UNIT V -APPLICATION LAYER

WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP.

PART A

1. What is the function (Define) of SMTP? (May & Nov 2015)

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

2. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

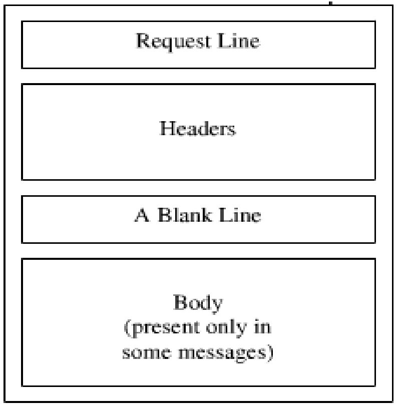
3. How doesMIME (Differ) enhance SMTP? (Nov/Dec 2007)(Or) State the difference between SMTP and MIME (NOV/DEC 2014)

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

4. Why is an application such as POP needed for electronic messaging?

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

5. Give the format of HTTP request message?



6. What is the purpose of Domain Name System?

Domain Name System can map a name to an address and conversely an address to name.

7. Discuss the three main division of the domain name space.

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.

Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.

Country domain: Uses two characters to identify a country as the last suffix.

Inverse domain:Finds the domain name given the IP address.

8. Define CGI?

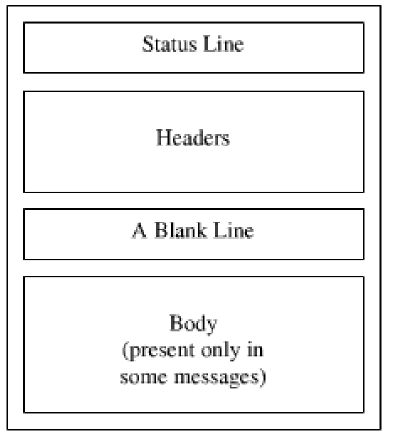
CGI is a standard for communication between HTTP servers and executable programs. It is used in crating dynamic documents.

9. What are the requests messages support SNMP and explain it?

- GET
- SET

The former is used to retrieve a piece of state from some node and the latter is used to store a new piece of state in some node.

10. Give the format of HTTP response message?



11. Why name services are sometimes called as middleware?

Name services are sometimes called middleware because they fill a gap between applications and the underlying network

12. What are the types of DNS Message

Two types of messages

- Query: header and question records
- Response: Header, question records, answer records, authoritative records, and additional records.

13. What is POP3? (Nov 2016)

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/serverprotocol in which e-mail is received and held for you by your Internet server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet.

14. What is IMAP4? (Nov 2016)

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which e-mail is received and held for you by your Internet server.IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

15.What is DNS? (Apr /may 2010)

The **DNS** translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

16. What is persistent HTTP?What are the advantages of allowing persistent TCP Connections in HTTP?(May 2013) (Nov 2016)

HTTP persistent connection, also called HTTP keep-alive, or HTTP connection reuse, is the idea of using a single TCP connection to send and receive multiple HTTP requests/responses, as opposed to opening a new connection for every single request/response pair.

Persistent HTTP connections have a number of advantages:

- By opening and closing fewer TCP connections, CPU time is saved in routers and hosts (clients, servers, proxies, gateways, tunnels, or caches), and memory used for TCP protocol control blocks can be saved in hosts.

17. Is a cryptographic hash function, an irreversible mapping? Justify your answer.

1. It is really, really hard to infer the input from the hash **because there are an infinite amount of input strings that will generate the same output** (irreversible property).
2. However, ***finding*** even a single instance of multiple input strings that generate the same output is also really, really hard (collision resistant property).

18. Define SNMP?

SNMP is a frame work for managing devices in an internet using TCP/IP suite. It provides fundamental operations for monitoring and maintaining an internet.

19. What DNS cache issues are involved in changing the IP address of a webServer host name? Nov/Dec 2013

The Domain Name System supports DNS cache servers which store DNS query results for a period of time determined in the configuration (time-to-live) of the domain name record in question. Typically, such caching DNS servers, also called DNS caches, also implement the recursive algorithm necessary to resolve a given name starting with the DNS root through to the authoritative name servers of the queried domain. With this function implemented in the name server, user applications gain efficiency in design and operation.

20.Differentiate application programs and application protocols. Nov/Dec 2013

An application program (sometimes shortened to application) is any program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of application programs include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs. Application programs use the services of the computer'soperating system and other supporting programs.

Application protocols govern various processes, such as the process for downloading a web page, or for sending e-mail. The application protocol directs how these processes are done.

21. What are the two mainly used application protocols

- SimpleMail Transfer Protocol (SMTP) is used to exchangeelectronic mail.
- Hypertext Transport Protocol (HTTP) is used to communicatebetween web browsers and web servers.

22.Define HTTP protocol .

HTTP PROTOCOL

- Protocol for transfer of data between Web servers and Web clients (browsers).
- “The Hypertext Transfer Protocol (HTTP) is an **application-level protocol** for **distributed**, collaborative, hypermedia information systems.
- Popular Web servers:
  - Apache HTTPD, JBoss and Tomcat
- Popular Web clients:
  - Firefox and Opera

23. Define web services.

The term *Web services* describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDIopenstandards over an Internet protocolbackbone. SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

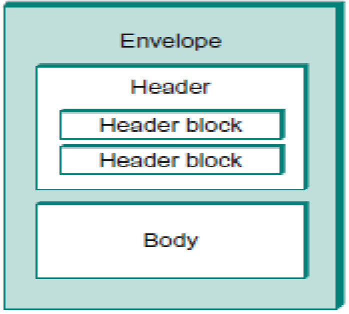
24. What is SOAP?

- SOAP stands for Simple Object Access Protocol
- SOAP is a communication protocol
- SOAP is for communication between applications
- SOAP is a format for sending messages
- SOAP communicates via Internet
- SOAP is platform independent
- SOAP is language independent
- SOAP is based on XML
- SOAP is simple and extensible
- SOAP allows you to get around firewalls

25. What is WSDL?Nov-Dec 2017

The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

26. Draw SOAP message structure



27. Define MIME

MIME, an acronym for **Multipurpose Internet Mail Extensions**, specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. MIME messages can contain text, images, audio, video, or other application-specific data.

28. List down the key lengths supported by PGP (NOV/DEC 2014)

The "length" is a formal characterization of one of the mathematical values that constitute the *key pair.* Thus, the public and the private key don't have independent lengths per se; the private/public key pair has a length, which, by extension, is also said to be the length of the public key *and* of the private key.

The length is not the actual bit length of the encoding of either the public or private key, although there are correlations

29. What are the groups of HTTP header? (May 2015)

- Accept
- HTTP_User-Agent
- Content-Language
- Content-Length
- Content-Type
- Date
- Expires:
- Host
- Location
- Retry-After

30 . Define URL (May 2016)

A URL (**Uniform Resource Locator**), as the name suggests, provides a way to locate a resource on the web, the hypertext system that operates over the internet. The URL contains the name of the protocol to be used to access the resource and a resource name. The first part of a URL identifies what protocol to use. The second part identifies the IP address or domain name where the resource is located.

31. Mention the different levels in domain name space (May 2016)

- Top Level Domains
- Second Level Domails
- Third Level Domails

32. Mention the types of HTTP messages

- HTTP request message
- HTTP response message

33.State the usage of conditional get in HTTP (Apr/May 2017)

A conditional GET is an HTTP GET request that may return an HTTP 304 response (instead of HTTP 200). An HTTP 304 response indicates that the resource has not been modified since the previous GET, and so the resource is not returned to the client in such a response.

34. Present the information contained in a DNS resource record? (Apr/May 2017)

A resource record is a name-to-value binding, a 5-tuple that contains the following fields:

- **Domain name**: the domain to which this record applies.

- **Class**: set to IN for internet information. For other information other codes may be specified.
- **Type**: tells what kind of record it is.
- **Time to live**: Upper Limit on the time to reach the destination
- **Value**: can be an IP address, a string or a number depending on the record type.

35. Write the use of HTTP (Apr-May 2017)

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

36. Name four factors needed for a secure network?

Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender’s identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent.

Non-Reputation: The receiver must able to prove that a received message came from a specific sender

37. Define SSH?

Secure Shell is used to provide a remote login, and used to remotely execute commands and transfer files and also provide strong client/server authentication / message integrity.

38. What is TELNET PROTOCOL?

A TELNET connection is a Transmission Control Protocol (TCP) connection used to transmit data with interspersed TELNET control information.

The TELNET Protocol is built upon three main ideas: first, the concept of a "Network Virtual Terminal"; second, the principle of negotiated options; and third, a symmetric view of terminals and processes.

39. What is PGP?

Pretty Good Privacy. A program using public key encryption popularly used with email
A high security RSA public-key encryption application for MS-DOS, Unix, VAX/VMS, and other computers. It was written by Philip R. Zimmermann of Phil's Pretty Good(tm) Software and later augmented by a cast of thousands, especially including Hal Finney, Branko Lankester, and Peter Gutmann.

40. What is SSH?

(**S**ecure **Sh**ell) A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs. Also serving as a secure client/server connection for applications such as database access and e-mail SSH supports a variety of authentication methods.

41.What are the applications of TELNET?

TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. TELNET general purpose client server application program.
Using the Telnet protocol user on a local host can remote-login and execute commands on another distant host **(Time sharing environment, Network virtual terminal)**

42. Define WWW

World Wide Web: The Web today is a repository of information in which the documents, called ***web pages,*** are distributed all over the world and related documents are linked together

The purpose of the Web has gone beyond the simple retrieving of linked documents.

