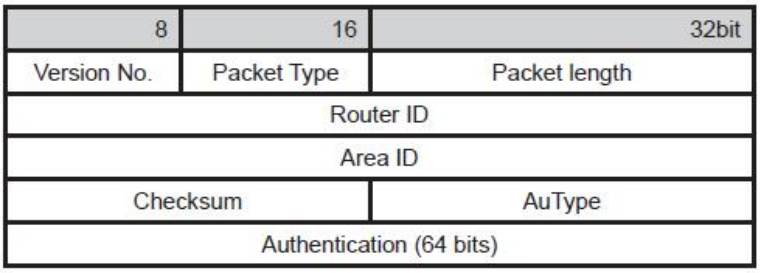
OSPF has been designed expressly for the TCP/IP internet environment, including explicit support for CIDR and the tagging of externally-derived routing information. OSPF also provides for the authentication of routing updates and utilizes IP multicast when sending/receiving the updates.

OSPF routes IP packets based solely on the destination IP address found in the IP packet header. IP packets are routed "as is"; they are not encapsulated in any further protocol headers as they transit the Autonomous System.

OSPF allows sets of networks to be grouped together. Such a grouping is called an area. The topology of an area is hidden from the rest of the Autonomous System. This information hiding enables a significant reduction in routing traffic. Also, routing within the area is determined only by the area's own topology, lending the area protection from bad routing data.

OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different sizes (i.e., different masks). This is commonly referred to as variable length subnetting. A packet is routed to the best (i.e., longest or most specific) match.

Protocol Structure



- Version number - Protocol version number (currently 2).
- Packet type - Valid types are as follows:
  - 1 Hello
  - 2 Database Descriptions
  - 3 Link State Request
  - 4 Link State Update
  - 5 Link State Acknowledgments.
- Packet length - The length of the protocol packet in bytes. This length includes the standard OSPF header.
- Router ID - The router ID of the packet's source. In OSPF, the source and destination of a routing protocol packet are the two ends of a (potential) adjacency.

• Area ID - identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Most travel a single hop only.

• Checksum - The standard IP checksum of the entire contents of the packet, starting with the OSPF packet header but excluding the 64-bit authentication field.

• AuType - Identifies the authentication scheme to be used for the packet.

• Authentication - A 64-bit field for use by the authentication scheme.

6. Write in detail Routing Information Protocol (6 marks)

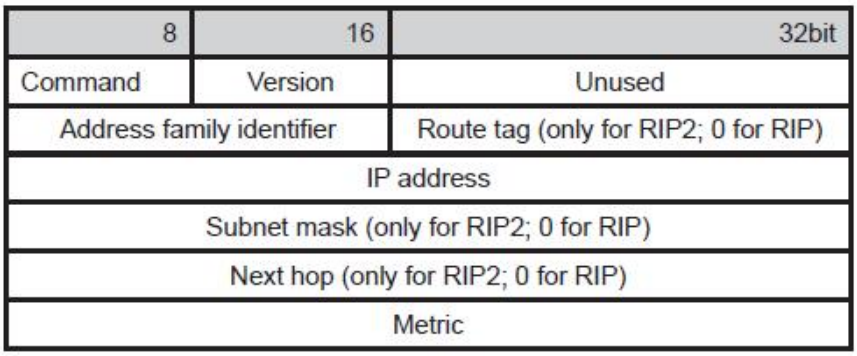
Protocol Description

Routing Information Protocol (RIP) is a standard for exchange of routing information among gateways and hosts. This protocol is most useful as an "interior gateway protocol". In a nationwide network such as the current Internet, there are many routing protocols used for the whole network. The network will be organized as a collection of "autonomous systems". Each autonomous system will have its own routing technology, which may well be different for different autonomous systems. The routing protocol used within an autonomous system is referred to as an interior gateway protocol, or "IGP". A separate protocol is used to interface among the autonomous systems. The earliest such protocol, still used in the Internet, is "EGP" (exterior gateway protocol). Such protocols are now usually referred to as inter-AS routing protocols. RIP is designed to work with moderate-size networks using reasonably homogeneous technology. Thus it is suitable as an IGP for many campuses and for regional networks using serial lines whose speeds do not vary widely. It is not intended for use in more complex environments.

RIP2, derives from RIP, is an extension of the Routing Information Protocol (RIP) intended to expand the amount of useful information carried in the RIP2 messages and to add a measure of security. RIP2 is a UDP-based protocol. Each host that uses RIP2 has a routing process that sends and receives datagram's on UDP port number 520.

RIP and RIP2 are for the IPv4 network while the RIPng is designed for the IPv6 network. In this document, the details of RIP and RIP2 will be described.

Protocol Structure



8	16	32bit
Command	Version	Unused
Address family identifier		Route tag (only for RIP2; 0 for RIP)
IP address		
Subnet mask (only for RIP2; 0 for RIP)		
Next hop (only for RIP2; 0 for RIP)		
Metric		

- Command -- The command field is used to specify the purpose of the datagram. There are five commands: Request, Response, Trace on (obsolete), Trace off (Obsolete) and Reserved.
- Version -- The RIP version number. The current version is 2.
- Address family identifier -- Indicates what type of address is specified in this particular entry. This is used because RIP2 may carry routing information for several different protocols. The address family identifier for IP is 2.
- Route tag -- Attribute assigned to a route which must be preserved and readvertised with a route. The route tag provides a method of separating internal RIP routes (routes for networks

within the RIP routing domain) from external RIP routes, which may have been imported from an EGP or another IGP.

- IP address -- The destination IP address.
- Subnet mask -- Value applied to the IP address to yield the non-host portion of the address. If zero, then no subnet mask has been included for this entry.
- Next hop -- Immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded.
- Metric -- Represents the total cost of getting a datagram from the host to that destination. This metric is the sum of the costs associated with the networks that would be traversed in getting to the destination.

7. Explain about Border Gateway Multicast Protocol (6 marks)

Protocol Description

Border Gateway Multicast Protocol (BGMP) is a protocol for inter- domain multicast routing. BGMP natively supports "source specific multicast" (SSM). To also support "any-source multicast" (ASM), BGMP builds shared trees for active multicast groups, and allows domains to build source-specific, inter-domain, distribution branches where needed. Building upon concepts from PIM-SM and CBT, BGMP requires that each global multicast group be associated with a single root. However, in BGMP, the root is an entire exchange or domain, rather than a single router.

For non-source-specific groups, BGMP assumes that ranges of the multicast address space have been associated with selected domains. Each such domain then becomes the root of the shared domain-trees for all groups in its range. An address allocator will generally achieve better distribution trees if it takes its multicast addresses from its own domain's part of the space, thereby causing the root domain to be local.

BGMP uses TCP as its transport protocol. This eliminates the need to implement message fragmentation, retransmission, acknowledgement, and sequencing. BGMP uses TCP port 264 for establishing its connections. This port is distinct from BGP's port to provide protocol independence, and to facilitate distinguishing between protocol packets.

Two BGMP peers form a TCP connection between one another, and exchange messages to open and confirm the connection parameters. They then send incremental Join/Prune Updates as group memberships change. BGMP does not require periodic refresh of individual entries. KeepAlive messages are sent periodically to ensure the liveness of the connection. Notification messages are sent in response to errors or special conditions. If a connection encounters an error condition, a notification message is sent and the connection is closed if the error is a fatal one.

Protocol Structure

16	24	32bit
Length	Type	Reserved

• Length - The total length of the message including the header in octets. It allows one to locate in the transport-level stream the start of the next message.

• Type - The type code of the message. The following type codes are available:

1 OPEN; 2 UPDATE; 3 NOTIFICATIONS; 4 KEEPALIVE

After a transport protocol connection is established, the first message sent by each side is an OPEN message. If the OPEN message is acceptable, a KEEPALIVE message confirming the OPEN is sent back. Once the OPEN is confirmed, UPDATE, KEEPALIVE, and NOTIFICATION messages may be exchanged.

The format of each message type is different.

8. Explain about Distance Vector Multicast Routing Protocol (11 marks)

Protocol Description

Distance Vector Multicast Routing Protocol (DVMRP) is an Internet routing protocol that provides an efficient mechanism for connectionless message multicast to a group of hosts across an internetwork. DVMRP is an "interior gateway protocol" (IGP); suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non-multicast datagram's, so a router that routes both multicast and unicast datagram's must run two separate routing processes.

DVMRP is developed based upon RIP. DVMRP combines many of the features of RIP with the Truncated Reverse Path Broadcasting (TRPB) algorithm. In addition, to allow experiments to traverse networks that do not support multicasting, a mechanism called tunneling was developed. The key differences of DVMRP from RIP are: RIP routes and forwards datagram's to a particular destination. The purpose of DVMRP is to keep track of
the return paths to the source of multicast datagrams.

DVMRP packets are encapsulated in IP datagram's, with an IP protocol number of 2 (IGMP).

Protocol Structure

DVMRP uses the IGMP to exchange routing diagrams. DVMRP data grams are composed of two portions: a small, fixed length IGMP header, and a stream of tagged data.

4	8	16	24	32 bit
Version	Type	Sub-type	Checksum	
DVMRP Data stream				

- Version – It is 1.
- Type – DVMRP type is 3.
- Sub-type - The subtype is one of:
  1 = Response; the message provides routes to some destination(s).
  2 = Request; the message requests routes to some destination(s).
  3 = Non-membership report; the message provides non-membership report(s).
  4 = Non-membership cancellation; the message cancels previous non-membership report(s).
- Checksum -- One's complement of the one's complement sum of the DVMRP message. The checksum must be calculated upon transmission and must be validated on reception of a packet. The checksum of the DVMRP message should be calculated with the checksum field set to zero.

9. **Explain about Internet Group Management Protocol (11 marks) (NOV 2013)**

Protocol Description

Internet Group Management Protocol (IGMP), a multicasting protocol in the internet protocols family, is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP messages are encapsulated in IP data grams, with an IP protocol number of 2. IGMP has versions IGMP v1, v2 and v3.

- IGMPv1: Hosts can join multicast groups. There are no leave messages. Routers use a time-out based mechanism to discover the groups that are of no interest to the members.

• IGMPv2: Leave messages were added to the protocol, allowing group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.

• IGMPv3: A major revision of the protocol allows hosts to specify the list of hosts from which they want to receive traffic. Traffic from other hosts is blocked inside the network. It also allows hosts to block inside the network packets that come from sources that send unwanted traffic.

The variant protocols of IGMP are:

• DVMRP: Distance Vector Multicast Routing Protocol.
• IGAP: IGMP for user Authentication Protocol.
• RGMP: Router-port Group Management Protocol.

Protocol Structure

There are basically 5 types of messages that must be implemented for IGMP v3 to function properly and be compatible with previous versions:

0x11: membership query
0x22: version 3 membership report
0x12: version 1 membership report
0x16: version 2 membership report
0x17: version 2 leave group

As an example, the message format for 0x11 (membership query) is displayed:

8		16		32 bit
Type		Max response time		Checksum
Group address				
RSV	S	QRV	QQIC	Number of source
Source Address (1)				
…				
Source Address (N)				

• Type -- The message type: 0x11 (Membership query).

• Max Response Time -- Used only in Membership query messages. Specifies the maximum time allowed, in units of 1/10 second, before sending a responding report. In all other messages, it is set to 0 by the sender and ignored by the receiver.

• Checksum -- The checksum for message errors

• Group Address -- The Group address is set to 0 when sending a general query. It is set to the group address being queried, when sending a group specific query or group-and-source-specific query. In a membership report of a leave group message, it holds the IP multicast group address of the group being reported or left.

• RSV – Reserved; Set to zero on transmission, and ignored on reception.
• QQIC – Querier's Query Interval Code
• Number of Source (N) -- The number of source addresses in this message.
• Source Address – The vector of the IP unicast address.

10. Explain in detail about Multiprotocol Label switching (11 marks)

Protocol Description

Multiprotocol Label Switching (MPLS), architecture for fast packet switching and routing, provides the designation, routing, forwarding and switching of traffic flows through the network. More specifically, it has mechanisms to manage traffic flows of various granularities. It is independent of the layer-2 and layer-3 protocols such as ATM and IP. It provides a means to map IP addresses to simple, fixed-length labels used by different packet forwarding and packet-switching technologies. It interfaces to existing routing and switching protocols, such as IP, ATM, Frame Relay, Resource Reservation Protocol (RSVP) and Open Shortest Path First (OSPF), etc.

In MPLS, data transmission occurs on Label-Switched Paths (LSPs). LSPs are a sequence of labels at each and every node along the path from the source to the destination. There are several label distribution protocols used today, such as Label Distribution Protocol (LDP) or RSVP or piggybacking on routing protocols like border gateway protocol (BGP) and OSPF. High speed switching of data is possible because the fixed-length labels are inserted at the very beginning of the packet or cell and can be used by hardware to switch packets quickly between
links.

MPLS is designed to address network problems such as networks- speed, scalability, quality-of-service (QoS) management, and traffic engineering. MPLS has also become a solution to the bandwidth-management and service requirements for next-generation IP-based backbone networks.

Protocol Structure

MPLS label structure:

20	23	24	32 bit
Label	Exp	S	TTL

• Label - Label Value carries the actual value of the Label. When a labeled packet is received, the label value at the top of the stack is looked up and the system learns:

a) the next hop to which the packet is to be forwarded;

b) the operation to be performed on the label stack before forwarding; this operation may be to replace the top label stack entry with another, or to pop an entry off the label stack, or to replace the top label stack entry and then to push one or more additional entries on the label stack.

• Exp - Experimental Use: Reserved for experimental use.

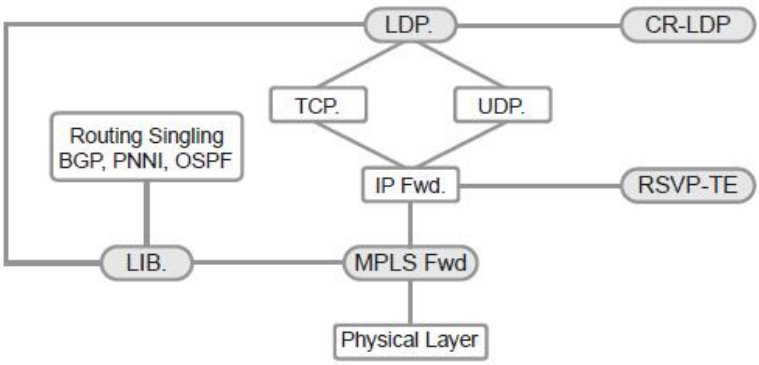
• S - Bottom of Stack: This bit is set to one for the last entry in the label stack, and zero for all other label stack entries

• TTL - Time to Live field is used to encode a time-to live value.

The MPLS architecture protocol family includes:

• MPLS related Signaling Protocols such as OSPF, BGP, ATM PNNI, etc.
• LDP: Label Distribution Protocol.
• CR-LDP: Constraint-Based LDP
• RSVP-TE: Resource Reservation Protocol – Traffic Engineering

The following figure depicts the MPLS protocol stack architecture:



11. Define OSPF and explain the function of OSPF header? (APRIL 2013)

- Two tier hierarchical design
- Dijkstra's algorithm – shortest path first
  - Used to calculate best paths to destinations
  - Based on link state database
  - Each router in OSPF runs SPF itself
- OSPF neighbor table – Adjacency Database
- OSPF topology table – OSPF topology DB – LSDB
- Routing table – Forwarding DB
- Two area types
  - Transit – backbone – area 0
  - Regular – user access – all other areas
  - All regular areas must connect to area 0
  - Areas minimize routing tables
  - Localize impact of topology changes
  - Stop detailed LSA floods at area boundaries
- ABR – area backbone router
  - Functions as default route or default path out of area
  - Separates LSA flood zones
  - Connects multiple areas
- DR/BDR – designated router / backup designated router
  - Multicast address for DR/BDR 224.0.0.6
  - All other routers on network form adjacency with DR/BDR
  - LSA's are only exchanged with these two
  - All other routers called DROTHERs
  - Elected by highest priority (default priority is 1)
    - Priority zero cannot be elected DR/BDR
      - Ip ospf priority **{#}** interface command
    - Changing DR/BDR priority to zero takes effect immediately
    - Changing priority on DROTHER to something else has no effect until re-election
    - If tie in priority, highest router-ID (active IP interface) is used to break tie
  - Any new routers brought onto the network will form full adjacency with dr/bdr and two way state with other neighbors.
  - Changing priority to zero on a DR/BDR will take effect immediately.
- ASBR

- Connects the OSPF AS to an outside AS
- Redistribution point

- Five OSPF Packet types
  - Hello – discover and building adjacency
    - Hello packets are sent every 10 seconds on multi access networks
    - Dead interval is 4 times hello interval
  - Database description – DBD/DDP – checks for db synchronization
  - Link-state request – requests specific link-state records
  - Link-state update – response to LSR
  - Link-state ack – acknowledges other packet types
- Operational States
  - Down
  - Init state – routers multicast initial hello (224.0.0.5)
  - Two way – routers send unicast hellos listing neighbors
  - Exstart – master/slave relationship established with DR/BDR
  - Exchange – DDPs are exchanged
  - Loading – LSRs for specific networks
  - Full – all LSDBs are synchronized with DR/BDR. Routers are able to route traffic
- Communication
  - 224.0.0.5 multicast to everyone
  - 224.0.0.6 multicast to DR/BDR
  - LSAcks are sent unicast
  - LSDB summaries are multicast every 30 minutes
    - Entries have a max life of 60 minutes
  - 32 bit sequence numbers are used for link-state advertisements
    - The sequence number can be seen with the "show ip ospf database" command
  - Loopback interfaces are recommended for stability and RID
    - RID can be manually set using **router-id** router configuration command
      - If RID was set with loopback, a router reboot is required for the **router-id** command to take effect
      - If RID was set with **router-id** command, it can be changed with "clear ip ospf process" command
- Network Types
  - Point to Point
    - Multicast 224.0.0.5 to discover neighbors
    - No DR/BDR
    - ip unnumbered is possible over point to point links
    - 10/40 hello/dead interval
  - Broadcast
    - DR/BDR are the central point of contact in the network
  - Non broadcast multi-access
    - By default, OSPF cannot form neighbor adjacencies
    - DR/BDR elections become crucial
      - Hub/spoke, not all spoke sites can communicate directly
    - Three topologies
      - Full mesh – costly, requires separate VC's for connectivity between each site
      - Partial mesh
      - Star – hub/spoke
    - Modes of operation

- **Ip ospf network {mode}** interface command
- Broadcast – Cisco Proprietary
  - WAN links are treated like LAN interfaces
  - Multicast hello for discover
  - Full/partial mesh
- Non broadcast – RFC Compliant
  - One IP subnet for all spokes
  - Neighbors are manually configured
  - DR/BDR is also manually rigged/configured to insure connectivity to DR
- Point to multi-point – RFC Compliant
  - Multicast hello for discover
  - No DR/BDR (requires additional LSAs)
  - Mesh/star
- point to multi-point non broadcast – Cisco Proprietary
  - Used in place of P2MP where broadcasts and multicast are disabled
  - Neighbors are manually configured
- point to point – Cisco Proprietary
  - Different IP subnet on each interface
  - No DR/BDR elected or needed
  - LAN or WAN interface
- Default Modes
  - Point to point FR – point to point mode
  - Multipoint FR (sub interfaces) – non broadcast
  - main FR interface – non broadcast
- NB mode neighbor configuration
  - Neighbor {ip} priority {# default 0} poll-interval {#} cost {1-65535} database-filter all

mode	prefer topo	subnet	hello timer	adjacency	RFC	example
bcast	Full/partial	Same	10 sec	Auto DR	Cisco	LAN
non bcast	Full/partial	Same	30 sec	Manual DR	RFC	FR
p2mp	Partial/star	Same	30 sec	Auto no DR	RFC	FR bcast
p2mp nb	Partial/star	Same	30 sec	Manual	Cisco	FR nbcast
p2p	Partial/star	Diff	10 sec	Auto no DR	Cisco	serial/sub

- LSA Types
  - Router LSA – type 1
    - IntraArea LSA generated by every router in the area. Advertises link states. The LSID = RID of originator
  - Network LSA – type 2
    - Network LSA generated for Multiaccess networks
    - Generated by DR – LSID = RID of DR
  - Summary LSA – type 3

        - Summary advertisements generated by ABR
        - Summarizes type 1 LSAs from one area to another
        - Describes routes to area's networks (aggregate routes)
        - LSID = destination network #
        - Not flooded to stubby, totally stubby, or not so stubby areas
        - Routes are NOT automatically summarized
    - Summary LSA – type 4
        - Generated by ABR to advertise the presence of an ASBR. ASBR sends type 1 with e-bit set to ID itself
        - Routes to ASBR
        - LSID = RID of describe ASBR
        - Not flooded to stubby, totally stubby, or not so stubby areas
        - Routes are NOT automatically summarized
    - AS External LSA – type 5
        - Generated by ASBRs to advertise external networks and autonomous systems. LSID = external network #
        - Contains all routes separately, unless manually summarized
        - ABRs pass type 5 LSAs on to the rest of the AS
    - Multicast OSPF LSA – type 6
    - NSSA External LSA – type 7
        - ASBR in a stubby area that needs to pass external routes back into the AS. Stubby area needs to be reclassified as NSSA to allow those routes.
        - ABR receives type 7 LSAs and forwards them as type 5 to the rest of the AS
    - External LSA for BGP – type 8
- Cost/Metric
    - 100mbps/link speed = cost
        - Example 100mbps interface has cost 1
        - Unfortunately, 1000mbps interface also has cost 1
            - **Auto-cost reference-bandwidth {ref bw}** interface command to change this behavior
        - **bandwidth {value}** interface command to define actual bandwidth
        - **ip ospf cost {value}** interface command
- Route summarization
    - Occurs at ABRs, relies on contiguous IP design
    - **Area # range {addr | mask} advertise/not-advertise cost {#}**
    - Router will create a summarized route to null 0
    - ASBR Summarization
        - **Summary-address {addr | mask } *tag*** router config command
- Default route
    - **Default-information originate *always* metric {value}**
    - Per Cisco, default metric of 10.
- OSPF Area Types
    - Standard Area
        - Accepts link updates, route summaries, and external routes
    - Stub Area
        - Blocks type 5 LSAs. No routes external to the AS. If stubs need to connect to external AS, they use default routes.
    - Totally Stubby Area
        - Blocks type 3, 4, and 5 LSAs. No external AS, no summary routes. Uses default route for everything outside of the local area.

- Not So Stubby Area
  - Acts like a stub/tsa but allows ASBR connected to it
  - ASBR in an NSSA generates type 7 LSA
  - ABR to NSSA translates Type 7 to Type 5 before passing along to the rest of the AS
  - Routes from Type 7 LSA show in routing table as O N1 or O N2 (type 2 is default)
- Stub/TSA/NSSA configuration
  - **Area # stub** router configuration command on all routers in area
  - **Area # stub *no-summary*** router configuration command on ABR for TSA
  - **area # nssa *no-summary***
- Virtual Links
  - Allow extension of Area 0 through another area
  - **Area # virtual-link *RID*** where RID is the RID of the neighbor on the other side of the VL
  - **sho ip ospf virtual-links**
- Helpful commands
  - **Sho ip ospf neighbor**
  - **Sho ip ospf database**
  - **Sho ip ospf adj** this is ADJ, not adjacency!!!!!!

Pondicherry University Questions

2 Marks

1. Write about Mobile IP?(UQ NOV 2013) (Ref.Pg.No.3 Qn.No.8)
2. List out the features of mobile IPV4 and Mobile IPV6 (UQ April 2013) (Ref.Pg.No.3 Qn.No.10)
3. List out the multicast characteristics?(UQ NOV 2013) (Ref.Pg.No.6 Qn.No.25)
4. What is multicasting?(UQ April 2013) (Ref.Pg.No.6 Qn.No.26)

11 Marks

(Regular)

1. Explain in detail about Internet Message Control Protocol and ICMP version 6?(UQ NOV 2013) (Ref.Pg.No.9 Qn.No.03)
2. Explain about Internet Group Management Protocol ?(UQ NOV 2013) (Ref.Pg.No.15 Qn.No.9)

(Arrear)

3. Explain in detail about Internet Protocol version 6?(UQ APRIL 2013) (Ref.Pg.No.8 Qn.No.2)
4. Define OSPF and explain the function of OSPF header? (UQ APRIL 2013) (Ref.Pg.No.18 Qn.No.11)

SRI VENKATESHWARAA COLLEGE OF ENGINEERING & TECHNOLOGY
(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry.)
13-A, Villupuram – Pondy Main road, Ariyur, Puducherry – 605 102.
Phone: 0413-2644426, Fax: 2644424 / Website: www.svcetpondy.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Subject: NETWORK PROTOCOL **Subject Code: CS E77**

UNIT IV

Data Link Layer Protocols: ARP, IPCP, RARP, SLIP, IEEE 802.3, IEEE 802.5, IEEE 802.11, FDDI, ISDN, xDSL, PPP, LCP, HDLC, PNNI – LANE – SONET/SDH Protocols..

Faculty Incharge **HOD** **PRINCIPAL**

2 MARKS

1. Define ARP?

Address Resolution Protocol (ARP) performs mapping of an IP address to a physical machine address (MAC address for Ethernet) that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the rules for making this correlation and providing address conversion in both directions.

2. Write a Protocol Structure for Address Resolution Protocol?

ARP and In ARP have the same structure:

<table>
<tr><th colspan="2">16</th><th>32 bit</th></tr>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>HLen</td><td>PLen</td><td>Operation</td></tr>
<tr><td colspan="3">Sender Hardware address</td></tr>
<tr><td colspan="3">Sender Protocol Address</td></tr>
<tr><td colspan="3">Target Hardware Address</td></tr>
<tr><td colspan="3">Target Protocol Address</td></tr>
</table>

- Hardware type - Specifies a hardware interface type for which the sender requires a response.
- Protocol type - Specifies the type of high-level protocol address the sender has supplied.
- HLen - Hardware address length.
- PLen - Protocol address length.
- Operation - The values are as follows:
  1. ARP request.
  2. ARP response.
  3. RARP request.
  4. RARP response.
  5. Dynamic RARP request.
  6. Dynamic RARP reply.
  7. Dynamic RARP error.
  8. InARP request.
  9. InARP reply.
- Sender hardware address -HLen bytes in length.
- Sender protocol address - PLen bytes in length.
- Target hardware address - HLen bytes in length.
- Target protocol address - PLen bytes in length.

3. Define IPCP?

IP Control Protocol (IPCP) and IPv6 Control Protocol (IPv6CP) define the Network Control Protocol for establishing and configuring the Internet Protocol or IPv6 over PPP, and a method to negotiate and use Van Jacobson TCP/IP header compression with PPP.

IPCP is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of the point-to-point link. IPCP uses the same packet exchange mechanism as the Link Control Protocol

(LCP). IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPCP packets received before this phase is reached should be silently discarded.

4. Define IPv6CP?

IPv6CP is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPv6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPv6CP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPv6CP packets received before this phase is reached should be silently discarded.

5. Draw a Protocol Structure for IPCP and IPv6CP?

IPCP and IPv6CP configuration option packet header:

8	16	32 bit
Type	Length	Configuration option

- Type – 1 for IP-Address, 2 for IP-Compression Protocol, and 3 for IP-Address
- Length >= 4
- Configuration Option - The field is two octets and indicates one of the following options:

For IPCP:
Type 1: IP-Addresses
Type 2: IP-Compression Protocol
Type 3: IP-Address.

For IPv6CP:
Type 1: Interface – Identifier
Type 2: IPv6-Compression Protocol

IPCP and IPv6CP header structure:

8	16	32 bit
Code	Identifier	Length
Data(variable)		

- Code - Specifies the function to be performed.
- Identifier - Used to match requests and replies.
- Length - Size of the packet including the header.
- Data -Zero or more bytes of data as indicated by the Length. This field may contain one or more Options.

6. Expand the term RARP?

Reverse Address Resolution Protocol (RARP) allows a physical machine in a local area network to request its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machines' (or Media Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests its IP address from the RARP server on the router. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use. RARP is available for Ethernet, Fiber Distributed-Data Interface, and Token Ring LANs.

7. Draw a Protocol Structure

The protocol header for RARP is the same as for ARP:

16		32 bit
Hardware type		Protocol type
HLen	PLen	Operation
Sender Hardware address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

- Hardware type - Specifies a hardware interface type for which the sender requires a response.
- Protocol type - Specifies the type of high-level protocol address the sender has supplied.
- Hlen - Hardware address length.
- Plen - Protocol address length.
- Sender hardware address -HLen bytes in length.
- Sender protocol address - PLen bytes in length.
- Target hardware address - HLen bytes in length.
- Target protocol address - PLen bytes in length.

8. Define SLIP?

Serial Line IP (SLIP) is used for point-to-point serial connections running TCP/IP. SLIP is commonly used on dedicated serial links and sometimes for dialup purposes, and is usually used with line speeds between 1200bps and 19.2Kbps. SLIP is useful for allowing mixes of hosts and routers to communicate with one another (host-host, host-router and router-router are all common SLIP network configurations).

9. Write a packet framing protocol?

SLIP defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection/correction or compression mechanisms.

10. Defines two special characters for The SLIP protocol?

The SLIP protocol defines two special characters: END and ESC. END is octal 300 (decimal 192) and ESC is octal 333 (decimal 219). To send a packet, a SLIP host simply starts sending the data in the packet. If a data byte is the same code as the END character, a two byte sequence of ESC and octal 334 (decimal 220) is sent instead. If it the same as an ESC character, a two byte sequence of ESC and octal 335 (decimal 221) is sent instead. When the last byte in the packet has been sent, an END character is then transmitted.

11. Expand the term CSLIP?

Compressed Serial Line IP (CSLIP) performs the Van Jacobson header compression on outgoing IP packets. This compression improves throughput for interactive sessions noticeably.
Today, SLIP is largely replaced by the Point–to-Point Protocol (PPP), which is more features rich and flexible.

12. What is Ethernet?

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

13. Explain the two modes of operation in Ethernet?

There are two modes of operation: half-duplex and full-duplex.

14. Explain the MAC sublayer has two primary responsibilities?

- Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception
- Media access control, including initiation of frame transmission and recovery from transmission failure

15. Draw a protocol Structure IEEE 802.3?

The basic IEEE 802.3 MAC Data Frame for 10/100Mbps Ethernet:

7	1	6	6	2	46-1500bytes	4bytes
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS

- Preamble (Pre) — 7 bytes. The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.
- Start-of-frame delimiter (SFD)—1 byte. The SOF is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.
- Destination address (DA) — 6 bytes. The DA field identifies which station(s) should receive the frame.
- Source addresses (SA) — 6 bytes. The SA field identifies the sending station.

16. Define protocol Structure MAC Frame with Gigabit Carrier Extension?

1000Base-X has a minimum frame size of 416bytes, and
1000Base-T has a minimum frame size of 520bytes. An extension field is used to fill the frames that are shorter than the minimum length.

7	1	6	6	2	46=< n =<1500	4bytes	Variable
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS	Ext

17. Define IEEE 802.5 LAN Protocol? (April 2013)

Token Ring is a LAN protocol, defined in IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring.

Token Ring as defined in IEEE 802.5 is originated from the IBM Token Ring LAN technologies. Both are based on the Token Passing technologies. While they differ in minor ways; they are generally compatible with each other.

18. Draw an IEEE 802.5 Protocol Structure?

1	2	3	9	15bytes
SDEL	AC	FC	Destination address	Source address
Route information 0-30 bytes				
Information (LLC or MAC) variable				
FCS (4 bytes)		EDEL	FS	

• SDEL / EDEL - Starting Delimiter / Ending Delimiter. Both the SDEL and EDEL have intentional Manchester code violations in certain bit positions so that the start and end of a frame can never be accidentally recognized in the middle of other data.

• AC - Access Control field contains the priority fields.

• FC - Frame Control field indicates whether the frame contains data or control information

• Destination address – Destination station address.

• Source address –Source station address.

• Route information – The field with routing control, route descriptor and routing type information.

• Information - The Information field may be LLC or MAC.

• FCS - Frame check sequence.

• Frame status - Contains bits that may be set on by the recipient of the frame to signal recognition of the address and whether the frame was successfully copied.

19. Define WLAN: Wireless LAN by IEEE 802.11 protocols?

The Wireless Local Area Network (WLAN) technology is defined by the IEEE 802.11 family of specifications. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance instead of CSMA/CD) for path sharing.

20. Define 802.11?

802.11 -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

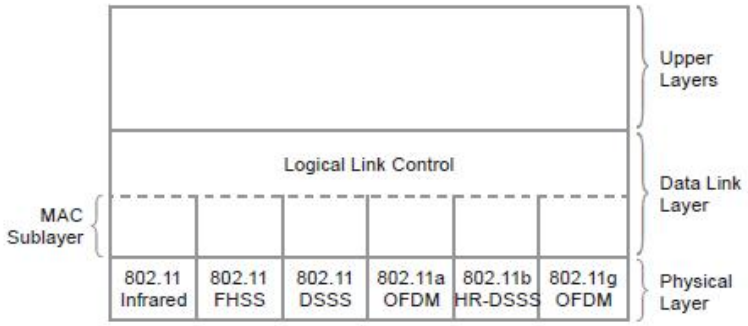
21. Define 802.11a?

802.11a -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band.802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. The 802.11a specification applies to wireless ATM systems and is used in access hubs.

22. Define 802.11b?

802.11b (also referred to as 802.11 High Rate or Wi-Fi) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b is a modification of the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

23. Draw the 802.11 stack structure?



For short range and low power wireless (less than 10 meters) communications among personal devices such as PDA, Bluetooth and subsequent IEEE standards (802.15) are taking effects. For long range wireless communications in the metropolitan areas, WiMax and IEEE 802.16 are the standards.

24. Draw the Protocol Structure for 801.11?

801.11 protocol family MAC frame structure:

2	2	6	6	6	2	6	0-2312	4bytes
Frame Con-trol	Dura-tion	Ad-dress 1	Ad-dress 2	Ad-dress 3	Seq	Ad-dress 4	Data	Check sum

- Address fields (1-4) - contain up to 4 addresses (source, destination, transmitter and receiver addresses) depending on the frame control field (the ToDS and FromDS bits).
- Sequence Control - consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame and to recognize packet duplications.
- Data - is information that is transmitted or received.
- CRC - contains a 32-bit Cyclic Redundancy Check (CRC).

25. What are the two classes of traffic in FDDI?

- Synchronous
- Asynchronous

26. Define Fiber Distributed Data Interface? (APRIL 2013)

Fiber Distributed Data Interface (FDDI) is a set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing (similar to IEEE 802.5 Token Ring protocol) and dual-ring networks, and support data rates of up to 100 Mbps. FDDI networks are typically used as backbone technology because of the protocol supports a high bandwidth and a great distance. A related copper specification similar to FDDI protocols, called Copper Distributed Data Interface (CDDI), has also been defined to provide 100-Mbps service over twisted-pair copper.

27. Draw the Protocol Structure for FDDI?

2	6	6	0-30	Variable	4bytes
Frame control	Desti-nation address	Source address	Route informa-tion	Informa-tion	FCS

• Frame control - The frame control structure is as follows

C	L	F	F	Z	Z	Z	Z

C Class bit: 0 Asynchronous frame; 1 Synchronous frame/
L Address length bit: 0 16 bits (never); 1 48 bits (always).
FF Format bits.
ZZZZ Control bits.