The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called *sites.* Each site holds one or more web pages.

PART-B

1. Explain WWW in detail (World Wide Web)

The idea of the Web was first proposed by Tim Berners-Lee in 1989 at *CERN.* The Web today is a repository of information in which the documents, called ***web pages,*** are distributed all over the world and related documents are linked together. The popularity and growth of the Web can be related to two terms in the above statement: *distributed* and *linked*

Distribution allows the growth of the Web. Each web server in the world can add a new web page to the repository and announce it to all Internet users without overloading a few servers. Linking allows one web page to refer to another web page stored in another server somewhere else in the world. The linking of web pages was achieved using a concept called ***hypertext***

Architecture

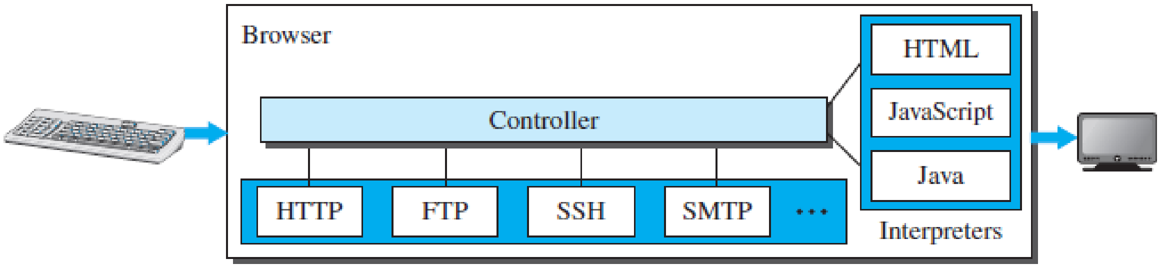
The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called ***sites***.

Each site holds one or more web pages. Each web page, however, can contain some links to other web pages in the same or other sites. In other words, a web page can be simple or composite. A simple web page has no links to other web pages; a composite web page has one or more links to other web pages. Each web page is a file with a name and address.

Web Client (Browser)

A variety of vendors offer commercial **browsers** that interpret and display a web page, and all of them use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocols, and interpreters.

Figure 26.2 *Browser*



The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described later, such as HTTP or

FTP. The interpreter can be HTML, Java, or JavaScript, depending on the type of document. Some commercial browsers include Internet Explorer, Netscape Navigator, and Firefox

Web Server

The web page is stored at the server. Each time a request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than a disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time. Some popular web servers include Apache and Microsoft Internet Information Server

Uniform Resource Locator (URL)

A web page, as a file, needs to have a unique identifier to distinguish it from other web pages. To define a web page, we need three identifiers: *host*, *port*, and *path*. However, before defining the web page, we need to tell the browser what client server application we want to use, which is called the *protocol*. This means we need four identifiers to define the web page. The first is the type of vehicle to be used to fetch the web page; the last three make up the combination that defines the destination object (web page).

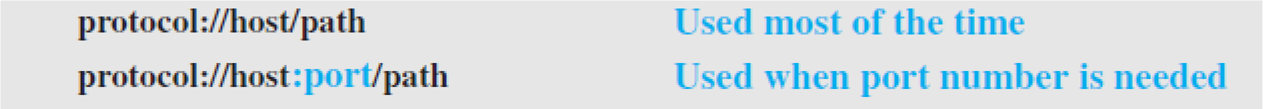
❑ ***Protocol.*** The first identifier is the abbreviation for the client-server program that we need in order to access the web page. Although most of the time the protocol is HTTP (HyperText Transfer Protocol), we can also use other protocols such as FTP (File Transfer Protocol).

❑ ***Host.*** The host identifier can be the IP address of the server or the unique name given to the server. IP addresses can be defined in dotted decimal notation, (such as 64.23.56.17); the name is normally the domain name that uniquely defines the host, such as *forouzan.com*

❑ ***Port.*** The port, a 16-bit integer, is normally predefined for the client-server application. For example, if the HTTP protocol is used for accessing the web page, the well-known port number is 80. However, if a different port is used, the number can be explicitly given.

❑ ***Path.*** The path identifies the location and the name of the file in the underlying operating system. The format of this identifier normally depends on the operating system. In UNIX, a path is a set of directory names followed by the file name, all separated by a slash. For example, */top/next/last/myfile* is a path that uniquely defines a file named *myfile,* stored in the directory *last*, which itself is part of the directory *next*, which itself is under the directory *top*.

To combine these four pieces together, the **uniform resource locator (URL)** has been designed; it uses three different separators between the four pieces as shown below:



protocol://host/path	Used most of the time
protocol://host:port/path	Used when port number is needed

Web Documents

The documents in the WWW can be grouped into three broad categories: static, dynamic, and active.

Static Documents

Static documents are fixed-content documents that are created and stored in a server. The client can get a copy of the document only. Languages used: HTML, XML, XSL, XHTML

Dynamic Documents

A **dynamic document** is created by a web server whenever a browser requests the document. When a request arrives, the web server runs an application program or a script that creates the dynamic document. The server returns the result of the program or script as a response to the browser that requested the document. Languages used: JSP, ASP

\

Active Documents

For many applications, we need a program or a script to be run at the client site. These are called ***active documents.*** Use java applets

2. Explain working of E-mail, describe how SMTP is used E-mail application in detail? (Apr/may 2011& 2010, Nov/Dec 2013) (Nov 2015)

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication.

- The model that works best for email is the Client-Server model.
- Clients carry out user interactions with the email server.
- Forms in which clients appear:
  - Application based - these are installed onto user's machines and include Microsoft Outlook and the freely available Outlook Express and Eudora.
  - Web based - these appear in a web browser's window and include Hotmail, Yahoo and Outlook web client.
- Basic functions include: (Services)
  - Ability to create new emails.
  - Display and store received emails.
  - Hold address lists of contacts, a calendar, journal and other extra functions that help organize the user's working day.
  - The client is also configured with the account information and names or IP addresses of the email servers with which it will be communicating.
- An email server is typically a combination of processes running on a server with a large storage capacity it includes a list of users and rules, and the capability to receive, send and store emails and attachments.
- Should process emails for months as sending, receiving and maintenance tasks are carried out at scheduled times. The client only has to connect to the email server when it sends and checks/receives new email.
- Sometimes it may be permanently connected to the server to allow access to shared address books or calendar information – this is typical of a LAN-based email server.
- Most email servers conduct email services by running two separate processes on the same machine.

- One process is the POP3 (Post Office protocol 3) server, which holds emails in a queue and delivers emails to the client when they are requested.
- The other is the SMTP (simple mail transfer protocol) server that receives outgoing emails from clients and sends and receives email from other SMTP servers.
- These two processes are linked by an internal mail delivery mechanism that moves mail between the POP3 and SMTP servers.
- When the client calls the email server to send or check for mail it connects to the server on certain TCP/IP ports:
  - SMTP on port 25
  - POP3 on port 110.

MAIL PROTOCOLS

- **SMTP** - Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol.
- **POP3** - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.
- **IMAP4** - Internet Mail Access Protocol version 4 is the replacement for POP3.
- **MIME** - Multipurpose Internet Mail Extension is the protocol that defines the way files are attached to SMTP messages.

3.Explain the salient features of the SMTP protocol (Email protocols) (12)(MAY/JUNE 2009) SMTP protocol (May 2015& 2016, Apr/May 2017)

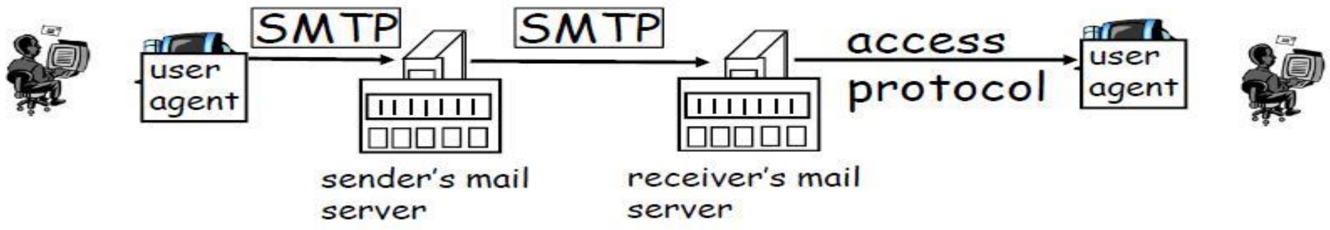
- Simple Mail Transfer Protocol (SMTP) is used to send mail across the internet. This protocol transfers electronic mail (e-mail) from the mail server of a source to the mail servers of destinations.
- The mail is enclosed in what is called an **envelope.** The envelope contains the TO and FROM fields and these are followed by the mail. The mail consists of two parts namely the Header and the Data. The Header has the TO and FROM fields.
- In SMTP data portion can contain only printable ASCII characters. The old method of sending a binary file was to send it in uuencoded form but there was no way to distinguish between the many types of binary files possible eg. .tar, .gz , .dvi etc.

There are four types of programs used in the process of sending and receiving mail. They are:

- **MUA** - Mail users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA.

- **MTA** - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine.

- **LDA** - Local delivery agent on the receiving machine receives the mail from its MTA.
- **Mail notifier** - This program notifies the recipient that they have mail.