• Destination address - The address structure is as follows:

I/G	U/L	Address bits

• Source address - The address structure is as follows:

I/G	RII	Address bits

I/G Individual/group address: 0 Group address; 1 Individual address.
RII Routing information indicator: 0 RI absent; 1 RI present.

28. Define Integrated Services Digital Network?

Integrated Services Digital Network (ISDN) is a system with digitized phone connections. For decades, telephony has used purely analogue connections. ISDN is the first protocol to define a digital communications line that allows for the transmission of voice, data, video and graphics, at high speeds, over standard communication lines. The various media are simultaneously carried by bearer channels (B channels) occupying a bandwidth of 64 kbits per second (some switches limit bandwidth to 56 kb/s). A defined data channel (D channel) handles signaling at 16 kb/s or 64 kb/s, depending on the service type. ISDN is not restricted to public telephone networks alone; it may be transmitted via packet switched networks, telex, CATV networks, etc.

29. Explain the two basic types of ISDN service?

- Basic Rate Interface (BRI) - consists of two 64 kb/s B channels and one 16 kb/s D channel for a total of 144 kb/s. This basic service is intended to meet the needs of most individual users. The U interface provided by the telco for BRI is a 2-wire, 160 kb/s digital connection. Echo cancellation is used to reduce noise, and data encoding schemes (2B1Q in North America, 4B3T in Europe) permit this relatively high data rate over ordinary single-pair local loops.
- Primary Rate Interface (PRI) is intended for users with greater capacity requirements. Typically the channel structure is 23 B channels plus one 64 kb/s D channel for a total of 1536 kb/s. In Europe, PRI consists of 30 B channels plus one 64 kb/s D channel for a total of 1984 kb/s. It is also possible to support multiple PRI lines with one 64 kb/s D channel using Non-Facility Associated Signaling (NFAS).

30. Draw Protocol Structure for ISDN?

8	7	6	5	4	3	2	1
Protocol discriminator							
0	0	0	0	Length of reference call value			
Flag	Call reference value						
0	Message type						
Other information elements as required							

- Protocol discriminator - The protocol used to encode the remainder of the Layer.
- Length of call reference value - Defines the length of the next field. The Call reference may be one or two octets long depending on the size of the value being encoded.
- Flag - Set to zero for messages sent by the party that allocated the call reference value; otherwise set to one.
- Call reference value - An arbitrary value that is allocated for the duration of the specific session, which identifies the call between the device maintaining the call and the ISDN switch.

- Message type - Defines the primary purpose of the frame. The message type may be one octet or two octets (for network specific messages). When there is more than one octet, the first octet is coded as eight zeros.

31. Explain in DSL?

DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

32. Define in Point-to-Point Protocols? (NOV 2013)(April 2013)

The Point-to-Point Protocol (PPP) suite provides a standard method for transporting multi-protocol datagrams over point-topoint links. PPP was originally devised as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol (layer 2 in the OSI model) in the TCP-IP protocol suite over synchronous modem links, as a replacement for the non-standard layer 2 protocol SLIP. However, other protocols other than IP can also be carried over PPP, including DECnet and Novell's Internetwork Packet Exchange (IPX).

33. Define in PPP Link Control Protocol?

The Link Control Protocol (LCP) is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing. The Link Control Protocol LCP in PPP is versatile and portable to a wide variety of environment.

34. Define in High Level Data Link Control?

The High Level Data Link Control (HDLC) protocol, an ISO data link layer protocol based on the IBM SDLC, ensures that data passed up to the next layer has been received exactly as transmitted (i.e. error free, without loss and in the correct order). Another important function of HDLC is flow control, which ensures that data is transmitted only as fast as the receiver can receive it. There are two distinct HDLC implementations: HDLC NRM (also known as SDLC) and HDLC Link Access Procedure Balanced (LAPB). The later is the more popular implementation. HDLC is part of the X.25 stack.

35 Define in ATM Private Network- to-Network Interface.

The ATM Private Network-Node Interface (PNNI), an ATM network- to-network signaling protocol, provides mechanisms to support scalable, QoS-based ATM routing and switch-to-switch switched virtual connection (SVC) interoperability.

36. Define in ATM LAN Emulation NNI?

The ATM LAN Emulation (LANE) enables the implementation of emulated LANs over an ATM network. An emulated LAN provides communication of user data frames among all its users, similar to a physical LAN. One or more emulated LANs could run on the same ATM network. However, each of the emulated LANs is logically independent of the others. Communication between emulated LANs requires

some type of interconnection device (bridge, router, etc.), even though direct ATM connections between emulated LANs are explicitly allowed in some circumstances.

37. Define in SONET/SDH?

The Synchronous Optical Network (SONET), also called and Synchronous Digital Hierarchy (SDH), are a set of related standards for synchronous data transmission over fiber optic networks that are often used for framing and synchronization at the physical layer. SONET is the United States version of the standard published by the American National Standards Institutes (ANSI). SDH is the international version of the standard published by the International Telecommunications Union (ITU).

38. What are the servers included in lane? (NOV 2013)

- LAN Emulation Configuration Server (LECS)
- LAN Emulation Server (LES)
- Broadcast/Unknown Server (BUS)
- Selective Multicast Server (SMS)

11 MARKS

1. Explain in detail about Address Resolution Protocol and Inverse ARP (11 marks)(NOV 2013)

Protocol Description

Address Resolution Protocol (ARP) performs mapping of an IP address to a physical machine address (MAC address for Ethernet) that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the rules for making this correlation and providing address conversion in both directions.

Since protocol details differ for each type of local area network, there are separate ARP specifications for Ethernet, Frame Relay, ATM, Fiber Distributed-Data Interface, HIPPI, and other protocols. InARP is an addition to ARP to address ARP in Frame Relay environment.

There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache. Details of RARP are presented in a separate document.

Protocol Structure

ARP and In RARP have the same structure:

<table>
<tr><td colspan="2">16</td><td>32 bit</td></tr>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>HLen</td><td>PLen</td><td>Operation</td></tr>
<tr><td colspan="3">Sender Hardware address</td></tr>
<tr><td colspan="3">Sender Protocol Address</td></tr>
<tr><td colspan="3">Target Hardware Address</td></tr>
<tr><td colspan="3">Target Protocol Address</td></tr>
</table>

- Hardware type - Specifies a hardware interface type for which the sender requires a response.
- Protocol type - Specifies the type of high-level protocol address the sender has supplied.
- HLen - Hardware address length.
- PLen - Protocol address length.
- Operation - The values are as follows:
  1. ARP request.
  2. ARP response.
  3. RARP request.
  4. RARP response.
  5. Dynamic RARP request.
  6. Dynamic RARP reply.
  7. Dynamic RARP error.
  8. InARP request.
  9. InARP reply.
- Sender hardware address -HLen bytes in length.
- Sender protocol address - PLen bytes in length.
- Target hardware address - HLen bytes in length.
- Target protocol address - PLen bytes in length.

2. Explain in detail about IP Control Protocol and IPv6 Control Protocol (6 marks)

Protocol Description

IP Control Protocol (IPCP) and IPv6 Control Protocol (IPv6CP) define the Network Control Protocol for establishing and configuring the Internet Protocol or IPv6 over PPP, and a method to negotiate and use Van Jacobson TCP/IP header compression with PPP.

IPCP is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of the point-to-point link. IPCP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPCP packets received before this phase is reached should be silently discarded.

Before any IP packets may be communicated, PPP must reach the Network-Layer Protocol phase, and the IP Control Protocol must reach the Opened state. Van Jacobson TCP/IP header compression reduces the size of the TCP/IP headers to as few as three bytes. This can be a significant improvement on slow serial lines, particularly for interactive traffic.

The IP Compression Protocol Configuration Option is used to indicate the ability to receive compressed packets. Each end of the link must separately request this option if bidirectional compression is desired.

IPv6CP is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPv6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPv6CP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPv6CP packets received before this phase is reached should be silently discarded.

Protocol Structure

IPCP and IPv6CP configuration option packet header:

8	16	32 bit
Type	Length	Configuration option

- Type – 1 for IP-Address, 2 for IP-Compression Protocol, and 3 for IP-Address
- Length >= 4
- Configuration Option - The field is two octets and indicates one of the following options:

For IPCP:
Type 1: IP-Addresses
Type 2: IP-Compression Protocol
Type 3: IP-Address.

For IPv6CP:
Type 1: Interface – Identifier
Type 2: IPv6-Compression Protocol

IPCP and IPv6CP header structure:

8	16	32 bit
Code	Identifier	Length
Data(variable)		

- Code - Specifies the function to be performed.
- Identifier - Used to match requests and replies.
- Length - Size of the packet including the header.

• Data -Zero or more bytes of data as indicated by the Length. This field may contain one or more Options.

3. Explain in detail about Reverse Address Resolution Protocol (6 marks)

Protocol Description

Reverse Address Resolution Protocol (RARP) allows a physical machine in a local area network to request its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machines' (or Media Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests its IP address from the RARP server on the router. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use.

RARP is available for Ethernet, Fiber Distributed-Data Interface, and Token Ring LANs.

Protocol Structure

The protocol header for RARP is the same as for ARP:

<table>
<tr><th colspan="2">16</th><th>32 bit</th></tr>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>HLen</td><td>PLen</td><td>Operation</td></tr>
<tr><td colspan="3">Sender Hardware address</td></tr>
<tr><td colspan="3">Sender Protocol Address</td></tr>
<tr><td colspan="3">Target Hardware Address</td></tr>
<tr><td colspan="3">Target Protocol Address</td></tr>
</table>

• Hardware type - Specifies a hardware interface type for which the sender requires a response.
• Protocol type - Specifies the type of high-level protocol address the sender has supplied.
• Hlen - Hardware address length.
• Plen - Protocol address length.
• Operation - The values are as follows:
    1. ARP request.
    2. ARP response.
    3. RARP request.
    4. RARP response.
    5. Dynamic RARP request.
    6. Dynamic RARP reply.
    7. Dynamic RARP error.
    8. InARP request.
    9. InARP reply.
• Sender hardware address -HLen bytes in length.
• Sender protocol address - PLen bytes in length.
• Target hardware address - HLen bytes in length.
• Target protocol address - PLen bytes in length.

4. Write in detail Serial Line IP (5 marks)

Protocol Description

Serial Line IP (SLIP) is used for point-to-point serial connections running TCP/IP. SLIP is commonly used on dedicated serial links and sometimes for dialup purposes, and is usually used with line speeds between 1200bps and 19.2Kbps. SLIP is useful for allowing mixes of hosts and routers to

communicate with one another (host-host, host-router and router-router are all common SLIP network configurations).

SLIP is merely a packet framing protocol: SLIP defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection/correction or compression mechanisms.

The SLIP protocol defines two special characters: END and ESC. END is octal 300 (decimal 192) and ESC is octal 333 (decimal 219). To send a packet, a SLIP host simply starts sending the data in the packet. If a data byte is the same code as the END character, a two byte sequence of ESC and octal 334 (decimal 220) is sent instead. If it the same as an ESC character, a two byte sequence of ESC and octal 335 (decimal 221) is sent instead. When the last byte in the packet has been sent, an END character is then transmitted.

Because there is no 'standard' SLIP specification, there is no real defined maximum packet size for SLIP. It is probably best to accept the maximum packet size used by the Berkeley UNIX SLIP drivers: 1006 bytes including the IP and transport protocol headers (not including the framing characters).

Compressed Serial Line IP (CSLIP) performs the Van Jacobson header compression on outgoing IP packets. This compression improves throughput for interactive sessions noticeably. Today, SLIP is largely replaced by the Point–to-Point Protocol (PPP), which is more features rich and flexible.

5. Write in detail Ethernet IEEE 802.3 Local Area Network protocols (11 marks)

Protocol Description

Ethernet protocols refer to the family of local-area networks (LAN) covered by a group of IEEE 802.3 standards. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex. In the half-duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium. The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance.

Four data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps—10Base-T Ethernet (802.3)
- 100 Mbps—Fast Ethernet (802.3u)
- 1000 Mbps—Gigabit Ethernet (802.3z)
- 10-Gigabit Ethernet - IEEE 802.3ae

In this document, we discuss the general aspects of the Ethernet. The specific issues on fast Ethernet, Gigabit and 10 Gigabit Ethernet will be discussed in separate documents.

The Ethernet system consists of three basic elements: 1) the physical medium used to carry Ethernet signals between computers, 2) a set of medium access control rules embedded in each Ethernet interface that allows multiple computers to fairly arbitrate access to the shared Ethernet channel, and 3) an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sublayers, the Media Access Control (MAC) sub-layer and the MAC-client sublayer. The IEEE 802.3 physical layer corresponds to the ISO physical layer.

The MAC sub layer has two primary responsibilities:

- Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception

- Media access control, including initiation of frame transmission and recovery from transmission failure

The MAC-client sub layer may be one of the following:

- Logical Link Control (LLC), which provides the interface between the Ethernet MAC and the upper layers in the protocol stack of the end station. The LLC sublayer is defined by IEEE 802.2 standards.
- Bridge entity, which provides LAN-to-LAN interfaces between LANs that use the same protocol (for example, Ethernet to Ethernet) and also between different protocols (for example, Ethernet to Token Ring). Bridge entities are defined by IEEE 802.1 standards.

Each Ethernet-equipped computer operates independently of all other stations on the network: there is no central controller. All stations attached to an Ethernet are connected to a shared signaling system, also called the medium. To send data a station first listens to the channel and, when the channel is idle then transmits its data in the form of an Ethernet frame, or packet.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered to the networking software running on that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

When it comes to how signals flow over the set of media segments that make up an Ethernet system, it helps to understand the topology of the system. The signal topology of the Ethernet is also known as the logical topology, to distinguish it from the actual physical layout of the media cables. The logical topology of an Ethernet provides a single channel (or bus) that carries Ethernet signals to all stations.

Multiple Ethernet segments can be linked together to form a larger Ethernet LAN using a signal amplifying and retiming device called a repeater. Through the use of repeaters, a given Ethernet system of multiple segments can grow as a “non-rooted branching tree.” “Non-rooted” means that the resulting system of linked segments may grow in any direction, and does not have
a specific root segment. Most importantly, segments must never be connected in a loop. Every segment in the system must have two ends, since the Ethernet system will not operate correctly in the presence of loop paths.

Even though the media segments may be physically connected in a star pattern, with multiple segments attached to a repeater, the logical topology is still that of a single Ethernet channel that carries signals to all stations.

Protocol Structure

The basic IEEE 802.3 MAC Data Frame for 10/100Mbps Ethernet:

7	1	6	6	2	46-1500bytes	4bytes
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS

- Preamble (Pre) — 7 bytes. The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.
- Start-of-frame delimiter (SFD)—1 byte. The SOF is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.
- Destination address (DA) — 6 bytes. The DA field identifies which station(s) should receive the frame.
- Source addresses (SA) — 6 bytes. The SA field identifies the sending station.
- Length/Type— 2 bytes. This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format.
- Data— Is a sequence of n bytes (46=< n =<1500) of any value. The total frame minimum is 64bytes.
- Frame check sequence (FCS) — 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.

MAC Frame with Gigabit Carrier Extension:

1000Base-X has a minimum frame size of 416bytes, and

1000Base-T has a minimum frame size of 520bytes. An extension field is used to fill the frames that are shorter than the minimum length.

7	1	6	6	2	46=< n =<1500	4bytes	Variable
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS	Ext

6. Write in detail Token Ring: IEEE 802.5 LAN Protocol (11 marks)

Protocol Description

Token Ring is a LAN protocol, defined in IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring.

Token Ring as defined in IEEE 802.5 is originated from the IBM Token Ring LAN technologies. Both are based on the Token Passing technologies. While they differ in minor ways; they are generally compatible with each other.

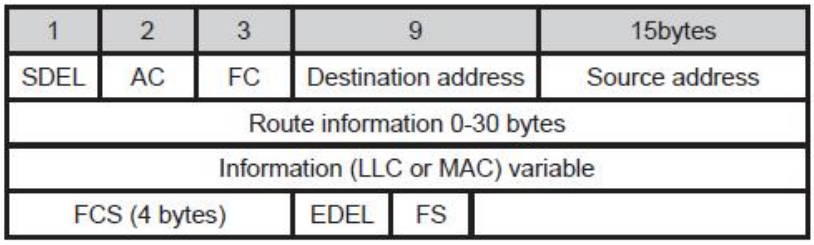
Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has information to send, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network, which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks.

The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

Unlike Ethernet CSMA/CD networks, token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of

transmitting. This feature and several reliability features make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important.
The Fiber Distributed-Data Interface (FDDI) also uses the Token Passing protocol.

Protocol Structure



• SDEL / EDEL - Starting Delimiter / Ending Delimiter. Both the SDEL and EDEL have intentional Manchester code violations in certain bit positions so that the start and end of a frame can never be accidentally recognized in the middle of other data.

• AC - Access Control field contains the priority fields.

• FC - Frame Control field indicates whether the frame contains data or control information

• Destination address – Destination station address.

• Source address –Source station address.

• Route information – The field with routing control, route descriptor and routing type information.

• Information - The Information field may be LLC or MAC.

• FCS - Frame check sequence.

• Frame status - Contains bits that may be set on by the recipient of the frame to signal recognition of the address and whether the frame was successfully copied.

7. Write in detail Wireless LAN by IEEE 802.11 protocols (11 marks) (APRIL 2013)

Protocol Description

The Wireless Local Area Network (WLAN) technology is defined by the IEEE 802.11 family of specifications. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance instead of CSMA/CD) for path sharing.