Example

1) Ali uses UA to compose message and send it “to” ahmed@ksu.edu.sa

2) Ali’s UA sends the message to his mail server; message placed in message queue

3) Client side of SMTP opens TCP connection with Ahmed’s mail server

4) SMTP client sends Ali’s message over the TCP connection

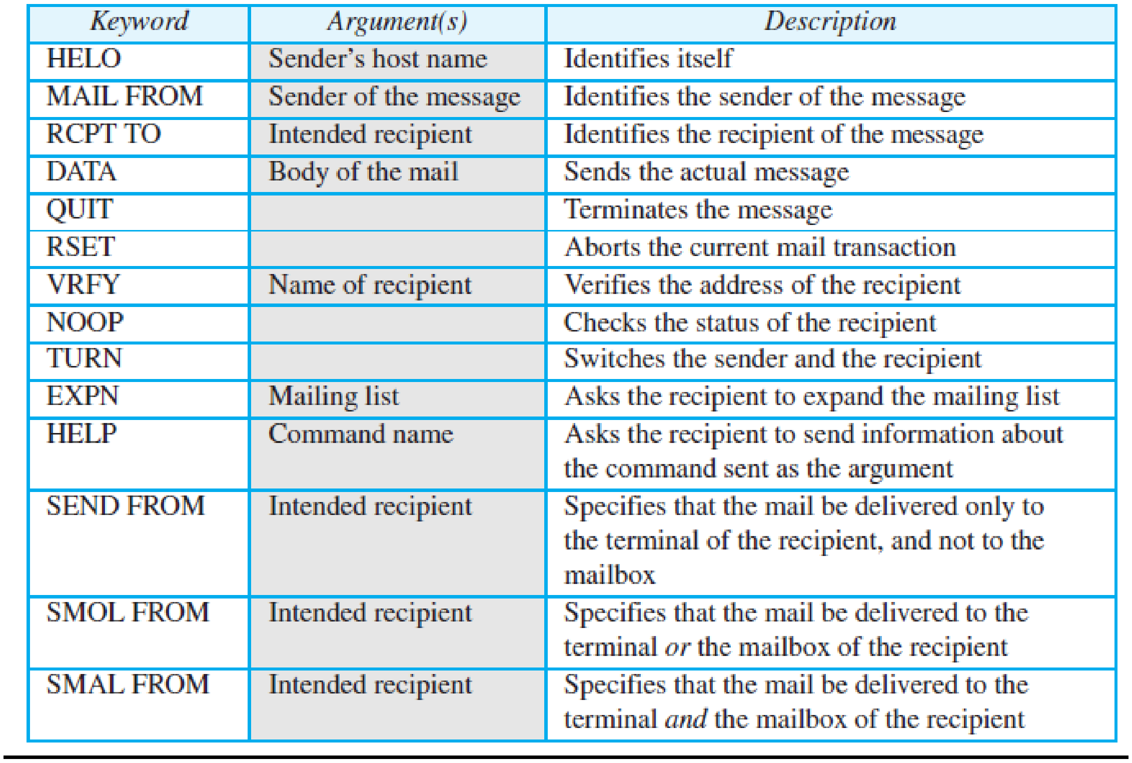
5) Ahmed’s mail server receives and places the message in Ahmed’s mailbox

6) Ahmed invokes his user agent to read message

SMTP Commands & Responses

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server. The command is from an MTA client to an MTA server; the response is from an MTA server to the MTA client. Each command or reply is terminated by a two character (carriage return and line feed) end-of-line token.
It consists of a keyword followed by zero or more arguments. SMTP defines 14 commands

Table 26.6 *SMTP commands*

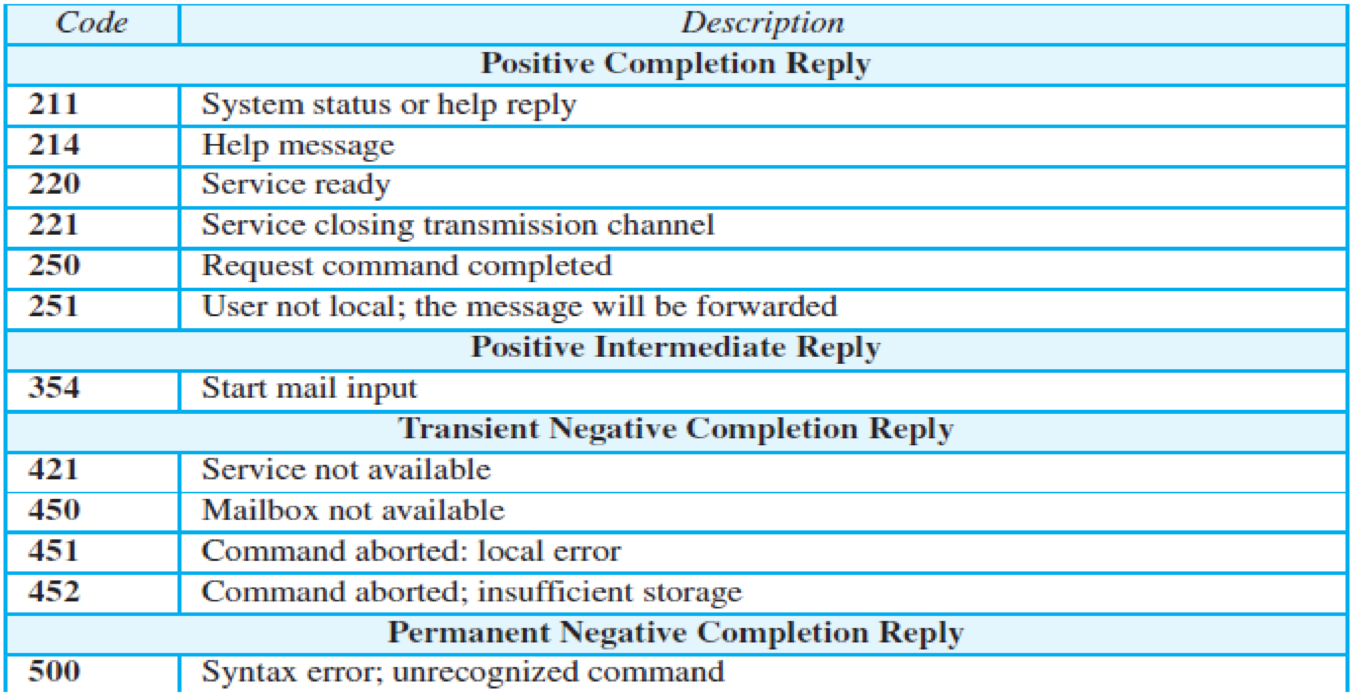


Keyword	*Argument(s)*	*Description*
HELO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies the sender of the message
RCPT TO	Intended recipient	Identifies the recipient of the message
DATA	Body of the mail	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the status of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list
HELP	Command name	Asks the recipient to send information about the command sent as the argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and not to the mailbox
SMOL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *or* the mailbox of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *and* the mailbox of the recipient

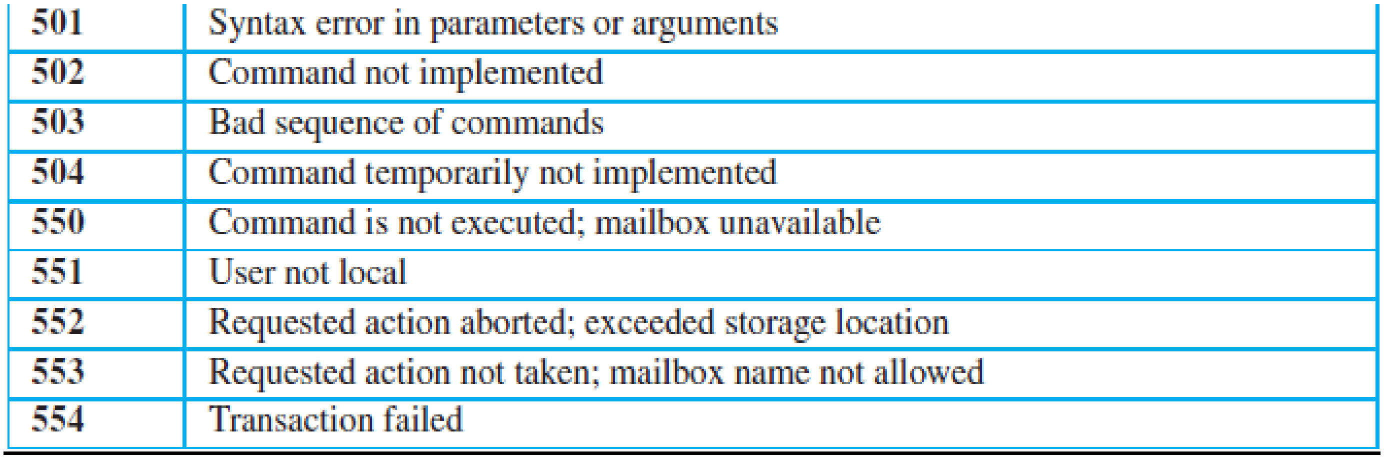
Responses

Responses are sent from the server to the client. A response is a three digit code that may be followed by additional textual information.