• 802.11 -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

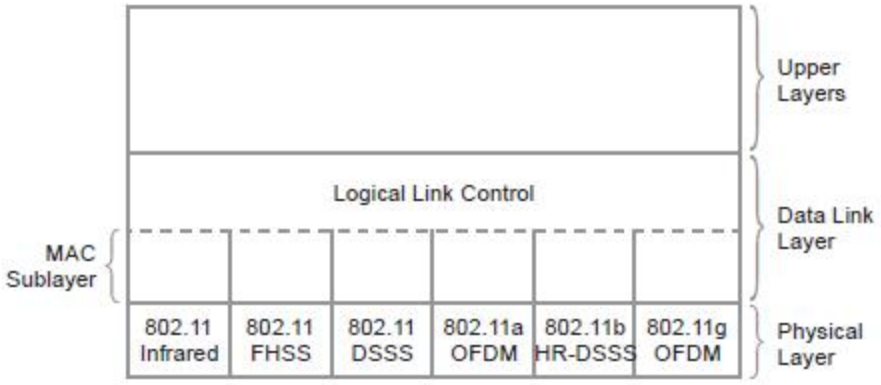
• 802.11a -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band.802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. The 802.11a specification applies to wireless ATM systems and is used in access hubs.

• 802.11b (also referred to as 802.11 High Rate or Wi-Fi) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b is a modification of the original
802.11 standard, allowing wireless functionality comparable to Ethernet.

• 802.11g -- offers wireless transmission over relatively short distances at 20 – 54 Mbps in the 2.4 GHz band. 802.11g also uses the OFDM encoding scheme. The modulation used in 802.11 has historically been phase-shift keying (PSK). The modulation method selected for 802.11b is known as complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11a uses a modulation scheme known as orthogonal

frequency-division multiplexing (OFDM) that makes possible data speeds as high as 54 Mbps, but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps.

The 802.11 stack structure is as follows:



For short range and low power wireless (less than 10 meters) communications among personal devices such as PDA, Bluetooth and subsequent IEEE standards (802.15) are taking effects. For long range wireless communications in the metropolitan areas, WiMax and IEEE 802.16 are the standards.

Protocol Structure

801.11 protocol family MAC frame structure:

2	2	6	6	6	2	6	0-2312	4bytes
Frame Con-trol	Dura-tion	Ad-dress 1	Ad-dress 2	Ad-dress 3	Seq	Ad-dress 4	Data	Check sum

• Frame Control Structure:

2	2	4	1	1	1	1	1	1	1	1
Ver-sion	Type	Sub-type	To DS	From DS	MF	Re-try	Pwr	More	W	O

• Protocol Version - indicates the version of IEEE 802.11 standard.
• Type – Frame type: Management, Control and Data.
• Subtype - Frame subtype: Authentication frame, Deauthentication frame; Association request frame; Association response frame; Re association request frame; Reassociation response frame; Disassociation frame; Beacon frame; Probe frame; Probe request frame or Probe response frame.
• To DS - is set to 1 when the frame is sent to Distribution System (DS)
• From DS - is set to 1 when the frame is received from the Distribution System (DS)
• MF- More Fragment is set to 1 when there are more fragments belonging to the same frame following the current fragment
• Retry indicates that this fragment is a retransmission of a previously transmitted fragment. (For receiver to recognize duplicate transmissions of frames)
• Pwr - Power Management indicates the power management mode that the station will be in after the transmission of the frame.
• More - More Data indicates that there are more frames buffered to this station.

• W - WEP indicates that the frame body is encrypted according to the WEP (wired equivalent privacy) algorithm.

• O - Order indicates that the frame is being sent using the Strictly-Ordered service class.

• Duration/ID (ID) –

• Station ID is used for Power-Save poll message frame type.

• The duration value is used for the Network Allocation Vector (NAV) calculation.

• Address fields (1-4) - contain up to 4 addresses (source, destination, transmitter and receiver addresses) depending on the frame control field (the ToDS and FromDS bits).

• Sequence Control - consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame and to recognize packet duplications.

• Data - is information that is transmitted or received.

• CRC - contains a 32-bit Cyclic Redundancy Check (CRC).

8. Explain about Fiber Distributed Data Interface (11 marks) (NOV 2013)

Protocol Description

Fiber Distributed Data Interface (FDDI) is a set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing (similar to IEEE 802.5 Token Ring protocol) and dual-ring networks, and support data rates of up to 100 Mbps. FDDI networks are typically used as backbone technology because of the protocol supports a high bandwidth and a great distance. A related copper specification similar to FDDI protocols, called Copper Distributed Data Interface (CDDI), has also been defined to provide 100-Mbps service over twisted-pair copper.

An extension to FDDI, called FDDI-2, supports the transmission of voice and video information as well as data. Another variation of FDDI, called FDDI Full Duplex Technology (FFDT) uses the same network infrastructure but can potentially support data rates up to 200 Mbps.

FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. As will be discussed in detail later in this chapter, the primary purpose of the dual rings is to provide superior reliability and robustness.

FDDI specifies the physical and media access portions of the OSI reference model. FDDI is not actually a single specification but is a collection of four separate specifications, each with a specific function. Combined, these specifications have the capability to provide high-speed connectivity between upper-layer protocols such as TCP/IP and IPX, and media such as fiberoptic cabling.

FDDI's four specifications are the Media Access Control (MAC), Physical Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT) specifications. The MAC specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and errorrecovery mechanisms. The PHY specification defines data encoding/ decoding procedures, clocking requirements, and framing, among other functions. The PMD specification defines the characteristics of the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors. The SMT specification defines FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

Protocol Structure

2	6	6	0-30	Variable	4bytes
Frame control	Desti-nation address	Source address	Route informa-tion	Informa-tion	FCS

• Frame control - The frame control structure is as follows

C	L	F	F	Z	Z	Z	Z

C Class bit: 0 Asynchronous frame; 1 Synchronous frame/
L Address length bit: 0 16 bits (never); 1 48 bits (always).
FF Format bits.
ZZZZ Control bits.

• Destination address - The address structure is as follows:

I/G	U/L	Address bits

• Source address - The address structure is as follows:

I/G	RII	Address bits

I/G Individual/group address: 0 Group address; 1 Individual address.
RII Routing information indicator: 0 RI absent; 1 RI present.

• Route Information - The structure of the route information is as follows:

3	5	1	6	1	16	16		16
RT	LTH	D	LF	r	RD1	RD2	...	RDn

RC - Routing control (16 bits).
RDn - Route descriptor (16 bits).
RT - Routing type (3 bits).
LTH - Length (5 bits).
D - Direction bit (1 bit).
LF - Largest frame (6 bits).
R - Reserved (1 bit).

• Information - The Information field may be LLC, MAC or SMT protocol.
• FCS - Frame check sequence.

9. Explain about Integrated Services Digital Network (11 marks)

Protocol Description

Integrated Services Digital Network (ISDN) is a system with digitized phone connections. For decades, telephony has used purely analogue connections. ISDN is the first protocol to define a digital communications line that allows for the transmission of voice, data, video and graphics, at high speeds, over standard communication lines. The various media are simultaneously carried by bearer channels

(B channels) occupying a bandwidth of 64 kbits per second (some switches limit bandwidth to 56 kb/s). A defined data channel (D channel) handles signaling at 16 kb/s or 64 kb/s, depending on the service type. ISDN is not restricted to public telephone networks alone; it may be transmitted via packet switched networks, telex, CATV networks, etc.

There are two basic types of ISDN service:

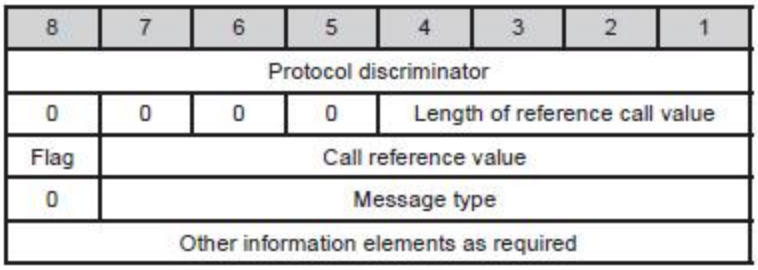
Basic Rate Interface (BRI) - consists of two 64 kb/s B channels and one 16 kb/s D channel for a total of 144 kb/s. This basic service is intended to meet the needs of most individual users. The U interface provided by the telco for BRI is a 2-wire, 160 kb/s digital connection. Echo cancellation is used to reduce noise, and data encoding schemes (2B1Q in North America, 4B3T in Europe) permit this relatively high data rate over ordinary single-pair local loops.

Primary Rate Interface (PRI) is intended for users with greater capacity requirements. Typically the channel structure is 23 B channels plus one 64 kb/s D channel for a total of 1536 kb/s. In Europe, PRI consists of 30 B channels plus one 64 kb/s D channel for a total of 1984
kb/s. It is also possible to support multiple PRI lines with one 64 kb/s D channel using Non-Facility Associated Signaling (NFAS).

The CCITT (now ITU-T) study group responsible for ISDN first published a set of ISDN recommendations in 1984. Prior to this publication, various geographical areas had developed different versions of ISDN. The use of nation-specific information elements is enabled by using the Codeset mechanism which allows different areas to use their own information elements within the data frames. A common nation-specific ISDN variant is National ISDN by Bellcore, used in the USA. It has four network-specific message types. It does not have any single octet information elements. Other changes are the addition of the SEGMENT, FACILITY and REGISTER message types and the Segmented Message and Extended Facility information elements. Also, some meanings of field values have changed and some new accepted field values have been added. Due to its limitation of bandwidth and services, this traditional ISDN is called narrowband ISDN, in contrast to the BISDN (Broadband ISDN).

Protocol Structure

Below is the general structure of the ISDN frame:



• Protocol discriminator - The protocol used to encode the remainder of the Layer.

• Length of call reference value - Defines the length of the next field. The Call reference may be one or two octets long depending on the size of the value being encoded.

• Flag - Set to zero for messages sent by the party that allocated the call reference value; otherwise set to one.

• Call reference value - An arbitrary value that is allocated for the duration of the specific session, which identifies the call between the device maintaining the call and the ISDN switch.

• Message type - Defines the primary purpose of the frame. The message type may be one octet or two octets (for network specific messages). When there is more than one octet, the first octet is coded as eight zeros. A complete list of message types is given in ISDN Message Types below.

• ISDN Information Elements - There are two types of information elements: single octet and variable length.

• Single octet information elements - The single octet information element appears as follows:

8	7	6	5	4	3	2	1
1	Information element identifier				Information element		

• Variable length information elements - The following is the format for the variable length information element:

8	7	6	5	4	3	2	1
0	Information element identifier						
Length of information elements							
Information elements (multiple bytes)							

• The information element identifier identifies the chosen element and is unique only within the given Code set. The length of the information element informs the receiver as to the amount of the following octets belonging to each information element.

• ISDN Message Types - The possible ISDN message types are: Call Establishment, Call Information Phase, Call Clearing, and Miscellaneous.

• Code set - Three main Code sets are defined. In each Code set, a section of the information elements are defined by the associated variant of the protocol:

Codeset 0	The default code, referring to the CCITT set of information elements.
Codeset 5	The national specific Codeset.
Codeset 6	The network specific Codeset.

• CPE - Customer Premises Equipment; Refers to all ISDN compatible equipment connected at the user site. Examples of devices are telephone, PC, Telex, Facsimile, etc. The exception is the FCC definition of NT1. The FCC views the NT1 as a CPE because it is on the customer site, but the CCITT views NT1 as part of the network. Consequently the network reference point of the network boundary is dependent on the variant in use.

• ISDN Channels B, D and H - The three logical digital communication channels of ISDN perform the following functions:

B-Channel	Carries user service information including: digital data, video, and voice.
D-Channel	Carries signals and data packets between the user and the network
H-Channel	Performs the same function as B-Channel, but operates at rates exceeding DS-0 (64 Kbps). They are implemented as H0 (384 kb/s (6 B channels), H10 (1472 kb/s -23 B channels), H11 (1536 kb/s; 24 B channels), and H12 (1920 kb/s for International -E1 only).

10. Explain about xDSL(5 marks)

Protocol Description

DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require short runs to a central telephone office (usually less than 20,000 feet). However, xDSL offers much higher speeds - up to 32 Mbps for upstream traffic, and from 32 Kbps to over 1 Mbps for downstream traffic.

Several modulation technologies are used by various kinds of DSL:

- Discrete Multitone Technology (DMT)
- Simple Line Code (SLC)
- Carrierless Amplitude Modulation (CAP)
- Multiple Virtual Line (MVL)
- Discrete Wavelet Multitone (DWMT).

To interconnect multiple DSL users to a high-speed backbone network, the telephone company uses a Digital Subscriber Line Access Multiplexer (DSLAM). The DSLAM aggregates data transmission from all access DSL lines and then connects to an asynchronous transfer mode (ATM) network. At the other end of each transmission, a DSLAM demultiplexes the signals and
forwards them to appropriate individual DSL connections. Most DSL technologies require that a signal splitter be installed at a customer's premises. However, it is possible to manage the splitting remotely from the central office. This is known as splitter less DSL, "DSL Lite," G.Lite, or Universal ADSL.

Protocol Structure

The following table provides a summary of various DSL specifications.

Type	Description	Data Rate	Mode	Distance	Applications
IDSL	ISDN Digital Subscriber Line	128 kbps	Duplex	18k ft on 24 gauge wire	ISDN service Voice and data communication
HDSL	High data rate Digital Subscriber Line	1.544 Mbps to 42.048 Mbps	Duplex	12k ft on 24 gauge wire	T1/E1 service Feeder plant, WAN, LAN access, server access
SDSL	Single Line Digital Subscriber Line	1.544 Mbps to 2.048 Mbps	Duplex	12k ft on 24 gauge wire	Same as HDSL plus premises access for symmetric services
ADSL	Asymmetric Digital Subscriber Line	1.5 to 9 Mbps 16 to 640 kbps	Down Up	Up to 18k ft on 24 gauge wire	Internet access, video on demand, simplex video, remote LAN access, interactive multimedia
DSL Lite (G.Lite)	"Splitter less" DSL	1.544 Mbps to 6 Mbps 16 to 640	Down Up	18k ft on 24 gauge wire	The standard ADSL; sacrifices speed for not having to install a

		kbps			splitter at the user's premises.
VDSL	Very high data rate Digital Subscriber Line	13 to 52 Mbps 1.5 to 2.3 Mbps	Down Up	1k to 4.5k ft depending on data rate	Same as ADSL plus HDTV

11. Explain about Point-to-Point Protocols (6 marks)

Protocol Description

The Point-to-Point Protocol (PPP) suite provides a standard method for transporting multi-protocol datagram over point-to point links. PPP was originally devised as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol (layer 2 in the OSI model) in the TCP-IP protocol suite over synchronous modem links, as a replacement for the non-standard layer 2 protocol SLIP. However, other protocols other than IP can also be carried over PPP, including DECnet and Novell's Internetwork Packet Exchange (IPX).

PPP is comprised of the following main components:

Encapsulation: A method for encapsulating multi-protocol data grams. The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link. The PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware.

Link Control Protocol: The LCP provided by PPP is versatile and portable to a wide variety of environments. The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing.

Network Control Protocol: An extensible Link Control Protocol (LCP) for establishing, configuring, and testing and managing the data-link connections.

Configuration: Easy and self configuration mechanisms using Link Control Protocol. This mechanism is also used by other control protocols such as Network Control Protocols (NCPs).

In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link. After the link has been stablished and optional facilities have been negotiated as needed by the LCP, PPP must send NCP packets to choose and configure one or more network-layer protocols. Once each of the chosen network- layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link.

The link will remain configured for communications until explicit LCP or NCP packets close the link down, or until some external event occurs (an inactivity timer expires or network administrator intervention).

Protocol Structure

1byte	2bytes	3bytes	5bytes	Variable…	2 – 4bytes
Flag	Address	Control	Protocol	Information	FCS

• Flag— indicates the beginning or end of a frame, consists of the binary sequence 01111110.

• Address— contains the binary sequence 11111111, the standard broadcast address. (Note: PPP does not assign individual station addresses.)

• Control— contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.

• Protocol— identifies the protocol encapsulated in the information field of the frame.

• Information—zero or more octet(s) contains the datagram for the protocol specified in the protocol field.

• FCS—Frame Check Sequence (FCS) Field, normally 16 bits. By prior agreement, consenting PPP implementations can use a 32-bit FCS for improved error detection.

12. Explain about PPP Link Control Protocol (6 marks)

Protocol Description

The Link Control Protocol (LCP) is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing. The Link Control Protocol LCP in PPP is versatile and portable to a wide variety of environment.

There are three classes of LCP packets:

1. Link Configuration packets used to establish and configure a link (Configure-Request, Configure-Ack, Configure- Nak and Configure-Reject).
2. Link Termination packets used to terminate a link (Terminate- Request and Terminate-Ack).
3. Link Maintenance packets used to manage and debug a link (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request).

In the interest of simplicity, there is no version field in the LCP packet. A correctly functioning LCP implementation will always respond to unknown Protocols and Codes with an easily recognizable LCP packet, thus providing a deterministic fallback mechanism for implementations of other versions.

Regardless of which Configuration Options are enabled, all LCP Link Configuration, Link Termination, and Code-Reject packets (codes 1 through 7) are always sent as if no Configuration Options were negotiated. In particular, each Configuration Option specifies a default value. This ensures that such LCP packets are always recognizable, even when one end of the link mistakenly believes the link to be open.

Exactly one LCP packet is encapsulated in the PPP Information field, where the PPP Protocol field indicates type hex c021 (Link Control Protocol).

Protocol Structure

8	16	32bit	Variable
Code	Identifier	Length	Data

• Code - Decimal value which indicates the type of LCP packet:

1. Configure-Request.
2. Configure-Ack.
3. Configure-Nak.
4. Configure-Reject.
5. Terminate-Request.
6. Terminate-Ack.
7. Code-Reject.
8. Protocol-Reject.
9. Echo-Request.

10. Echo-Reply.
11. Discard-Request.
12. Link-Quality Report.

- Identifier - Decimal value which aids in matching requests and replies.
- Length - Length of the LCP packet, including the Code, Identifier, Length and Data fields.
- Data - Variable length field which may contain one or more configuration options.

13. Explain in detail about HDLC (5 marks)

Protocol Description

The High Level Data Link Control (HDLC) protocol, an ISO data link layer protocol based on the IBM SDLC, ensures that data passed up to the next layer has been received exactly as transmitted (i.e. error free, without loss and in the correct order). Another important function of HDLC is flow control, which ensures that data is transmitted only as fast as the receiver can receive it. There are two distinct HDLC implementations: HDLC NRM (also known as SDLC) and HDLC Link Access Procedure Balanced (LAPB). The later is the more popular implementation. HDLC is part of the X.25 stack.

LAPB is a bit-oriented synchronous protocol that provides complete data transparency in a full-duplex point-to-point operation. It supports a peer-to-peer link in that neither end of the link plays the role of the permanent master station. HDLC NRM, on the other hand, has a permanent primary station with one or more secondary stations.

HDLC LAPB is a very efficient protocol, which requires a minimum of overhead to ensure flow control, error detection and recovery. If data is flowing in both directions (full duplex), the data frames themselves carry all the information required to ensure data integrity.

The concept of a frame window is used to send multiple frames before receiving confirmation that the first frame has been correctly received. This means that data can continue to flow in situations where there may be long “turn-around” time lags without stopping to wait for an acknowledgement. This kind of situation occurs, for instance in satellite communication.

There are three categories of frames:

- Information frames transport data across the link and may encapsulate the higher layers of the OSI architecture.
- Supervisory frames perform the flow control and error recovery functions.
- Unnumbered frames provide the link initialization and termination.

Protocol Structure

1 byte	1-2 bytes	1 byte	variable	2 bytes	1 byte
Flag	Address field	Control field	Information	FCS	Flag

- Flag - The value of the flag is always (0x7E).
- Address field - Defines the address of the secondary station which is sending the frame or the destination of the frame sent by the primary station. It contains Service Access Point (6bits), a Command/Response bit to indicate whether the frame relates to information frames (I-frames) being sent from the node or received by the node, and an address extension bit which is usually set to true to indicate that the address is of length one byte. When set to false it indicates an additional byte follows.
- Extended address - HDLC provides another type of extension to the basic format. The address field may be extended to more than one byte by agreement between the involved parties.

• Control field - Serves to identify the type of the frame. In addition, it includes sequence numbers, control features and error tracking according to the frame type.

• FCS - The Frame Check Sequence (FCS) enables a high level of physical error control by allowing the integrity of the transmitted frame data to be checked.

14. Explain in detail about ATM PNNI (7marks)

Protocol Description

The ATM Private Network-Node Interface (PNNI), an ATM network- to-network signaling protocol, provides mechanisms to support scalable, QoS-based ATM routing and switch-to-switch switched virtual connection (SVC) interoperability.

The PNNI (Private Network-to-Network Interface) is a hierarchical, dynamic link-state routing protocol. It is designed to support large-scale ATM networks. The PNNI protocol uses VPI/VCI 0,18 for its messages. In addition, it uses signaling messages to support connection establishment across multiple networks. PNNI is based on UNI 4.0 and Q.2931. Specific information elements were added to UNI 4.0 in order to support the routing process of PNNI. PNNI Signaling contains the procedure to dynamically establish, maintain and clear ATM connections at the private network to network interface or network node interface between 2 ATM networks or 2 ATM network nodes. The PNNI signaling protocol is based on the ATM forum UNI specification and on Q.2931.

PNNI Messages include:

ALERTING, CALL PROCEEDING, CONNECT, SETUP, RELEASE, RELEASE COMPLETE, NOTIFY, STATUS, STATUS ENQUIRY, RESTART, RESTART ACKNOWLEDGE, STATUS, ADD PARTY, ADD PARTY ACKNOWLEDGE, PARTY ALERTING, ADD PARTY REJECT, DROP PARTY, DROP PARTY ACKNOWLEDGE

Protocol Structure

The structure of the PNNI header is shown in the following illustration:

2	2	1	1	1	1
Packet type	Packet length	Prot ver	Newest ver	Oldest ver	Reserved

• Packet type: The following packet types are defined:

1. Hello - Sent by each node to identify neighbor nodes belonging to the same peer group.
2. PTSP - PNNI Topology State Packet. Passes topology information between groups.
3. PTSE - PNNI Topology State Element (Request and Ack). Conveys topology parameters such as active links, their available bandwidth, etc.
4. Database Summary - Used during the original database exchange between two neighboring peers.

• Packet length - The length of the packet.

• Prot ver - Protocol Version. The version according to which this packet was formatted.

• Newest ver / Oldest ver - Newest version supported / oldest version supported. The newest version supported and the oldest version supported fields are included in order for nodes to negotiate the most recent protocol version that can be understood by both nodes exchanging a particular type of packet.

15. Explain in detail about LANE NNI (6 marks)

Protocol Description

The ATM LAN Emulation (LANE) enables the implementation of emulated LANs over an ATM network. An emulated LAN provides communication of user data frames among all its users, similar to a physical LAN. One or more emulated LANs could run on the same ATM network. However, each of the emulated LANs is logically independent of the others. Communication between emulated LANs requires some type of interconnection device (bridge, router, etc.), even though direct ATM connections between emulated LANs are explicitly allowed in some circumstances.

The LAN Emulation LUNI defines the protocols and interactions between LAN Emulation Clients (LE Clients) and the LAN Emulation Service. Each LE Client connects across the LUNI to a single LES and BUS, may connect to a single LECS, and may have connections to multiple SMSs. The LAN Emulation NNI (LNNI) defines the behavior of these LANE service components as seen by each other, the procedures necessary to provide a distributed and reliable LAN Emulation Service. A single ELAN may be served by multiple LECSs, LESs, BUSs and SMSs. Each LES, BUS, and SMS serves a single ELAN, while an LECS may serve multiple ELANs. LANE service components interconnect with multiple VCCs for Configuration, Status, Database Synchronization, Control and Data forwarding. The LNNI specification provides multivendor interoperability among the components serving an ELAN so that consumers may mix and match the LANE Service implementations of different vendors.

LANE service consists of four major components:

• LAN emulation client (LEC) - located in ATM end systems, implements the LUNI interface, serves as a proxy for LAN systems to perform data forwarding and address resolution, provides a MAC level emulated Ethernet/ IEEE 802.3 or IEEE 802.5 service interface to higher
level software.

• LAN emulation server (LES) - supports the address resolution protocol (LE-ARP), and is used to determine the ATM address of the target LEC responsible for a certain destination MAC address. An LE Client is connected to only one LE Server. An LE Client may register LAN Destinations it represents and/or multicast MAC addresses it wishes to receive with its LE Server. An LE Client will also query its LE Server to resolve a MAC address or route descriptor of an ATM address.

• Broadcast/Unknown Server (BUS) - handles all multicast traffic forwarding to all attached LECs. An LE Client sees a single Broadcast and Unknown Server.

• Selective Multicast Server (SMS) - may be used to offload much of the multicast processing from the BUSs, which also have to forward broadcast frames and frames for unresolved LAN destinations, to efficiently forward multicast frames.

The multiple LANE Service entities serving an ELAN need to cooperate and communicate in order to provide a distributed and reliable LAN Emulation Service. The communications required for LNNI may be partitioned as follows:

a) Control Plane

• Configuration and Status Communications - LESs and SMSs obtain configuration information from an LECS over Configuration Direct VCCs. LECSs obtain the status of LESs and SMSs over the same connection.

• LANE Control Communications - Each LES is responsible for distributing LE_ARP requests for unregistered destinations from local LE Clients to local LE Clients and to other LESs. LESs must also forward LE_ARP responses back to the originator. Additionally, LESs must be able to forward LE_FLUSH responses and LE_TOPOLOGY requests to the correct destination(s).b) Synchronization Plane

• LECS Synchronization - A particular LECS may not directly receive status from all service components. Thus, LECSs must exchange LES and SMS status information among themselves. In order

to distribute this status information, all LECSs participating in an ELAN must maintains an LECS Synchronization VCC to all other LECSs in the network.

• LES-SMS Database Synchronization – LESs and SMSs use SCSP to synchronize their databases.

c) Data Plane

• BUS Data Communications - Each BUS is assumed to be logically paired with an LES, and the BUS is assumed to have access to the registration database maintained by the LES, which includes the ATM address of all BUSs. No protocol is defined between a paired LES and BUS.

• SMS Data Communications – Every SMS (and LES) obtains a complete copy of the registration database for the entire ELAN via SCSP, so every SMS knows of every other SMS and BUS. When an LE Client LE_ARPs for a multicast address, the LES should assign the client
to an SMS as a sender if an SMS is available for that destination, otherwise a BUS's ATM address is returned in the LE_ARP response. An ELAN, and hence all the ELAN's SMSs, may operate in either distributed or stand-alone mode, as determined by the network administrator.

Protocol Structure

LANE Data Frames:

The LNNI Control frame format is shown below:

<table>
<tr><td></td><td>0</td><td colspan="3">LLC = X"AAAA03"</td><td>OUI</td></tr>
<tr><td></td><td>4</td><td>OUI</td><td colspan="3">Frame Type</td></tr>
<tr><td></td><td>8</td><td colspan="4">ELAN-ID</td></tr>
<tr><td rowspan="9">LANE Control Frame</td><td>12</td><td colspan="2">REQUESTER-LECID</td><td colspan="2">FLAGS</td></tr>
<tr><td>16</td><td colspan="4">SOURCE-LAN-DESTINATION</td></tr>
<tr><td>24</td><td colspan="4">TARGET-LAN-DESTINATION</td></tr>
<tr><td>32</td><td colspan="4">SOURCE-ATM-ADDRESS</td></tr>
<tr><td>52</td><td>LAN-Type</td><td>MAX-Frame-Size</td><td>Number-TLVS</td><td>ELAN-Name-Size</td></tr>
<tr><td>56</td><td colspan="4">TARGET-ATM-ADDRESS</td></tr>
<tr><td>76</td><td colspan="4">ELAN-NAME</td></tr>
<tr><td>108</td><td colspan="4">TLVs BEGIN</td></tr>
</table>

• LLC - Logical Link Control: The Control Coordinate VCCs are all LLC encapsulated.
• OUI - Organizationally Unique Identifier = X"00A03E" which indicates ATM Forum.
• FRAME-TYPE = X"000F"
• ELAN-ID - Emulated LAN ID
• OP-CODE (2 Bytes) - Control frame Operation type.

Some defined OP-Code are:

OP-CODE Value	OP-CODE Function
X"000b"	LNNI_CONFIGURE_TRIGGER
X"000C"	LNNI_LECS_SYNC_REQUEST
X"000d"	LNNI_KEEP_ALIVE_REQUEST
X"000d"	LNNI_KEEP_ALIVE_RESPONSE
X"000e"	LNNI_VALIDATE_REQUEST
X"000e"	LNNI_VALIDATE_RESPONSE

• Status - (2 Bytes) Control frame Operation status.
• TLV - Type/ Length / Value Encoded Parameter, Examples of LNNI TLVs are:

Item	Type	LEN	Description
ServerId	00-A0-3E-14	2	Unique identifier for a server within an ELAN
ServerGroupId	00-A0-3E-15	2	Uniquely correlates to an ELAN-ID. Required for SCSP.
Synchroniza-tionPeerServer	00-A0-3E-16	20	Multiplexed ATM Address of ES or SMS to synchro-nize DB using SCSP.
SmsModeOf-Operation	00-A0-3E-19	1	Indicates SMS operational mode. 0 = STAND_ALONE 1 = DISTRIBUTED

16. Explain in detail about LANE UNI (11 marks)

Protocol Description

The ATM LAN emulation (LANE) specification defines how an ATM network can emulate a sufficient set of the medium access control (MAC) services of existing LAN technologies such as Ethernet and Token Ring, so that higher layer protocols can be used without modification. An emulated LAN (ELAN), which provides the appearance of either an Ethernet or Token-Ring LAN segment over a switched ATM network, is composed of a collection of LE Clients and a set of co-operating service entities: LAN Emulation Configuration Servers (LECSs), LAN Emulation Servers (LESs), Broadcast and Unknown Servers (BUSs), and Selective Multicast Servers (SMSs).

The LAN Emulation LUNI defines the protocols and interactions between LAN Emulation Clients (LE Clients) and the LAN Emulation Service, including initialization, registration, address resolution, and data transfer procedures. Each LE Client connects across the LUNI to a single LES and BUS, may connect to a single LECS, and may have connections to multiple SMSs.

Communication among LE Clients and between LE Clients and the LE Service is performed over ATM virtual channel connections (VCCs). Each LE Client must communicate with the LE Service over control and data VCCs. LANE assumes the availability of point-to-point and point-to-multipoint Switched Virtual Circuits (SVCs). Multicast Forward and Control Distribute flows are carried on point-to-multipoint VCCs. Data Direct, Control Direct, Configure Direct, Default Multicast Send and Selective Multicast Send flows are carried on point-to-point VCCs. Only Data Direct flows may be LLC-multiplexed. All other flows are non-multiplexed.

LAN Emulation encompasses both Ethernet and Token Ring emulation. In Ethernet emulation, a LAN Emulation component need examine only a data frame's destination MAC address in order to direct the frame towards its ultimate destinations. In Token Ring emulation, however, a LAN emulation component may have to use a "Route Descriptor" extracted from the data frame's Routing Information Field (RIF) in order to properly direct the frame over the Emulated LAN.

Most LAN emulation services would be implemented as device drivers below the network layer in ATM-to-legacy LAN bridges and ATM end systems. In LANE, the bandwidth management capability is currently supported by the "available bit rate" (ABR) service.

Protocol Structure

LE Data Frames:

1) For 802.3 (Ethernet) Frame – Non-multiplexed data frame:

0	LE Header	Destination Address
4	Destination Address	
8	Source Address	
12	Source Address	Type / Length
16 and on	User Info	

2) For 802.5 (Token Ring) Frame– Non-multiplexed data frame:

0	LE Header	AC PAD	FC
4	Destination Address		
8	Destination Address	Source Address	
12	Source Address	Type / Length	
16-46	Routing Information Field		
	User Info		

• LE Header— LAN Emulation header which contains either the LAN Emulation client identifier value, the sending client, or X'0000'.

LE Control Frame:

Except for LLC multiplexed Data with Direct VCCs, all LAN Emulation control frames, such as LE_FLUSH_REQUESTs, READY_IND and READY_QUERY, use the format described below:

0	MARKER = X"FF00"		PROTOCOL = X"01"	VERSION = X"01"
4	OP-CODE		STATUS	
8	TRANSACTION-ID			
12	REQUESTER-LECID		FLAGS	
16	SOURCE-LAN-DESTINATION			
24	TARGET-LAN-DESTINATION			
32	SOURCE-ATM-ADDRESS			
52	LAN-Type	MAX-Frame-Size	Number-TLVS	ELAN-Name-Size
56	TARGET-ATM-ADDRESS			
76	ELAN-NAME			
108	TLVs BEGIN			

• OP-CODE – (2 Bytes) Control frame Operation type.Some defined OP-Code are:

OP-CODE Value	OP-CODE Function
X"0001" & X"0101"	LE_CONFIGURE_REQUEST & LE_CONFIG-URE_RESPONSE
X"0002" & X"0102"	LE_JOIN_REQUEST & LE_JOIN_RESPONSE
X"0003" & X"0103"	READY_QUERY & READY_IND
X"0004" & X"0104"	LE_REGISTER_REQUEST & LE_REGIS-TER_RESPONSE
X"0005" & X"0105"	LE_UNREGISTER_REQUEST & LE_UNREG-ISTER_RESPONSE
X"0006" & X"0106"	LE_ARP_REQUEST & LE_ARP_RESPONSE
X"0007" & X"0107"	LE_FLUSH_REQUEST LE_FLUSH_RE-SPONSE
X"0008" & X"0108"	LE_NARP_REQUEST & Undefined
X"0009" & X"0109"	LE_TOPOLOGY_REQUEST & Undefined
X"000A" & X"010A"	LE_VERIFY_REQUEST & LE_VERIFY_RE-SPONSE

- Status – (2 Bytes) Control frame Operation status. Some defined Status codes are:

Code (dec)	Name	Code (dec)	Name
0	Success	1	Version Not Supported
2	Invalid request param-eters	4	Duplicate LAN Destina-tion registration
5	Duplicate ATM address	6	Insufficient resources to grant request
7	Access denied	8	Invalid REQUESTOR-ID
9	Invalid LAN Destination	10	Invalid ATM Address
20	No Configuration	21	LE_CONFIGURE Error
22	Insufficient Information	24	TLV Not Found

- TLV - Type / Length / Value Encoded Parameter.

LANE LLC-multiplexed Frame - has a 12-octet LLC multiplexing header:

0	LLC- X"AA"	LLC- X"AA"	LLC X"03"	OUI-X"00"
4	OUI-X"A0"	OUI-X"3E"	Frame-Type	
8	ELAN-ID			
12-28/ 58	LANE Data Frame Header (802.3 or 802.5)			
	User Info			

LLC field is three octets, containing the constant value X"AAAA03", indicating that an OUI follows. OUI field is three octets, containing the constant value X"00A03E", indicating "ATM Forum". The next two octets are a FRAME-TYPE field containing the value X"000C" for IEEE 802.3 data frame, X"000D" for IEEE 802.5 data frame, X"000E" for LANE LLC-multiplexed READY_IND and READY_QUERY control frames. The ELAN-ID field identifies the emulated LAN for this data frame.