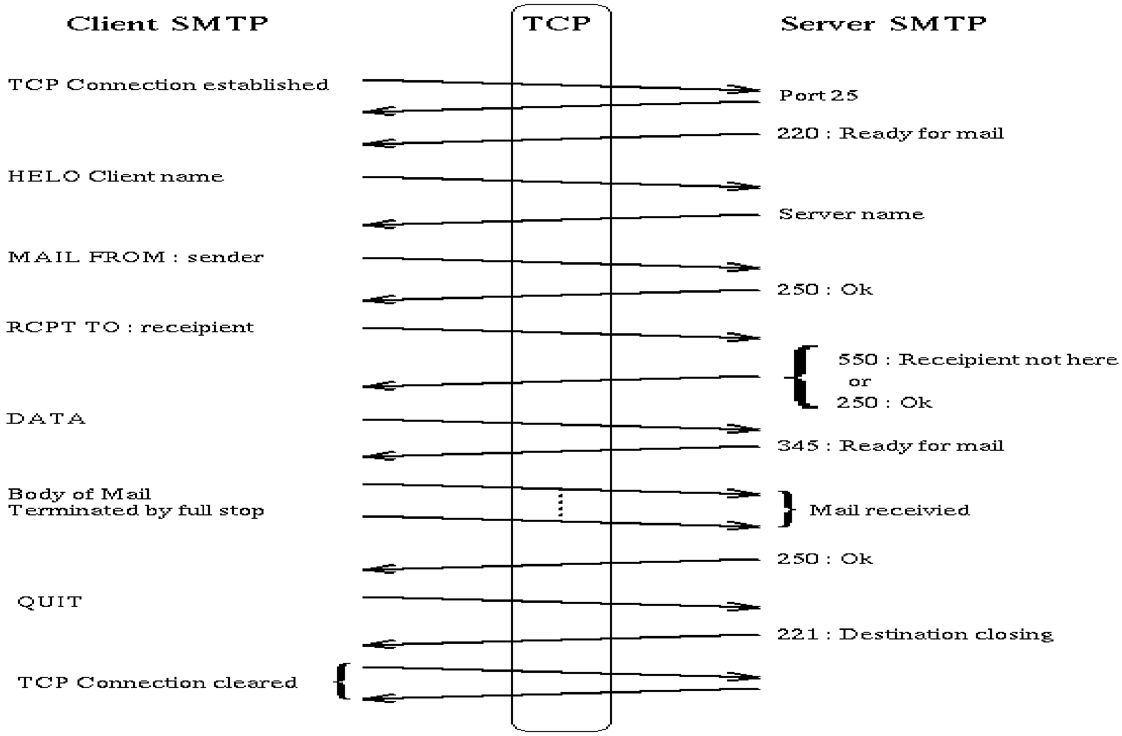
Table 26.7 *Responses*



Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage
	Permanent Negative Completion Reply
500	Syntax error; unrecognized command



501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed



<u>Mail Transfer Phases</u>

Connection Establishment
Message Transfer
Connection Termination

<u>PROBLEMS WITH SMTP</u>

1. There is no convenient way to send nonprintable characters
2. There is no way to know if one has received mail or not or has read it or not.
3. Someone else can send a mail on my behalf.

4.Explain in detail about MIME: Multipurpose Internet Mail Extensions.

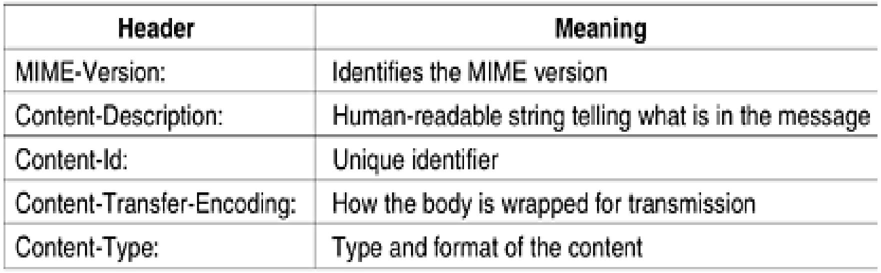
MIME, an acronym for Multipurpose Internet Mail Extensions, specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. MIME messages can contain text, images, audio, video, or other application-specific data. Specifically, MIME allows mail messages to contain:

- Multiple objects in a single message.
- Text having unlimited line length or overall length.
- Character sets other than ASCII, allowing non-English language messages.
- Multi-font messages.
- Binary or application specific files.
- Images, Audio, Video and multi-media messages.

A secure version of MIME, S/MIME (Secure/Multipurpose Internet Mail Extensions), is defined to support encryption of email messages. Based on the MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin and privacy and data security.

MIME standard converts (encodes) non-text files into text that is normally unreadable and then, at the other end, reconverts (decodes) the files to their originalform.

MIME defines five new message headers



Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

MIME-Version: *Any message not containing a MIME-Version: header is assumed to be an English plaintext message and is processed as such.*

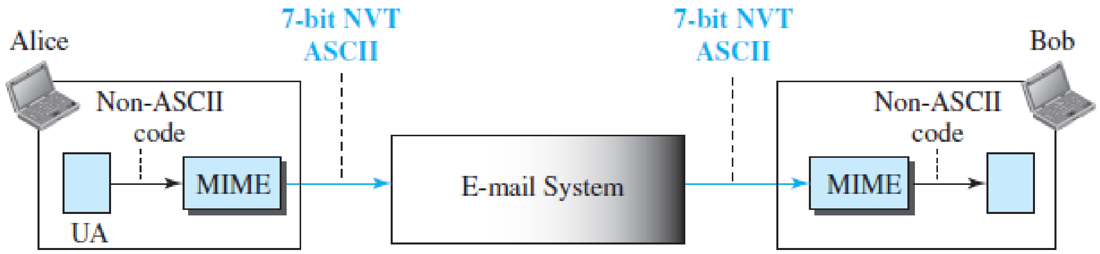
The Content-Description: header is an ASCII string telling what is in the message. This header is needed so the recipient will know whether it is worth decoding and reading the message.

The Content-Id: header identifies the content.

The Content-Transfer-Encoding: tells how the body is wrapped for transmission through a network that may object to most characters other than letters, numbers, and punctuation marks.

Content-Type: It specifies the nature of the message body. Seven types are defined in RFC 2045, each of which has one or more subtypes. The type and subtype are separated by a slash, as in Content-Type: video/mpeg

Figure 26.18 *MIME*



5.Write notes on IMAP, POP3 (8)Nov/Dec 2013 (May 2015,Apr/May 2017)

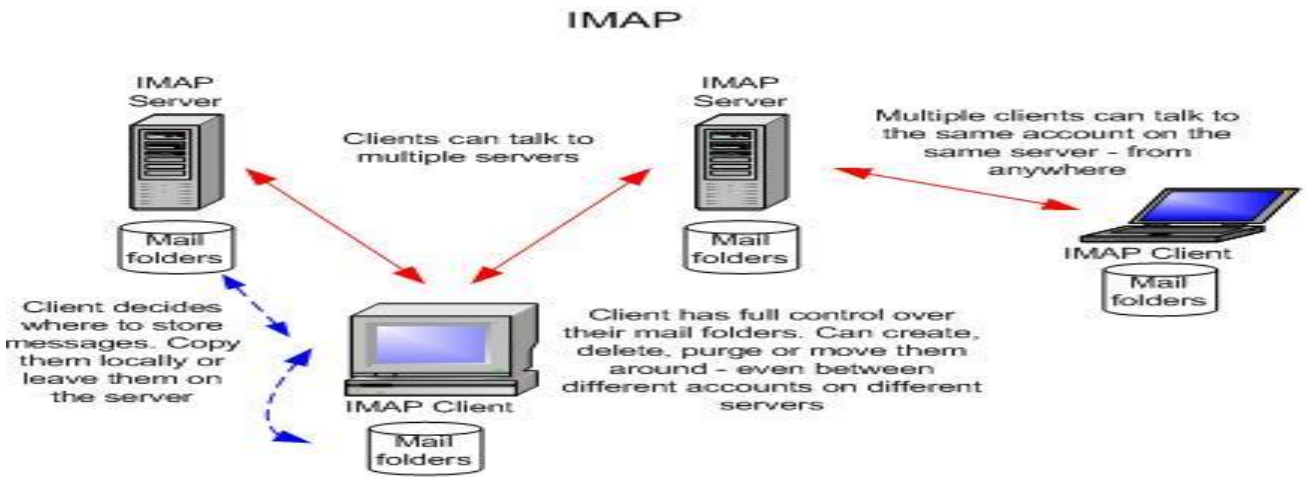
Internet Message Access Protocol (IMAP) is a method of accessing electronic mail that is kept on a mail server. IMAP permits a "client" email program to access remote message stores as if they were local. Clients may store local copies of the messages, but these are considered to be a temporary cache. Email stored on an IMAP server can be manipulated from a desktop computer remotely, without the need to transfer messages or files back and forth between these computers.

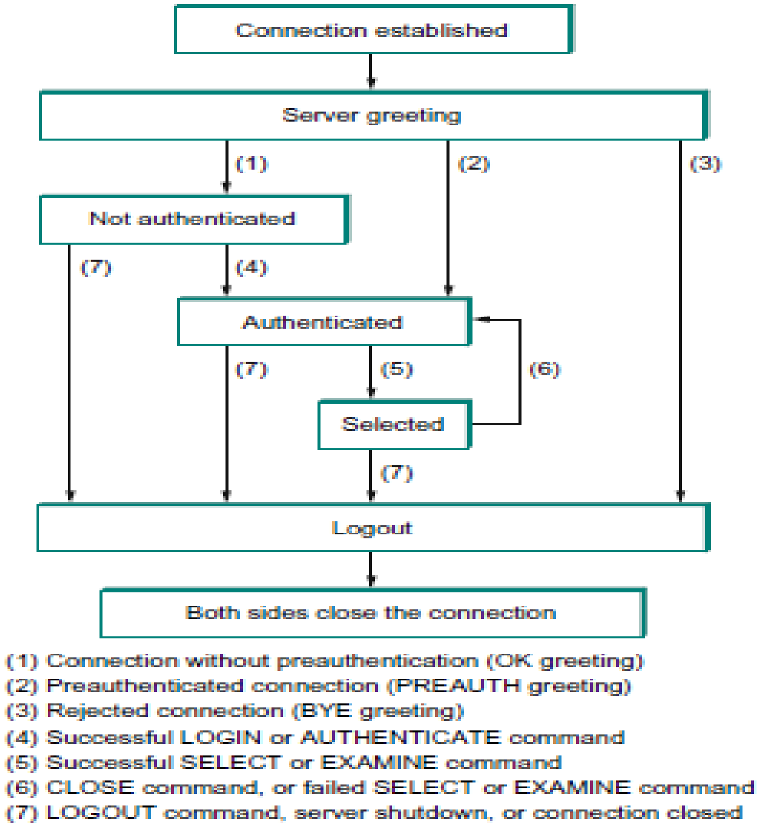
- IMAP can do all three modes: offline, online processing and disconnected operations. In the online mode, the mail client does not copy mails in a shared server all at once and then delete them. It is an interactive client-server model, where the client can ask the server for headers, or the bodies of specified messages, or to search for messages meeting certain criteria.

- IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; server-based and MIME parsing, and searching; and selective fetching of message attributes, texts, and portions thereof for efficiency. IMAP allows clients to access messages (both new and saved) from more than one computer, that feature has become extremely important as reliance on electronic messaging and use of multiple computers increase.

The current version of IMAP is version 4 revision 1(IMAP4 rev1). Key features for IMAP4 include:

- Fully compatible with Internet messaging standards, e.g. MIME.
- Allow message access and management from more than one computer.
- Provide support for "online", "offline", and "disconnected" access modes
- Support for concurrent access to shared mailboxes
- Client software needs no knowledge about the server's file store format


IMAP
IMAP Server
Mail folders
Clients can talk to multiple servers
IMAP Server
Mail folders
Multiple clients can talk to the same account on the same server - from anywhere
IMAP Client
Mail folders
Client decides where to store messages. Copy them locally or leave them on the server
IMAP Client
Mail folders
Client has full control over their mail folders. Can create, delete, purge or move them around - even between different accounts on different servers



(1) Connection without preauthentication (OK greeting)
(2) Preauthenticated connection (PREAUTH greeting)
(3) Rejected connection (BYE greeting)
(4) Successful LOGIN or AUTHENTICATE command
(5) Successful SELECT or EXAMINE command
(6) CLOSE command, or failed SELECT or EXAMINE command
(7) LOGOUT command, server shutdown, or connection closed

FIGURE 9.2 IMAP state transition diagram.

POP3 Protocol (8.M) (Nov 2016)

- The **POP (Post Office Protocol 3)** protocol provides a simple, standardized way for users to access mailboxes and download messages to their computers.
- There are two main versions of this protocol, POP2 and POP3, to which ports 109 and 110 are allocated respectively and which operate using radically different text commands.
- When using the POP protocol all your eMail messages will be downloaded from the mail server to your local computer.
- POP was designed to support "offline" mail processing, in which, mail is delivered to a server, and a personal computer user periodically invokes a mail "client" program that connects to the server and downloads all of the pending mail to the user's own machine. The offline access mode is a kind of

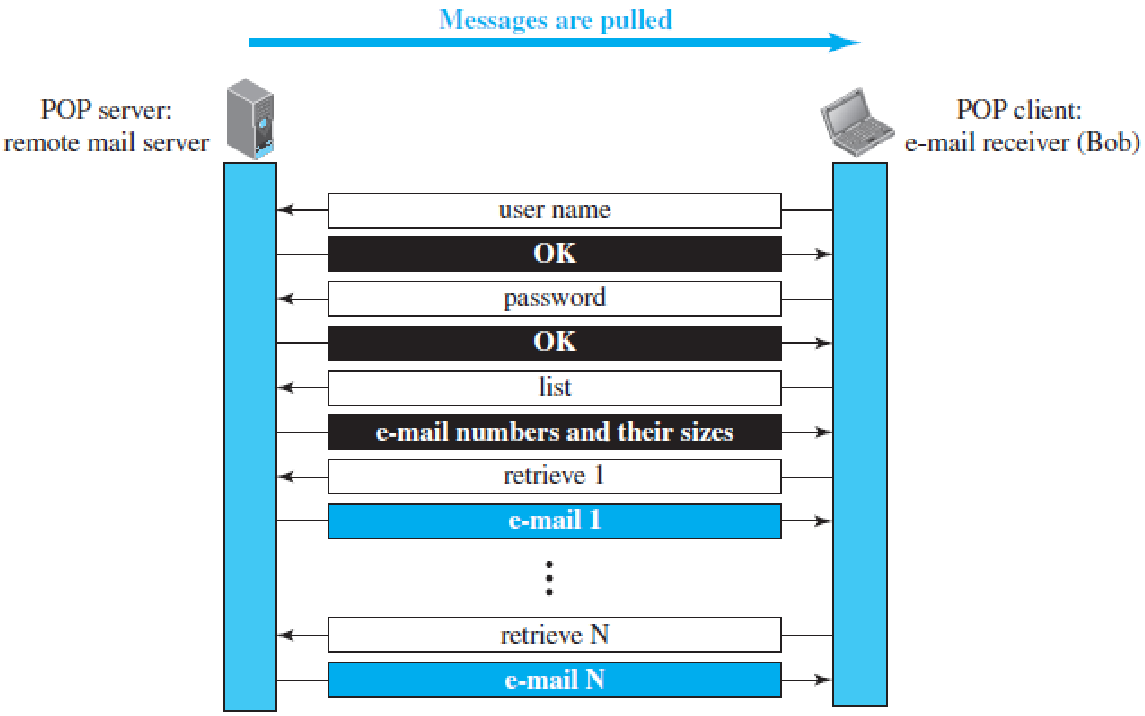
store-and-forward service, intended to move mail (on demand) from the mail server (drop point) to a single destination machine, usually a PC or Mac. Once delivered to the PC or Mac, the messages are then deleted from the mail server.

Once the connection is established, the POP3 protocol goes through three states in sequence:

- Authorization - The authorization state deals with having the user log in.
- Transactions - The transaction state deals with the user collecting the e-mails and marking them for deletion from the mailbox.
- Update – The update state actually causes the e-mails to be deleted

Command	**Description**
USER identification	This command makes it possible to be authenticated. It must be followed by the user name, i.e. a character string identifying the user on the server. The USER command must precede the *PASS* command.
PASS password	The *PASS* command makes it possible to specify the user's password where the name has been specified by a prior *USER* command.
STAT	Information on the messages contained on the server
RETR	Number of the message to be picked up
DELE	Number of the message to be deleted
LIST [msg]	Number of the message to be displayed
NOOP	Allows the connection to be kept open in the event of inactivity
TOP <messageID><n>	Command displaying *n* lines of the message, where the number is given in the argument. In the event of a positive response from the server, it will send back the message headers, then a blank line and finally the first *n* lines of the message.
UIDL [msg]	Request to the server to send back a line containing information about the message possibly given in the argument. This line contains a character string called a *unique identifier listing*, making it possible to uniquely identify the message on the server, independently of the session. The optional argument is a number relating to a message existing on the POP server, i.e. an undeleted message).
QUIT	The *QUIT* command requests exit from the POP3 server. It leads to the deletion of all messages marked as deleted and sends back the status of this action.

Figure 26.17 *POP3*



6. i) What is HTTP protocol used for? (OR) Write notes on URLS(NOV/DEC 2014) (Nov 2015) (May 2016)

ii) What is the default port number of HTTP protocol?

iii) Discuss the features of HTTP and also discuss how HTTP works.

<u>HTTP PROTOCOL</u>

The **HyperText Transfer Protocol (HTTP)** is used to define how the client-server programs can be written to retrieve web pages from the Web. An HTTP client sends a request; an HTTP server returns a response. The server uses the port number 80; the client uses a temporary port number.

- <u>Protocol for transfer of data between Web servers and Web clients (browsers).</u>
- "The Hypertext Transfer Protocol (HTTP) is an **application-level protocol** for **distributed**, collaborative, hypermedia information systems.
- Popular Web servers:
  - Apache HTTPD, JBoss and Tomcat
- Popular Web clients:
  - Firefox and Opera

<u>HTTP Properties</u>

1) A comprehensive addressing scheme

The HTTP protocol uses the concept of reference provided by the Universal Resource Identifier (URI) as a location (URL) or name (URN), for indicating the resource on which a method is to be applied.

- Every resource accessible through HTTP is identified by a Uniform Resource Location (URL), which is a location-specific identifier.
  - For example,
    - http://www.cs.uct.ac.za:80/
    - ftp://ftp.cs.uct.ac.za/
- A Uniform Resource Identifier (URI) is a standard format (<scheme>:<identifier>) generic identifier.
  - For example,
    - mailto:hussein@cs.uct.ac.za
- A Uniform Resource Name (URN) is one example of a location-independent URI.
  - For example urn:isbn:123-456-789

2) Client-Server architecture

The HTTP protocol is based on a request/response paradigm. The communication generally takes place over a TCP/IP connection on the Internet. The default port is 80, but other ports can be used. A requesting program (a client) establishes a connection with a receiving program (a server) and sends a request to the server in the form of a request method, URI, and protocol version, followed by a message containing request modifiers, client information, and possible body content. The server responds with a status line, including its protocol version and a success or error code, followed by a message containing server information, entity meta_information, and possible body content.

3) HTTP protocol is connectionless

This HTTP protocol is called connectionless because once the single request has been satisfied, the connection is dropped.

4) HTTP protocol is stateless

After the server has responded to the client's request, the connection between client and server is dropped and forgotten. There is no "memory" between client connections. The pure HTTP server implementation treats every request as if it was brand-new (without context), i.e. not maintaining any connection information between transactions.