17. Explain in detail about SONET/SDH (11 marks)(APRIL 2013)

Protocol Description

The Synchronous Optical Network (SONET), also called and Synchronous Digital Hierarchy (SDH), are a set of related standards for synchronous data transmission over fiber optic networks that are often used for framing and synchronization at the physical layer. SONET is the United States version of the standard published by the American National Standards Institute (ANSI). SDH is the international version of the standard published by the International Telecommunications Union (ITU).

SONET/SDH can be used in an ATM or non-ATM environment. Packet Over SONET/SDH (POS) maps IP datagram into the SONET frame payload using Point-to-Point Protocol (PPP). In the ATM environment, connections to SONET/SDH lines may be via multi-mode, single-mode or UTP.

SONET is based on transmission at speeds of multiples of 51.840 Mbps (STS-1) and SDH is based on STM-1 which has a data rate of 155.52 Mbps, equivalent to STS-3.

The following table lists the hierarchy of the most common SONET/ SDH data rates:

SONET Signal	Bit Rate (Mbp)	SDH Signal	SONET Capacity	SDH Capacity
STS-1/ OC-1	51.840	STM-0	28 DS1 or DS3	21 E1s
STS-3/ OC-3	155.520	STM-1	84 DS1s or 3 DS3s	63 E1s or E4
STS-12/ OC-12	622.080	STM-4	336 DS1s or 12 DS3s	252 E1s or 4 E4s
STS-48 / OC-48	2.488.32	STM-16	1,344 DS1s or 48 DS3s	1,008 E1s or 16 E4s
STS-192/ OC-192	9,953.280	STM-64	5,376 DS1s or 192 DS3s	4,032 E1s or 64 E4s
STS-768/ OC-768	39,813.120	STM-256	21,504 DSs or 786 DS3	16,128 E1s or 256 E4s

Other rates such as OC-9, OC-18, OC-24, OC-36, OC-96 and OC-768 are referenced in some of the standards documents but were not widely implemented. Higher rate maybe defined for future implementations.

Protocol Structure

The frame structure of STS and STM is different. We only display the details of the STS-1 frame structure here. The STS-1 frame is composed of octets which are nine rows high and 90 columns wide. The first three columns are used by the Transport Overhead (TOH) and contain framing, error monitoring, management and payload pointer information. The data (Payload) uses the remaining 87

columns, of which the first column is used for Path Overhead (POH). A pointer in the TOH identifies the start of the payload, which is referred to as the Synchronous Payload Envelope or SPE.

9 Columns	POH	260 Columns	
	J1		9 Rows
	B3		
	C2		
	G1		
	F2		
	H4		
	Z3		
	Z4		
	Z5		

• SOH— Section Overhead.

A1, A2— Frame alignment. These octets contain the value of 0xF628. The receiver searches for these values in the incoming bit stream. These bytes are not scrambled.

C1— STS-1 identification. Since OC-3c and STM-1 contain three STS-1 streams, the three C1 bytes contain 0x01, 0x02 and 0x03, respectively.

B1— Section error monitoring. Contains BIP-8 of all bits in the previous frame using even parity, before scrambling.

• LOH— Line Overhead

B2— Line error monitoring. Contains BIP-24 calculated over all bits of the line overhead of the previous frame with even parity.

H1 (bits 1-4)— New data flag (specifies when the pointer has changed), path AIS.

H1 and H2 (bits 7-16)— Pointer value, path AIS. These bytes specify the offset between the pointer and the first payload byte. A change in this value is ignored until received at least three consecutive times.

H1* and H2*— Concatenation indication, path AIS.

H3— Pointer action (used for frequency justification), path AIS.

K2 (bits 6-8)— Line AIS, line FERF, removal of line FERF.

Z2— Line FEBE. This contains the number of B2 (BIP-24) errors detected in the previous interval.

• POH— Path Overhead

J1— STS path trace. This byte is used repetitively to transmit a 64-byte fixed string so that the receiving terminal in a path can verify its continued connection to the transmitter. Its contents are unspecified.

B3— Path error monitoring. Path BIP-8 over all bits of the payload of the previous frame, using even parity before scrambling.

C2— Path signal level indicator. Contains one of two codes:

Code 0: indicates STS payload unequipped: no path originating equipment.

Code 1: indicates STS payload equipped: nonspecific payload for payloads that need no further differentiation.

G1 (bits 1-4)— Path FEBE. Allows monitoring of complete full-duplex path at any point along a complex path.

G1 (bit 5) — Path yellow alarm, path RDI (Remote Defect Indicator).

18. Explain the various functions ISDN? (April 2013)

ISDN Interfaces and Functions

- Transmission Structure
- User-Network Interface Configurations
- ISDN Protocol Architecture
- ISDN Connection
- Addressing
- Interworking

Principles of ISDN

1. Support of voice and non-voice applications using a limited set of standardized facilities
    - Defines the purpose of ISDN and the means of achieving it
2. Support for switched and non-switched applications
    - Both circuit-switched and packet-switched connections
    - Support non-switched services in the form of dedicated lines
3. Reliance on 64-kbps connections
    - Fundamental block of ISDN
    - 64 kbps were chosen because it was the standard rate for digitized voice
4. Intelligence in the network
    - Sophisticated serviced beyond simple setup a circuit-switched call
    - Sophisticated network management and maintenance capabilities
    - Use of SS7 ((common channel) signaling system number 7) and intelligent switching nodes in the network
    - SS7 is a set of telephony signaling protocols which are used to set up the vast majority of the world's public switched telephone network telephone calls.
5. Layered protocol architecture
    - User access to ISDN protocol is a layered architecture that can be mapped to OSI model
    - Standards can be developed independently for various layers and functions
6. Variety of configurations
    - configuration is possible for implementing ISDN

User Interface

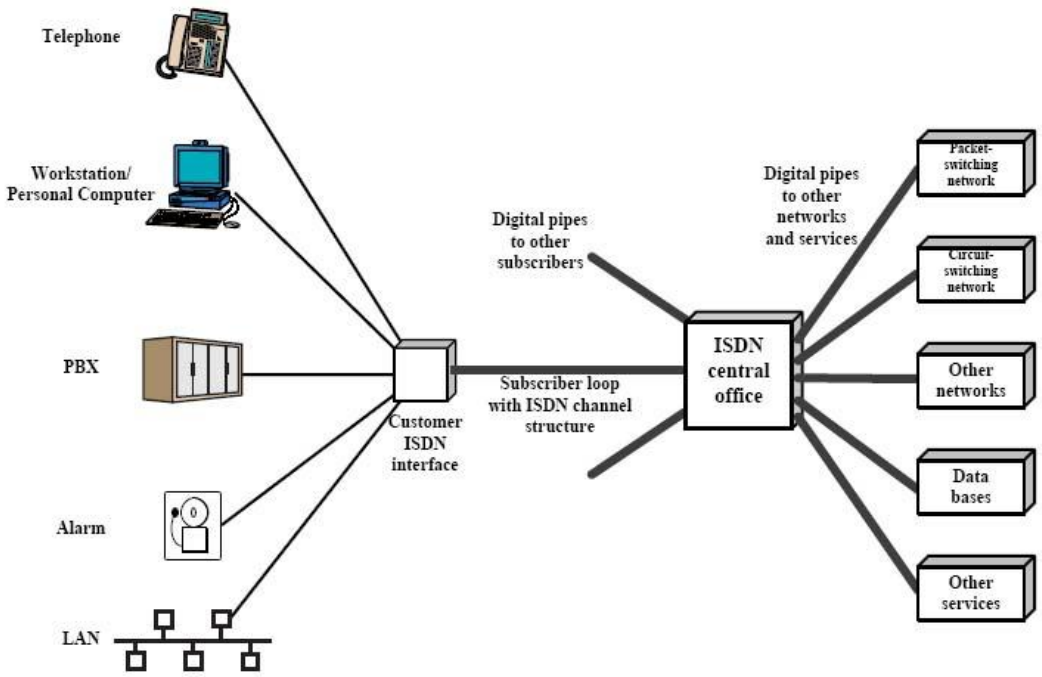


Figure 5.3 Conceptual View of ISDN Connection Features

- User has access to ISDN via a local interface to a digital "pipe".
- Pipes of various sizes are available to satisfy different needs
- Pipe to the user's promises has a fixed capacity but the traffic on the pipe may be a variable mix up to the capacity limit
- ISDN requires control signals to instruct how to sort out the time-multiplexed data and provide the required services
- Control signals are multiplexed onto the same digital pipe
- Recommendation from I.410: more than one size of pipe is needed
    - A single terminal (e.g. a residential telephone)
    - Multiple terminals (e.g. a residential telephone, PC, and alarm system)
    - A network of devices attached to a LAN or PBX (ISDN gateway**)**

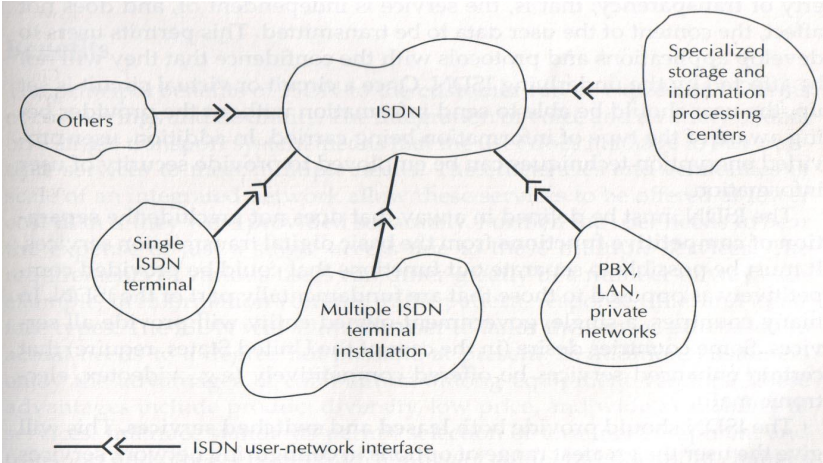


FIGURE 4.5 ISDN User–Network Interface Examples

- The principle benefits of ISDN to the customer can be expressed in terms of cost savings and flexibility
- Integrated voice and data means that the user does not have to buy multiple services to meet multiple needs
    - Access charges to a single line only
    - Purchasing services based on actual needs
    - Product diversity, low price, and wide availability of equipment

ISDN Architecture

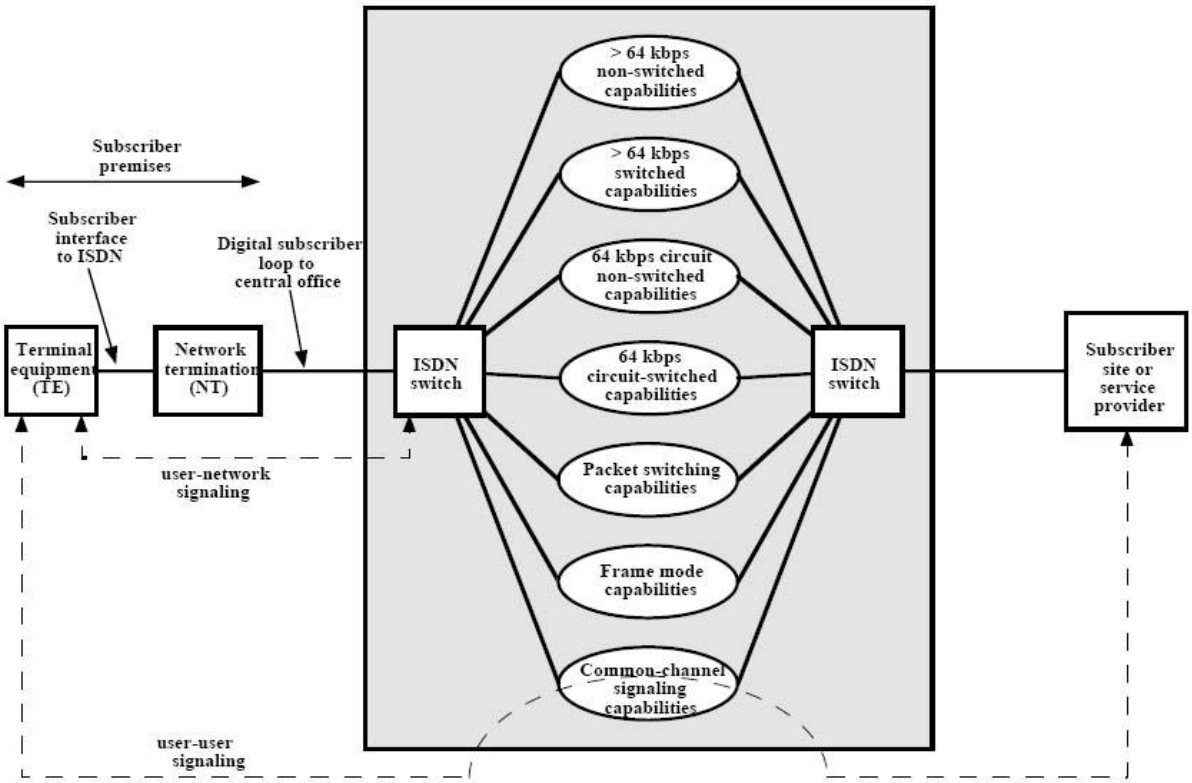


Figure 5.5 ISDN Architecture

- Physical interface provides a standardized means of attaching to the network
- The interface supports a basic service consisting of three time-multiplexed channels, two at 64 kbps and one at 16 kbps
- In addition, there is a primary service that provide multiple 64-kbps channels
- An interface is defined between the customer's terminal equipment (TE) and a device on the customer's premises, known as a network termination (NT)
- The subscriber loop is the physical path from the subscriber's NT to the ISDN central office
    - Must support full-duplex digital transmission for both basic and primary data rates

ISDN Standard

Issue	Protocol	Key Examples
Telephone Network and ISDN	E-Series	E.164 – International Telephone Numbering Plan
ISDN Concepts, Aspects and Interfaces	I-Series	I.100 Series – Concepts, Structures, Terminology I.400 - User-Network Interface (UNI)
Switching and Signaling	Q-Series	Q.921 – LAPD (Link Access Procedure on the D channel) Q.931 – ISDN Network Layer between Terminal and Switch

Transmission Structure

- Digital pipe between central office and ISDN subscriber carry a number of communication channels, varies from user to user
- The transmission structure of access links includes channels of:
    - B channel: 64 kbps
    - D channel: 16 or 64 kbps
    - H channel: 384 (H_0), 1536 (H_{11}), or 1920 (H_{12}) kbps

B Channel

- A user channel, carrying digital data, PCM-encoded digital voice, or a mixture of lower-rate traffic at a fraction of 64 kbps
- **The information is carried in frame format, using either high-level data link control (HDLC) or PPP as the Layer 2 protocol. PPP is more robust than HDLC because it provides a mechanism for authentication and negotiation of compatible link and protocol configuration**

ISDN Channel Functions

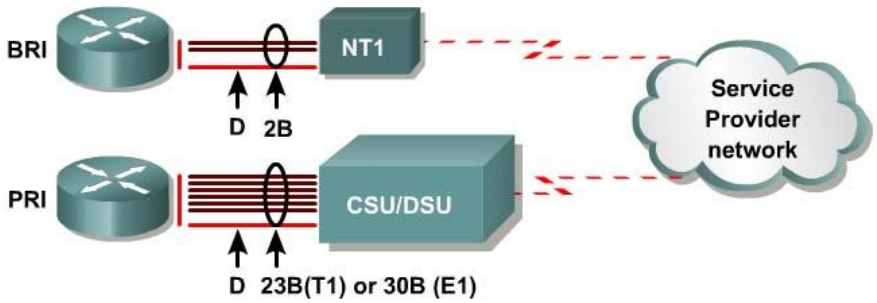
TABLE 5.1 ISDN Channel Functions

B Channel (64 kbps)	D Channel (16 kbps)
Digital voice	Signaling
64-kbps PCM	Basic
Low bit rate (32 kbps)	Enhanced
High-speed data	Low-speed data
Circuit-switched	Videotex
Packet-switched	Terminal
Other	Telemetry
Facsimile	Emergency services
Slow-scan video	Energy management

H Channel

- Provides user information transmission at higher data rates
- Use the channel as a high-speed trunk or subdivide it based on TDM
- Examples: fast fax, video, high-speed data, high quality audio

Basic and Primary Channel Structures

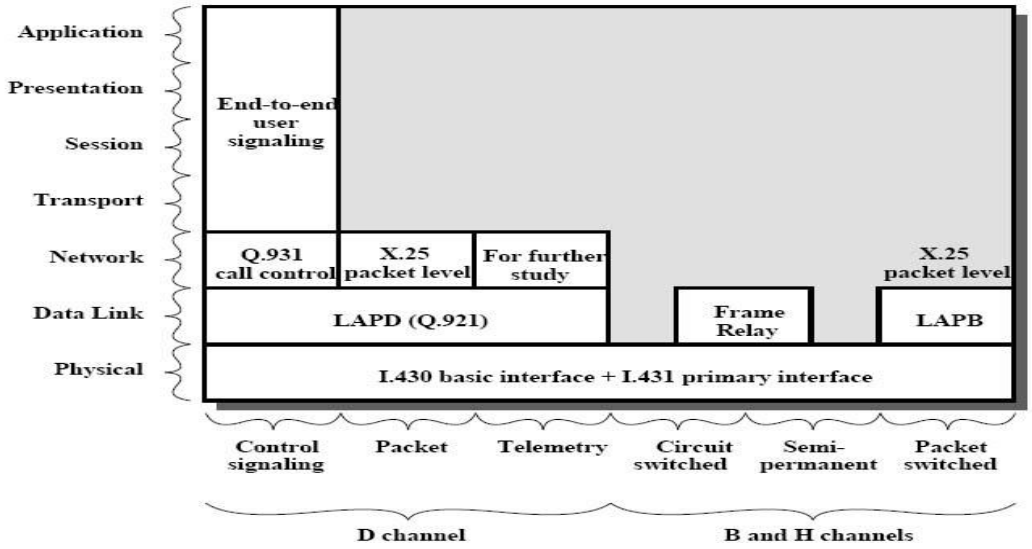


Channel	Capacity	Mostly Used for
B	64 kbps	Circuit-switched data (HDLC, PPP)
D	16/64 kbps	Signaling information (LAPD)