Other HTTP Features

- Persistent connections
- Cache control

Persistent Connections

Persistent connections provide a mechanism by which a client and a server can signal the close of a TCP connection. With them, it is possible to establish a TCP connection, send a request and get a response, and then send additional requests and get additional responses. By amortizing the TCP setup and release over multiple requests, the relative overhead due to TCP is much less per request. It is also possible to pipeline requests, that is, send request 2 before the response to request 1 has arrived.

Persistent HTTP connections have a number of advantages:

- By opening and closing fewer TCP connections, CPU time is saved in routers and hosts (clients, servers, proxies, gateways, tunnels, or caches), and memory used for TCP protocol control blocks can be saved in hosts.
- HTTP requests and responses can be pipelined in a connection. Pipelining allows a client to make multiple requests without waiting for each response, allowing a single TCP connection to be used much more efficiently, with much lower elapsed time.

Caching

The goal of caching in HTTP is to eliminate the need to send requests in many cases, and to eliminate the need to send full responses in many other cases. That is, there are two main reasons that web caching is used:

- To reduce latency because the request is satisfied from the cache (which is closer to the client) instead of the origin server, it takes less time for the client to get the object and display it. This makes Web sites seem more responsive.
- To reduce traffic because each object is only gotten from the server once, it reduces the amount of bandwidth used by a client. This saves money if the client is paying by traffic, and keeps their bandwidth requirements lower and more manageable.

Nonpersistent versus Persistent Connections

- ***Nonpersistent Connections***

In a **nonpersistent connection**, one TCP connection is made for each request/response.
The following lists the steps in this strategy:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.

- ***Persistent Connections***

HTTP version 1.1 specifies a **persistent connection** by default. In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached. The sender usually sends the length of the data with each response.

Message Formats

The HTTP protocol defines the format of the request and response messages

Request Message

HTTP Methods

HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. The three most often used methods are **GET, HEAD**, and **POST**.

Method	Description
OPTIONS	capabilities of resource/server
GET	retrieve resource
HEAD	retrieve headers for resource
POST	submit data to server
PUT	replace/insert resource on server
DELETE	remove resource from server
TRACE	trace request route through Web

The GET method

The GET method requests the server to send the page. The page is suitably encoded in MIME. The vast majority of requests to Web servers are GETs. The usual form of GET is GET filename HTTP/1.1 Where filename names the resource (file) to be fetched and 1.1 is the protocol version being used.

The Head Method

The HEAD method is used to ask only for information about a document, not for the document itself. HEAD is much faster than GET, as a much smaller amount of data is transferred. It's often used by clients who use caching, to see if the document has changed since it was last accessed. If it was not, then the local copy can be reused, otherwise the updated version must be retrieved with a GET.

The PUT method

The PUT method is the reverse of GET: instead of reading the page, it writes the page. This method makes it possible to build a collection of Web pages on a remote server.

The POST method

The POST method is used to transfer data from the client to the server.

DELETE

DELETE does what you might expect: it removes the page. There is no guarantee that DELETE succeeds, since even if the remote HTTP server is willing to delete the page

TRACE

The TRACE method is for debugging. It instructs the server to send back the request. This method is useful when requests are not being processed correctly and the client wants to know what request the server actually got.

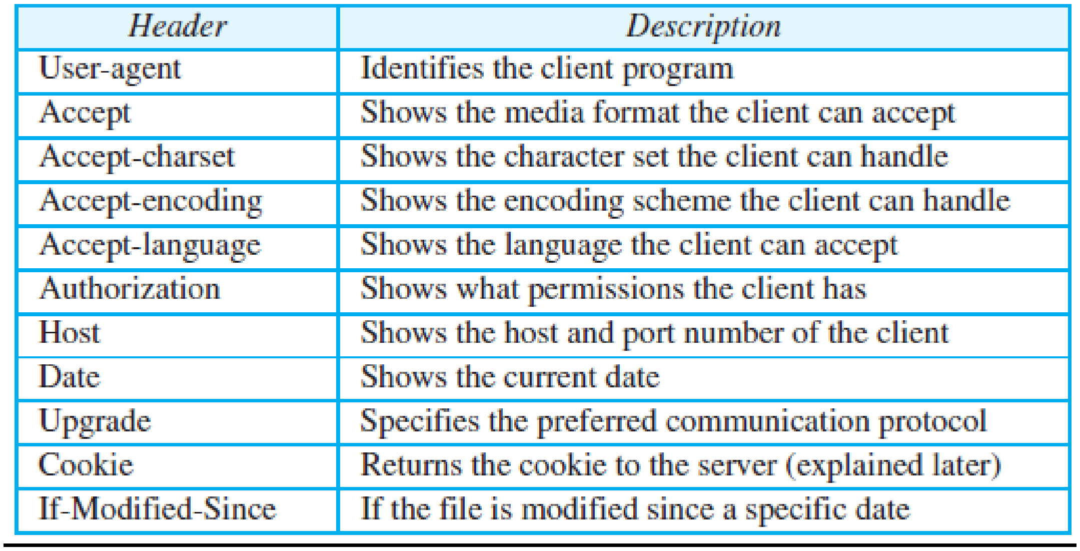
OPTION The OPTIONS method provides a way for the client to query the server about its properties or those of a specific file. Telling whether the request was satisfied, and if not, why not.

Status	Reason	Description
200	OK	Successful request
206	Partial Content	Successful request for partial content
301	Moved Permanently	Resource has been relocated
304	Not Modified	Conditional GET but resource has not changed
400	Bad Request	Request not understood

403	Forbidden	Access to resource not allowed
404	Not Found	URI/resource not found on server
500	Internal Server Error	Unexpected error

HTTP Header Fields(Nov/Dec 2007)

Table 26.2 *Request header names*

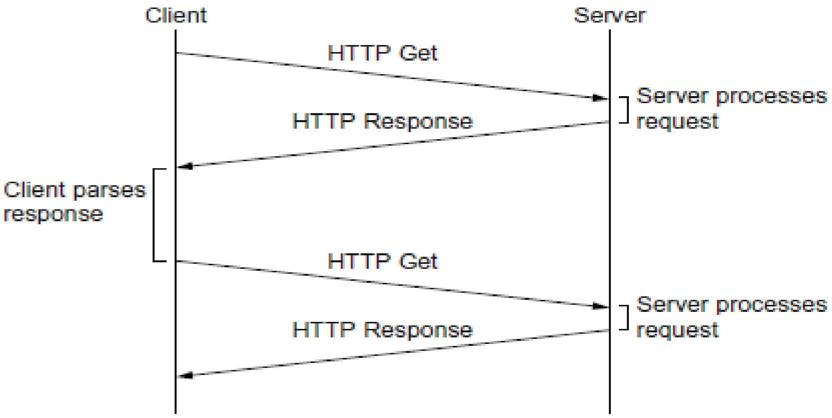


Header	*Description*
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server (explained later)
If-Modified-Since	If the file is modified since a specific date

An HTTP transaction consists of a header followed optionally by an empty line and some data. The header will specify such things as the action required of the server, or the type of data being returned, or a status code. The use of header fields sent in HTTP transactions gives the protocol great flexibility. These fields allow descriptive information to be sent in the transaction, enabling authentication, encryption, and/or user identification. The header is a block of data preceding the actual data, and is often referred to as meta information, because it is information about information.

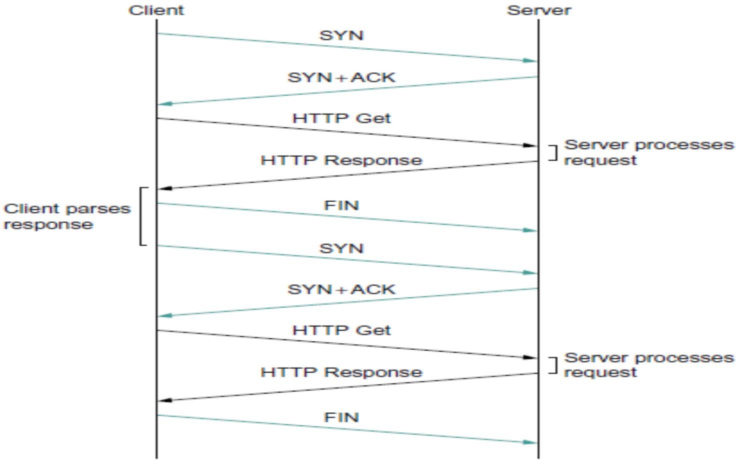
- ***Accept***: Indicates which data formats are acceptable.
  - Accept: text/html, text/plain
- ***HTTP_User-Agent***.

  The browser the client is using to send the request.
  General format: software/version library/version.
- ***Content-Language***: Language of the content
  - Content-Language: english
- ***Content-Length***: Size of message body
  - Content-Length: 1234
- ***Content-Type***: MIME type of content body
  - Content-Type: text/html



■ **FIGURE 9.5** HTTP 1.1 behavior with persistent connections.

- ➢ ***Date***: The Date header represents the date and time at which the message was originated
  - – Date: Tue, 15 Nov 1994 08:12:31 GMT
- ➢ ***Expires***: When content is no longer valid
  - – Expires: Tue, 15 Nov 1994 08:12:31 GMT
- ➢ ***Host***: Machine that request is directed to
  - – Host: www.cs.uct.ac.za



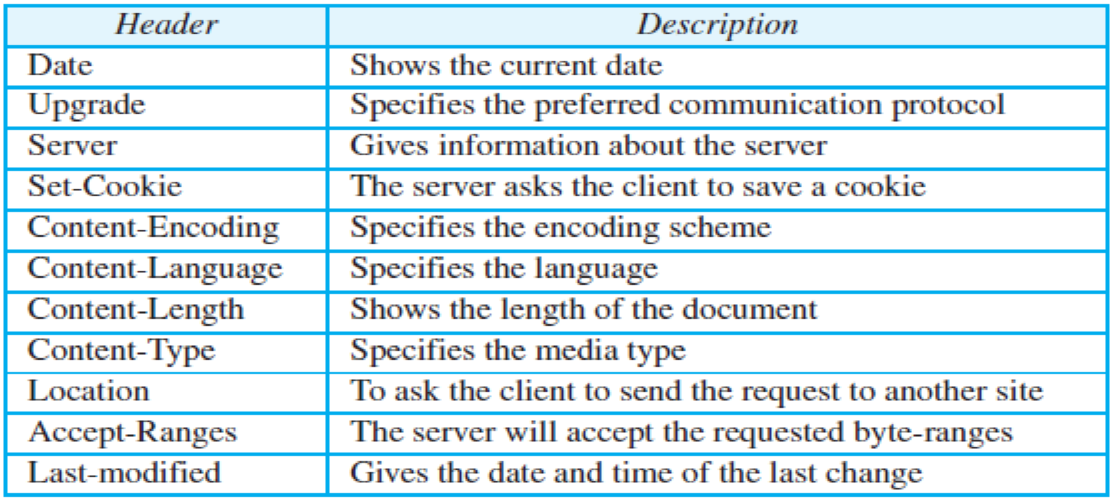
■ **FIGURE 9.4** HTTP 1.0 behavior.

- ➢ ***Location***:
  The Location response header field defines the exact location of the resource that was identified by the request URI. If the value is a full URL, the server returns a "redirect" to the client to retrieve the specified object directly.
  - – Location: http://myserver.org/
- ➢ ***Retry-After***: Indicates that client must try again in future
  - – Retry-After: 120

Response Message

A response message consists of a status line, header lines, a blank line, and sometimes a body. The first line in a response message is called the *status line*. There are three fields in this line separated by spaces and terminated by a carriage return and line feed

Table 26.3 *Response header names*

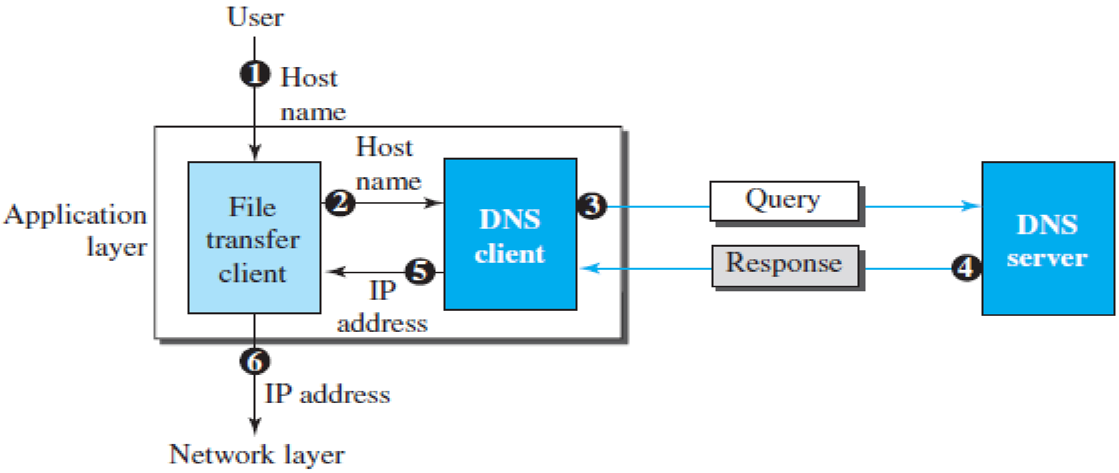


Header	*Description*
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change

7.Discuss briefly DNS (Domain Name System)& its advantages *(Apr /may2010) (Nov/Dec 2014)(Nov 2015 & 2016)(Apr/May 2017)*

The **DNS** translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

Figure 26.28 *Purpose of DNS*



The following six steps map the host name to an IP address:

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client.

3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client.
6. The file transfer client now uses the received IP address to access the file transfer server.

Namespace:

The names assigned to computers must be selected from a name space. The name must be unique because the addresses are unique. A namespace that maps each address to a unique name can organize in two ways.

1. Flat Namespace
2. Hierarchical Namespace

Flat Namespace A name is assigned to an address. A name in this space is a sequence of characters without structure. The main disadvantage of flat namespace is that, it cannot use in a large system such as the internet.

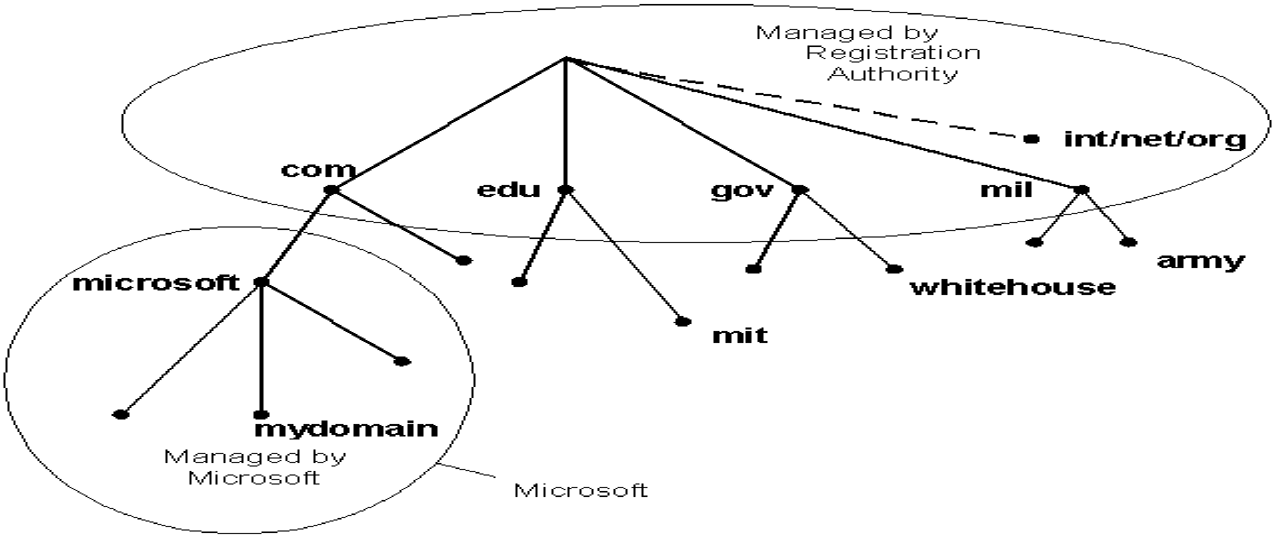
Hierarchical Namespace Each name is made of several parts. The first part can defined the nature of the organization, the second part can defined the name, and the third part can define department and so on. The authority to assign and control the namespaces can be decentralized.

Domain Hierarchy:

DNS is hierarchical in structure. A domain is a subtree of the domain name space. All the related information about a particular network (generally maintained by an organization, firm or university) should be available at one place. The organization should have complete control over what it includes in its network and how does it "organize" its network. Meanwhile, all this information should be available transparently to the outside world.

Conceptually, the internet is divide into several hundred top level domains where each domain covers many hosts. Each domain is partitioned in subdomains which may be further partitioned into subsubdomains and so on... So the domain space is partitioned in a tree like structure as shown below.

The internet uses a hierarchical tree structure of Domain Name Servers for IP address resolution of a host name.



The top level domains are either generic or names of countries. eg of generic top level domains are .edu .mil .gov .org .net .com .int etc. For countries we have one entry for each country as defined in ISO3166. eg. .in (India) .uk (United Kingdom).

The leaf nodes of this tree are target machines. Obviously we would have to ensure that the names in a row in a subdomain are unique. The max length of any name between two dots can be 63 characters. The absolute address should not be more than 255 characters. Domain names are case insensitive. Also in a name only letters, digits and hyphen are allowed. For eg. www.iitk.ac.in is a domain name corresponding to a machine named www under the sub domain iitk.ac.in.