ISDN Model

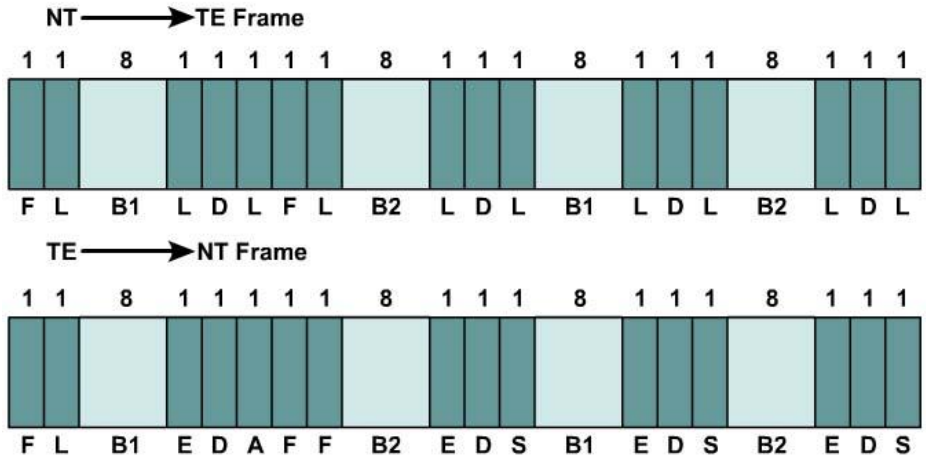
OSI Layer	D-Channel	B-Channel
3	Q.931 - ISDN Network Layer between Terminal and Switch	IP
2	Q.921 – LAPD (Link Access Procedure on the D channel)	PPP HDLC
1	I.430/I.431 – ISDN physical-layer interface: • I.430 for the basic interface • I.431 for the primary interface	

ISDN Protocols at the user-network interface



ISDN Physical Layer

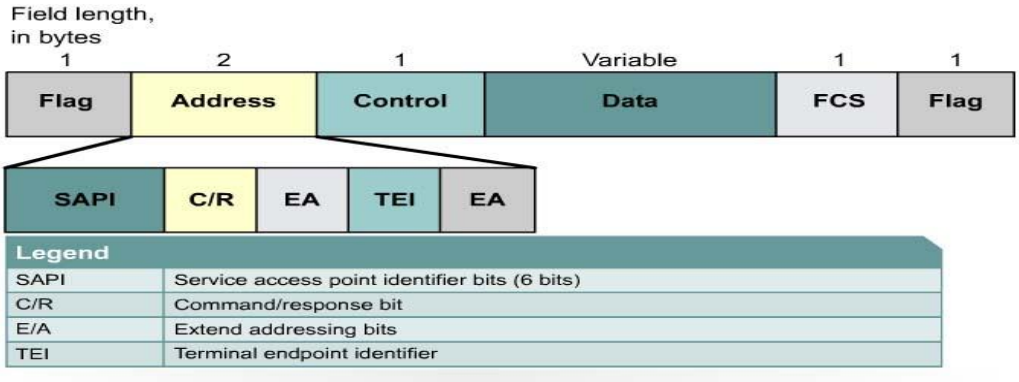
- Each ISDN BRI frame contains two sub-frames each containing the following:
  - 8 bits from the B1 channel, 8 bits from the B2 channel, 2 bits from the D channel, and 6 bits of overhead
- So, each BRI frame contains 48 bits



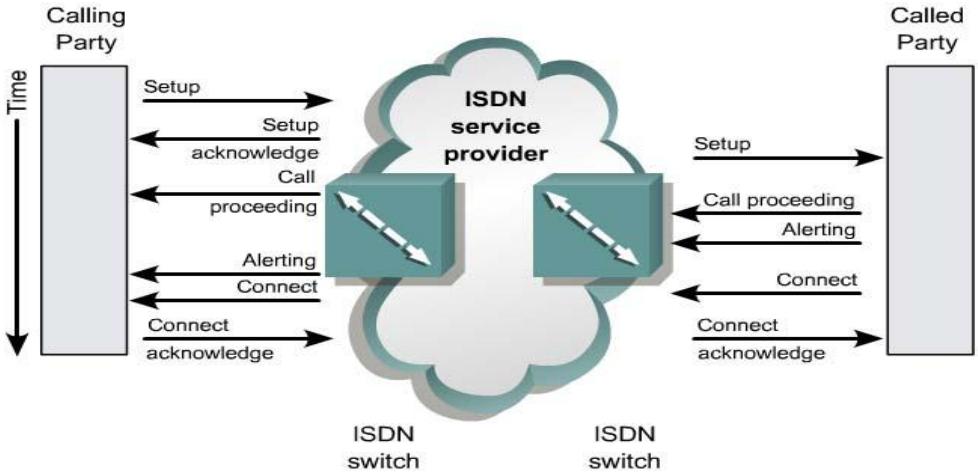
- The overhead bits of an ISDN sub-frame are used as follows**:**
  - **Framing bit — Provides synchronization**
  - **Load balancing bit- Adjusts the average bit value**
  - **Echo of previous D channel bits — Used for contention resolution when several terminals on a passive bus contend for a channel**
  - **Activation bit — Activates devices**
  - **Spare bit — Unassigned**
- 4,000 frames are transmitted per second.

- Each B channel, B1and B2, has a capacity of 8 * 4000 * 2 = 64 kbps, while channel D has a capacity of 2 * 4000 * 2 = 16 kbps.
- This accounts for 144 kbps (B1 + B2 + D) of the total ISDN BRI physical interface bit rate of 192 kbps.
- The remainder of the data rate are the overhead bits that are required for transmission: 6 * 4000 * 2 = 48 kbps.

ISDN Data-link Layer



ISDN Layer 3: Q.931 Messaging Call Setup



Reference Points and Functional Groupings

- ITU-T approach for actual user's physical configuration
  - Functional grouping: certain arrangements of physical equipment or combination of equipment
    - NT1, NT2, TE1, TE2, TA
  - Reference points: conceptual points of separation of group function
    - R, S, T, U

Functional Groupings

- NT1 (Network Termination 1)

- Includes functions similar to OSI layer 1
- May be controlled by ISDN provider (a boundary to network)
- Isolate the user from the transmission technology of subscriber loop
- Supports multiple channels (e.g. 2B+D) using TDM
- Might support multiple devices in a multidrop arrangement
    - E.g. a residential interface might include a telephone, PC, and alarm system, all attached to a single NT1 interface via a multidrop line

- NT2 (Network Termination 2)
    - An intelligent device that may include up to OSI layer 3
    - Perform switching and concentration functions
        - Switching: the construction of a private network using semi-permanent circuit among a number of sites
        - Concentration: multiple devices, attached to a digital PBX, LAN, or terminal controller, may transmit data across ISDN
    - E.g. digital PBX, a terminal controller, LAN
        - Digital PBX provides NT2 functions at layers 1, 2, and 3
        - A simple terminal controller provides layers 1 and 2
        - A simple Time Division MUX provides layer 1
- TE1 (Terminal Equipment type 1)
    - Devices that support the standard ISDN interface
    - E.g. digital telephone, integrated voice/data terminal, digital fax
- TE2 (Terminal Equipment type 2)
    - The existing non-ISDN equipment
    - E.g. physical interface RS-232, host computer with X.25
    - Requires a terminal adaptor (TA) to plug into an ISDN interface
- TA (Terminal Adaptor)
    - Converts standard electrical signals into the form used by ISDN
    - Needed for connection with TE2 devices
    - The ISDN TA can be either a standalone device or a board inside the TE2

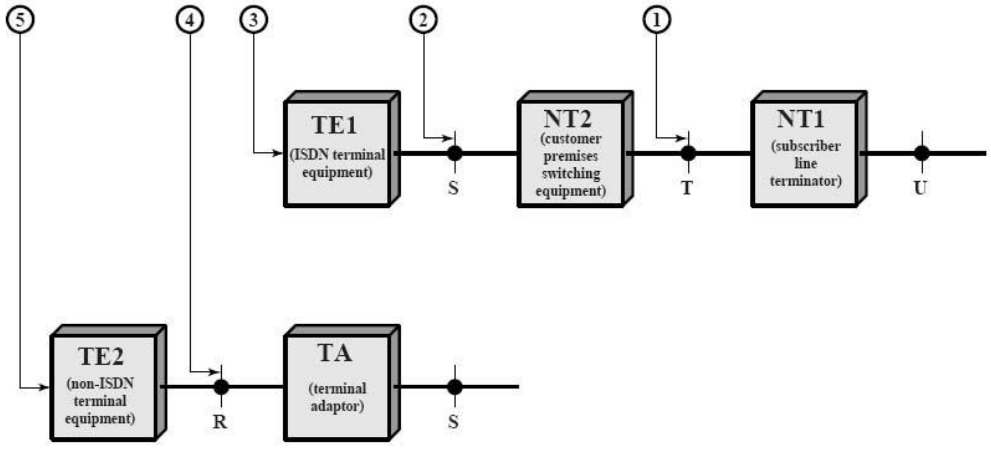


Figure 6.2 ISDN Reference Points and Functional Groupings

Reference Points

- Reference point R (connect TE2-TA)
  - Provides a non-ISDN interface between user equipment that is non-ISDN compatible and adaptor equipment
  - Comply with X or V series ITU-T recommendation
- Reference point S (connect TE1-NT2, TA-NT2)
  - The interface of individual ISDN terminals
  - Separate user terminal from network communications functions
- Reference point T (connect NT2-NT1)
  - A minimal ISDN network termination at CPE
  - Separate network's provider equipment from the user's one
- Reference point U (connect NT1-provider)

Describes full-duplex data signal on the subscriber line

Pondicherry University Questions

2 Marks

1. Define IEEE 802.5 LAN Protocol? (UQ April 2013) (Ref.Pg.No.5Qn.No.17)
2. Define Fiber Distributed Data Interface? (UQ APRIL 2013) (Ref.Pg.No.7 Qn.No.26)
3. Define in Point-to-Point Protocols? (UQ NOV 2013& April 2013) (Ref.Pg.No. 9 Qn.No.32)
4. What are the servers included in lane?(UQ NOV 2013) (Ref.Pg.No.10Qn.No.38)

11 Marks

(Regular)

1. Explain about Fiber Distributed Data Interface?(UQ NOV 2013) (Ref.Pg.No.19 Qn.No.8)
2. Explain in detail about Address Resolution Protocol and Inverse ARP?(UQ NOV 2013) Ref.Pg.No.11 Qn.No.1)

(Arrear)

3. Write in detail Wireless LAN by IEEE 802.11 protocols?(UQ APRIL 2013) Ref.Pg.No.17 Qn.No.7)
4. Explain in detail about SONET/SDH?(UQ APRIL 2013)(Ref.Pg.No.17 Qn.No.33)
5. Explain the various functions ISDN? (UQ April 2013) (Ref.Pg.No.35 Qn.No.18)

SRI VENKATESHWARAA COLLEGE OF ENGINEERING & TECHNOLOGY

(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry.)
13-A, Villupuram – Pondy Main road, Ariyur, Puducherry – 605 102.
Phone: 0413-2644426, Fax: 2644424 / Website: www.svcetpondy.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Subject: NETWORK PROTOCOL **Subject Code: CS E77**

UNIT V

Network Security Protocols: SSH, RADIUS, SSL, Kerberos, TLS, IPSec, Voice over IP.

Faculty Incharge **HOD** **PRINCIPAL**

2 Marks

1. Write about SSH protocol?

SSH is a protocol for secure remote login and other secure network services over an insecure network. SSH consists of three major components:

1. The Transport Layer Protocol [SSH-TRANS]
2. The User Authentication Protocol [SSH-USERAUTH
3. The Connection Protocol [SSH-CONNECT]

2. Write about the Transport Layer Protocol

The Transport Layer Protocol [SSH-TRANS]provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream. SSH-Trans provides strong encryption, cryptographic host authentication, and integrity protection. Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

3. Write about the User Authentication Protocol

The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol SSH-TRANS. When SSH-USERAUTH starts, it receives the session identifier from the lower-level protocol (this is the exchange hash H from the first key exchange). The session identifier uniquely identifies this session and is suitable for signing in order to prove ownership of a private key. SSH-USERAUTH also needs to know whether the lower-level protocol provides confidentiality protection.

4. Write about the Connection Protocol

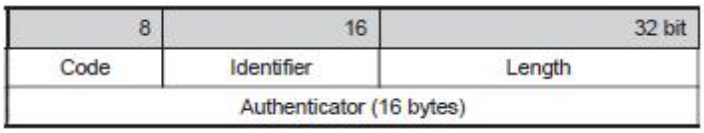
The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol. It provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above. The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and X11 connections.

5. Write about RADIUS (Nov 13)

RADIUS stands for Remote Authentication Dial In User Service.RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS uses UDP as the transport protocol. RADIUS also carries accounting information between a Network Access Server and a shared Accounting Server.

6. Draw the Protocol Structure of RADIUS (Nov 13)



7. Write about Kerberos

Kerberos is a network authentication protocol. Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography, i.e., shared secret key.

8. Write short notes on TLS (Nov 13)

Transport Layer Security (TLS) Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (TCP) is the TLS Record Protocol.

9. List out the properties of TLS Record Protocol (Nov 13)

The TLS Record Protocol provides connection security that has two basic properties:

• Private - Symmetric cryptography is used for data encryption (DES, RC4, etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record
Protocol can also be used without encryption.

• Reliable - Message transport includes a message integrity check using a keyed MAC. Secure hash functions (SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

10. List out the properties of the TLS Handshake Protocol

. The TLS Handshake Protocol provides connection security that has three basic properties:

1. The peer's identity can be authenticated using asymmetric, or public key, cryptography (RSA, DSS, etc.). This authentication can be made optional, but is generally required for at least one of the peers.

2. The negotiation of a shared secret is secure: The negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.

3. The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

11. Write about IPsec

Internet Security architecture (IPsec) defines the security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

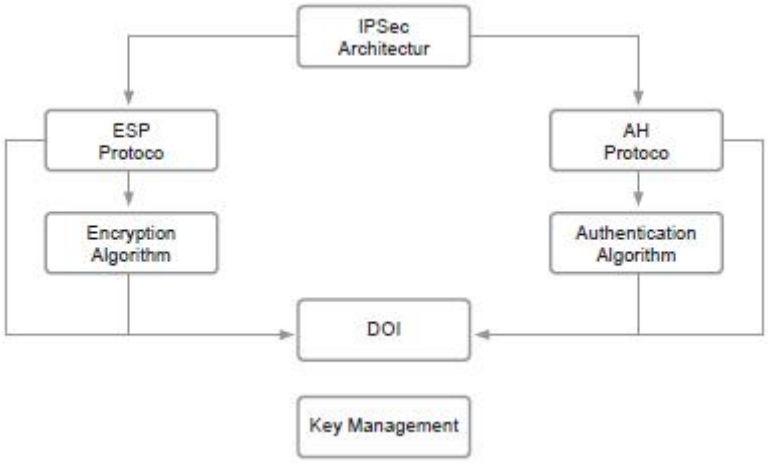
12. Write out the set of security services that IPsec

The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity),

confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc.

13. Draw the protocol Structure of IPsec

IPsec Architecture includes many protocols and algorithms. The relationship of these protocols are displayed as follows:



14. Write about VOIP Protocols (April 13)

Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. Using VOIP protocols, voice communications can be achieved on any IP network regardless whether it is Internet, Intranet or Local Area Networks (LAN). In a VOIP enabled network, the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. VOIP signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. The key benefits of Internet telephony (Voice over IP) are the very low cost, the integration of data, voice and video on one network, the new services created on the converged network and simplified management of end user and terminals.

15. Write about H.323

H.323 is the ITU-T's standard, which was originally developed for multimedia conferencing on LANs, but was later extended to cover Voice over IP. The standard encompasses both point to point communications and multipoint conferences. H.323 defines four logical components: Terminals, Gateways, Gatekeepers and Multipoint Control Units (MCUs). Terminals, gateways and MCUs are known as endpoints.

16. Write about SIP

Session Initiation Protocol (SIP) is the IETF's standard for establishing VOIP connections. SIP is an application layer control protocol for creating, modifying and terminating sessions with one or more participants. The architecture of SIP is similar to that of HTTP (client-server protocol). Requests are generated by the client and sent to the server. The server processes the requests and then sends a response to the client. A request and the responses for that request make a transaction.

17. Write about MGCP

Media Gateway Control Protocol (MGCP) is a Cisco and Telcordia proposed VOIP protocol that defines communication between call control elements (Call Agents or Media Gateway) and telephony gateways. MGCP is a control protocol, allowing a central coordinator to monitor events in IP phones and gateways and instructs them to send media to specific addresses. In the MGCP architecture, The call control intelligence is located outside the gateways and is handled by the call control elements (the Call

Agent). Also the call control elements (Call Agents) will synchronize with each other to send coherent commands to the gateways under their control.

18. Write the key issues of VOIP (April 13)

1. The VOIP industry has been working on addressing the following key issues
2. Quality of voice
3. Interoperability
4. Security
5. Integration with Public Switched Telephone Network(PSTN
6. Scalability

19. What is the function of Secure Socket layer? (April 13)

Secure socket layer is used to provide the security protocol used by the Internet to provide an easy access to the websites.

- It provides a way to validate or identify the website by creating the information file and making the accessing possible.
- It creates an encrypted connection that provides the sending of the data from one source to another using the SSL.
- SSL provides a way to ensure that the security is being provided to the transaction and the data in use.
- The lock is used to display the browsers connection is closed or opened on the secure channel of SSL or TLS.

20. What is PPP? (April 13) (Nov 13)

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

11 Marks

1. Write in detail Secure Shell Protocol (5 marks)

Protocol Description

SSH is a protocol for secure remote login and other secure network services over an insecure network. SSH consists of three major components:

The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream. SSH-Trans provides strong encryption, cryptographic host authentication, and integrity protection. Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol SSH-TRANS. When SSH-USERAUTH starts, it receives the session identifier from the lower-level protocol (this is the exchange hash H from the first key exchange). The session identifier uniquely identifies this session and is suitable for signing in order to prove ownership of a private key. SSH-USERAUTH also needs to know whether the lower-level protocol provides confidentiality protection.

The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol. It provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above. The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and X11 connections.

2. Write in detail Remote Authentication Dial in User Service (6 marks)

Protocol Description

RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS uses UDP as the transport protocol. RADIUS also carries accounting information between a Network Access Server and a shared Accounting Server.

Key features of RADIUS are:

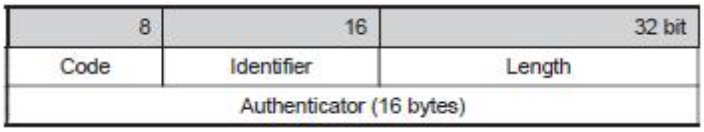
Client/Server Model: A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

Network Security: Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an insecure network could determine a user's password.

Flexible Authentication Mechanisms: The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms.

Extensible Protocol: All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

Protocol Structure



• Code - The message types are described as follows:
1 -Access-Request
2 -Access-Accept
3 -Access-Reject
4 -Accounting-Request
5 - Accounting-Response
11- Access-Challenge
12 -Status-Server (experimental)
13 -Status-Client (experimental)
255- Reserved
• Identifier - The identifier matches requests and replies.
• Length - The message length including the header.
• Authenticator - A field used to authenticate the reply from the radius server and in the password hiding algorithm.

3. Write in detail Kerberos (6 marks) (April 13)

Protocol Description

Kerberos is a network authentication protocol. Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography, i.e., shared secret key.

The authentication process proceeds as follows: A client sends a request to the authentication server (AS) requesting "credentials" for a given server. The AS responds with these credentials, encrypted in the client's key. The credentials consist of 1) a "ticket" for the server and 2) a temporary encryption key (often called a "session key"). The client transmits the ticket (which contains the client's identity and a copy of the session key, both encrypted in the server's key) to the server. The session key (now shared by the client and server) is used to authenticate the client, and may optionally be used to authenticate the server. It may also be used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

The authentication exchanges mentioned above require read only access to the Kerberos database. Sometimes, however, the entries in the database must be modified, such as when adding new principals or changing a principal's key. This is done using a protocol between a client and a third

Kerberos server, the Kerberos Administration Server (KADM). The administration protocol is not described in this document. There is also a protocol for maintaining multiple copies of the Kerberos database, but this can be considered an implementation detail and may vary to support different database technologies.

Protocol Structure

Kerberos messages:

The Client/Server Authentication Exchange

Message direction	**Message type**
1. Client to Kerberos	KRB_AS_REQ
2. Kerberos to client	KRB_AS_REP or KRB_ERROR

The Client/Server Authentication Exchange

Message direction	**Message type**
Client to Application server	KRB_AP_REQ
[optional] Application server to client	KRB_AP_REP or KRB_ERROR

The Ticket-Granting Service (TGS) Exchange

Message direction	**Message type**
1. Client to Kerberos	KRB_TGS_REQ
2. Kerberos to client	KRB_TGS_REP or KRB_ERROR

The KRB_SAFE Exchange

The KRB_PRIV Exchange

The KRB_CRED Exchange

4. Write in detail Transport Layer Security Protocol (11 marks)

Protocol Description

Transport Layer Security (TLS) Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (TCP) is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- Private - Symmetric cryptography is used for data encryption (DES, RC4, etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.
- Reliable - Message transport includes a message integrity check using a keyed MAC. Secure hash functions (SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

The TLS Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties:

1. The peer's identity can be authenticated using asymmetric, or public key, cryptography (RSA, DSS, etc.). This authentication can be made optional, but is generally required for at least one of the peers.

2. The negotiation of a shared secret is secure: The negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.
3. The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

TLS is based on the Secure Socket Layer (SSL), a protocol originally created by Netscape. One advantage of TLS is that it is application protocol independent. The TLS protocol runs above TCP/IP and below application protocols such as HTTP or IMAP. The HTTP running on top of TLS or SSL is often called HTTPS. The TLS standard does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers and implementers of protocols which run on top of TLS.

Protocol Structure

TLS protocol includes two protocol groups: TLS Record Protocol and TLS Handshake Protocols, which have many messages with different formats. We only summarize the protocols here without details, which can be found in the reference documents.

TLS Record Protocol is a layered protocol. At each layer, messages may include fields for length, description, and content. The Record Protocol takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. Received data is decrypted, verified, decompressed, and reassembled, then delivered to higher level clients.

TLS connection state is the operating environment of the TLS Record Protocol. It specifies a compression algorithm, encryption algorithm, and MAC algorithm.

TLS Record Layer receives uninterrupted data from higher layers in non-empty blocks of arbitrary size. Key calculation: The Record Protocol requires an algorithm to generate keys, IVs, and MAC secrets from the security parameters provided by the handshake protocol.

TLS Handshake Protocol: consists of a suite of three sub-protocols which are used to allow peers to agree upon security parameters for the record layer, authenticate themselves, instantiate negotiated security parameters, and report error conditions to each other.

Change cipher spec protocol
Alert protocol
Handshake protocol

5. Explain about IPSec (11 marks) (April 13)

Protocol Description

Internet Security architecture (IPsec) defines the security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more “paths” between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPsec protocols employed in any context, and the

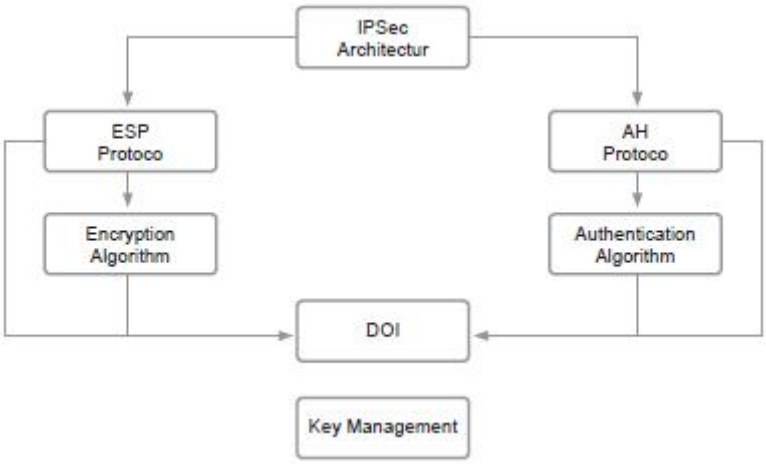
ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations.

When these mechanisms are correctly implemented and deployed, they ought not to adversely affect users, hosts, and other Internet components that do not employ these security mechanisms for protection of their traffic. These mechanisms also are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting the other parts of the implementation. For example, different user communities may select different sets of algorithms (creating cliques) if required.

A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.

Protocol Structure

IPsec Architecture includes many protocols and algorithms. The relationships of these protocols are displayed as follows:



6. Explain about VOIP Protocols (11 marks) (Nov 13)

Description

Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. Using VOIP protocols, voice communications can be achieved on any IP network regardless whether it is Internet, Intranet or Local Area Networks (LAN). In a VOIP enabled network, the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. VOIP signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. The key benefits of Internet telephony (Voice over IP) are the very low cost, the integration of data, voice and video on one network, the new services created on the converged network and simplified management of end user and terminals.

There are a few VOIP protocol stacks which are derived by various standard bodies and vendors, namely H.323, SIP, MEGACO and MGCP.

H.323 is the ITU-T's standard, which was originally developed for multimedia conferencing on LANs, but was later extended to cover Voice over IP. The standard encompasses both point to point communications and multipoint conferences. H.323 defines four logical components: Terminals, Gateways, Gatekeepers and Multipoint Control Units (MCUs). Terminals, gateways and MCUs are known as endpoints.

Session Initiation Protocol (SIP) is the IETF's standard for establishing VOIP connections. SIP is an application layer control protocol for creating, modifying and terminating sessions with one or more

participants. The architecture of SIP is similar to that of HTTP (client-server protocol). Requests are generated by the client and sent to the server. The server processes the requests and then sends a response to the client. A request and the responses for that request make a transaction.

Media Gateway Control Protocol (MGCP) is a Cisco and Telcordia proposed VOIP protocol that defines communication between call control elements (Call Agents or Media Gateway) and telephony gateways. MGCP is a control protocol, allowing a central coordinator to monitor events in IP phones and gateways and instructs them to send media to specific addresses. In the MGCP architecture, The call control intelligence is located outside the gateways and is handled by the call control elements (the Call Agent). Also the call control elements (Call Agents) will synchronize with each other to send coherent commands to the gateways under their control.

The Media Gateway Control Protocol (Megaco) is a result of joint efforts of the IETF and the ITU-T (ITU-T Recommendation H.248). Megaco/H.248 is a protocol for the control of elements in a physically decomposed multimedia gateway, which enables separation of call control from media conversion. Megaco/H.248 addresses the relationship between the Media Gateway (MG), which converts circuit-switched voice to packet-based traffic, and the Media Gateway Controller, which dictates the service logic of that traffic. Megaco/H.248 instructs an MG to connect streams coming from outside a packet or cell data network onto a packet or cell stream such as the Real-Time Transport Protocol (RTP). Megaco/H.248 is essentially quite similar to MGCP from an architectural standpoint and the controller-to-gateway relationship, but Megaco/H.248 supports a broader range of networks, such as ATM.

In the past few years, the VOIP industry has been working on addressing the following key issues

Quality of voice - As IP was designed for carrying data, it does not provide real time guarantees but only provides best effort service. For voice communications over IP to become acceptable to users, the packet delay and getter needs to be less than a threshold value.

Interoperability - In a public network environment, products from different vendors need to operate with each other for Voice over IP to become common among users.

Security - Encryption (such as SSL) and tunneling (L2TP) technologies have been developed to protect VOIP signaling and bear traffic.

Integration with Public Switched Telephone Network (PSTN) - While Internet telephony is being introduced; it will need to work in conjunction with PSTN in the foreseeable future. Gateway technologies are being developed to bridge the two networks.

Scalability - VOIP systems need to be flexible enough to grow to the large user market for both private and public services. Many network management and user management technologies and products are being developed to address the issue.

Key VOIP Protocols

The key protocols for AAA and VPN:

Signaling

ITU-T H.323

H.323: Packet-based multimedia communications (VoIP) architecture
H.225: Call Signaling and RAS in H.323 VOIP Architecture
H.235: Security for H.323 based systems and communications
H.245: Control Protocol for Multimedia Communication
T.120: Multipoint Data Conferencing Protocol Suite

IETF

Megaco / H.248: Media Gateway Control protocol
MGCP: Media Gateway Control Protocol
RTSP: Real Time Streaming Protocol

SIP: Session Initiation Protocol
SDP: Session Description Protocol
SAP: Session Announcement Protocol

Cisco Skinny

SCCP: Skinny Client Control Protocol

Media/CODEC

G.7xx: Audio (Voice) Compression Protocols (G.711, G.721, G.722, G.723, G.726, G.727. G.728, G.729)
H.261: Video Coding and Decoding (CODEC)
H.263: Video Coding and Decoding (CODEC)
RTP: Real Time Transport Protocol
RTCP: RTP Control Protocol

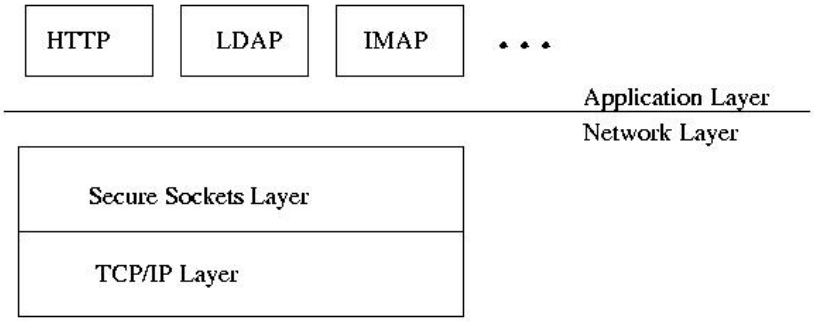
Others

COPS: Common Open Policy Service
SCTP: Stream Control Transmission Protocol
TRIP: Telephony Routing Over IP

7. Explain about SSL Protocol (11 marks) (Nov 13)

The Transmission Control Protocol/Internet Protocol (TCP/IP) governs the transport and routing of data over the Internet. Other protocols, such as the Hypertext Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), or Internet Messaging Access Protocol (IMAP), run "on top of" TCP/IP in the sense that they all use TCP/IP to support typical application tasks such as displaying web pages or running email servers.

Figure 1 SSL runs above TCP/IP and below high-level application protocols



The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

These capabilities address fundamental concerns about communication over the Internet and other TCP/IP networks:

- SSL server authentication allows a user to confirm a server's identity. SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs. This confirmation might be important if the user, for example, is sending a credit card number over the network and wants to check the receiving server's identity.
- SSL client authentication allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's

certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs. This confirmation might be important if the server, for example, is a bank sending confidential financial information to a customer and wants to check the recipient's identity.

- An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality. Confidentiality is important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering--that is, for automatically determining whether the data has been altered in transit.

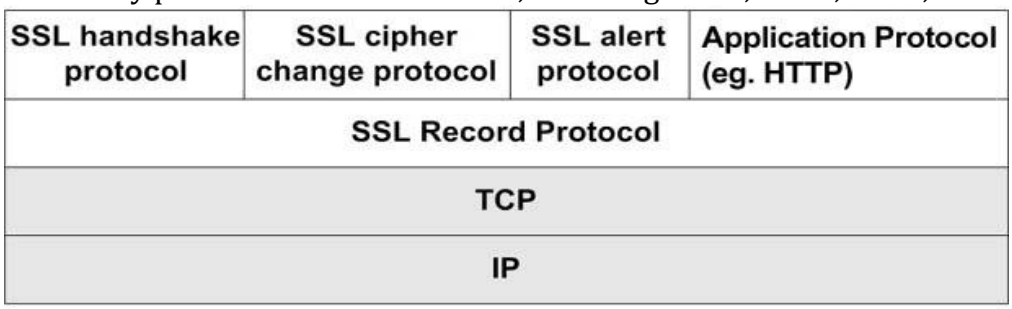
The SSL protocol includes two sub-protocols: the SSL record protocol and the SSL handshake protocol. The SSL record protocol defines the format used to transmit data. The SSL handshake protocol involves using the SSL record protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection. This exchange of messages is designed to facilitate the following actions:

- Authenticate the server to the client.
- Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
- Optionally authenticate the client to the server.
- Use public-key encryption techniques to generate shared secrets.
- Establish an encrypted SSL connection.

SSL technology is used to establish a secure and encrypted communication channel between two Internet connected devices.

SSL and the Protocol Stack

- SSL between Transmission Control Protocol (TCP) layer and Application layer
- Actually 2 layers
  - Record
  - Secure Application
- Can run under any protocol that relies on TCP, including HTTP, LDAP, POP3, FTP



The Four Upper Layer Protocols

- Handshaking Protocol
  - Establish communication variables
- ChangeCipherSpec Protocol
  - Alert to a change in communication variables
- Alert Protocol
  - Messages important to SSL connections
- Application Encryption Protocol
  - Encrypt/Decrypt application data

Record Layer

- Frames and encrypts upper level data into one protocol for transport through TCP
- 5 byte frame
    - 1st byte protocol indicator
    - 2nd byte is major version of SSL
    - 3rd byte is minor version of SSL
    - Last two bytes indicate length of data inside frame, up to 2^{14}
- Message Authentication Code (MAC)

Message Authentication Code

- MAC secures connection in two ways
    - Ensure Client and Server are using same encryption and compression methods
    - Ensure messages sent were received without error or interference
- Both sides compute MACs to match them
- No match = error or attack

Pondicherry University Questions

2 Marks

1. Write about RADIUS (UQ NOV 2013) (Ref.Pg.No.2 Qn.No.5)
2. Draw the Protocol Structure of RADIUS (UQ NOV 2013) (Ref.Pg.No.2 Qn.No.6)
3. Write short notes on TLS (UQ NOV 2013) (Ref.Pg.No.3 Qn.No.8)
4. List out the properties of TLS Record Protocol (UQ NOV 2013) (Ref.Pg.No.9 Qn.No.9)
5. 14. Write about VOIP Protocols (UQ April 2013) (Ref.Pg.No.4 Qn.No.14)
6. 18. Write the key issues of VOIP (UQ April 2013) (Ref.Pg.No.5 Qn.No.18)
7. 19. What is the function of Secure Socket layer? (UQ April 2013) (Ref.Pg.No.5 Qn.No.19)
8. 20. What is PPP? (UQ April, Nov 2013) (Ref.Pg.No.5 Qn.No.20)

11 Marks

(Regular)

1. Explain about VOIP Protocols (11 marks) (UQ NOV 2013) (Ref.Pg.No.10 Qn.No.6)
2. Explain about SSL Protocol (11 marks) (UQ NOV 2013) (Ref.Pg.No.12 Qn.No.7)

(Arrear)

3. Write in detail Kerberos (6 marks) (April 13) 7 (UQ April 2013) (Ref.Pg.No.7 Qn.No.3)
4. Explain about IPSec (11 marks) (UQ April 2013) (Ref.Pg.No.9 Qn.No.5)