Domain Name
A name that identifies one or more *IP addresses*. For example, the domain name *microsoft.com* represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL *http://www.pcwebopedia.com/index.html*, the domain name is *pcwebopedia.com.*

Types of Domain Name

1. Fully Qualified Domain Name (FQDN)
2. Partially Qualified Domain Name (PQDN)

    1. FQDN: A fully qualified domain name (FQDN) consists of the host name plus domain name. e.g. **computername.domain.com**
    2. PQDN: A partially Qualified Domain Name (PQDN) stats from a node, but it does not reach the root. E.g. **computername**

Three main components of DNS

1. Resolver
2. Name server
3. Database of Resource Records(RRs)

Resolver: A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver. The resolver accesses the closest DNS server with a mapping request. If the server has the information, its satisfies the resolver; after the resolver receives the mapping, it interprets the response to see if it’s a real resolution or an error, and finally delivers the result to the process that requested it.

i) Mapping names to address
The resolver gives a domain name to the server and ask for the corresponding address.

ii) Mapping address to names
A client can send an IP address to a server to be mapped to a domain name.

iii) Recursive resolution
The resolver can ask for a recursive answer from a name server. This means that the resolver expects the server to supply the final answer. If the server is the authority for the domain name, it checks its database

and response. When the query is finally resolved, the response travel back until it finally reaches the requesting client. This is called recursive resolution.

iv) Iterative resolution

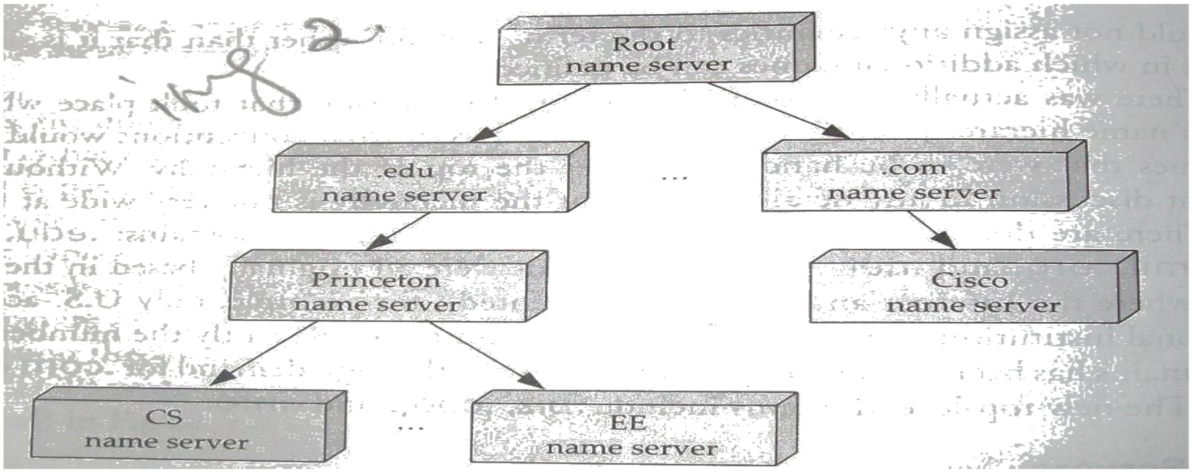
If the client doesn't ask for a recursive answer, the mapping can done iteratively. If the newly addressed the server can resolve the problem, it answers the query with the IP address. Otherwise it returns the IP address of a new server to a client. Now the client must repeat the query to the second server. This process is called iterative resolution because the client repeats the same query to multiple servers.

v) Caching

Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. Reduction of this time put increase efficiency. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client. If the same or another client asks for the same mapping, it can check its cache memory and solve the problem. This mechanism is called caching.

Name Servers

- The first step is to partition the hierarchy into sub trees called zones. Each zone can be thought of a corresponding to some administrative authority that is responsible for that portion of the hierarchy.
- DNS server is used to distribute the information among many computers. Specifically, the information contained in each zone is implemented in two or more name servers for the sake of redundancy, that is, the information is still available even if one name server fails. Each name server, in turn, is a program that can be accessed over the Internet.
- Client send queries to name servers, and name servers respond with the requested information. Sometimes the response contains the final answer that the client wants, and sometimes the response contains a pointer to another server that the client should query next.



Name Server Types

Name server types are:

1. **Root Server :**A root server is a server whose zone consist of the whole tree. A root server usually does not store any information about domains. But delegates it's authority to other servers, keeping references to those servers.
2. **Primary Server:** A Primary server is a server that stores a file about the zone for which it is an authority. It is responsible for creating, maintaining and updating the zone file. It stores the zone file on a local disk.
3. **Secondary Server:** A secondary server transfers the complete information about a zone from another server and stores the file on its local disk. The secondary server neither creates nor updates the zone files. If updating is required it must be done by the primary server, which sends the updated version to the secondary. When the secondary downloads information from the primary it is called zone transfer.

Types of Records

There are two types of records are used in DNS.

1. The question records
2. Resource Records

The question records: Is used by the client to get information from a server. This contains a domain name.
Resource Records: Each domain name is associated with a record called the resource record. The server database consists of resource records. The resource records are used in the answer, authoritative and additional information section of the response message.
Each name server implements the zone information as a collection of resource records. In essence, a resource record is a name-to-value binding, a 5-tuple that contains the following fields:

- **Domain name**: the domain to which this record applies.
- **Class**: set to IN for internet information. For other information other codes may be specified.
- **Type**: tells what kind of record it is.
- **Time to live**: Upper Limit on the time to reach the destination
- **Value**: can be an IP address, a string or a number depending on the record type.

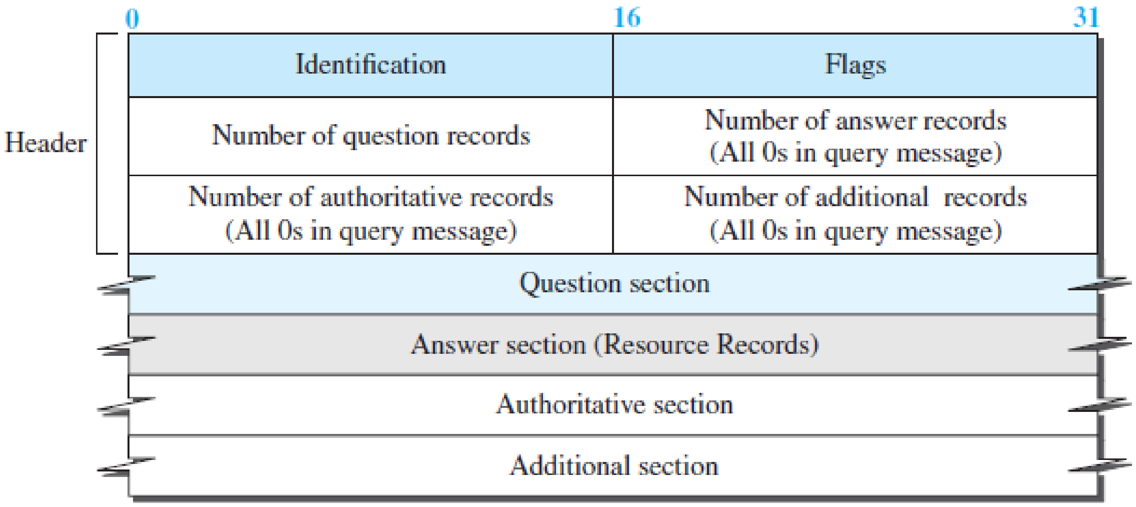
Resource Record Type	**Contents**	**Use**
A	Host Address	Used to hold a specific host's IP address.
CNAME	Canonical Name (alias)	Used to make an alias name for a host.
MX	Mail Exchanger	Provides message routing to a mail server, plus backup server(s) in case the target server isn't active.
NS	Name Server	Provides a list of authoritative servers for a domain or indicates authoritative DNS servers for any delegated sub-domains.
PTR	Pointer	Used for reverse lookup—resolving an IP address into a domain name using the IN-ADDR.ARPA domain.

SOA	Start of Authority	Used to determine the DNS server that's the primary server for a DNS zone and to store other zone property information.

DNS Messages

To retrieve information about hosts, DNS uses two types of messages: *query* and *response*. Both types have the same format

Figure 26.38 *DNS message*


0
16
31
Header
Identification
Flags
Number of question records
Number of answer records
(All 0s in query message)
Number of authoritative records
(All 0s in query message)
Number of additional records
(All 0s in query message)
Question section
Answer section (Resource Records)
Authoritative section
Additional section

Note:
The query message contains only the question section.
The response message includes the question section,
the answer section, and possibly two other sections.

DDNS

When the DNS was designed, no one predicted that there would be so many address changes. In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. These types of changes involve a lot of manual updating. The size of today's Internet does not allow for this kind of manual operation The DNS master file must be updated dynamically.

The **Dynamic Domain Name System (DDNS)** therefore was devised to respond to this need. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP to a primary DNS server To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

Advantages:

More Reliable: Delivers messages to the users with zero downtime.

Faster: DNS are connected well at intersections of internet. Anycast technology enables requests are answered to the next closest node in the case of maintenance or downtime.

Smarter: Automatic corrections of typos.

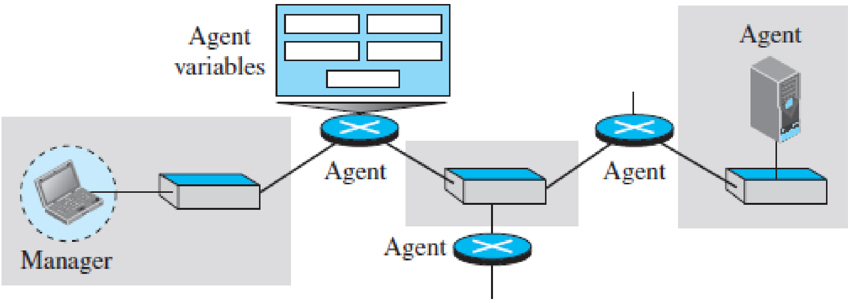
8.BrieflyExplain the concept of SNMP (Simple Network Management Protocol) (Apr /may2011) (May 2015) (Nov 2016)

SNMP is a frame work for managing devices in an internet using TCP/IP suite. It provides fundamental operations for monitoring and maintaining an internet.

Concept:

- SNMP uses the concept of manager and agent. Manager usually a host controls and monitors a set of agents, usually routers. A management station, called a manager, is a host that runs the SNMP client program. A managed station, called an agent, is a router or host that runs the SNMP server program.
- Management is achieved through simple interaction between a manager and an agent. The agent keeps performance information in a database. The manager has access to the values in the database.

Figure 27.2 *SNMP concept*



Managers and Agents

A management station, called a *manager*, is a host that runs the SNMP client program. A managed station, called an *agent*, is a router (or a host) that runs the SNMP server program. Management is achieved through simple interaction between a manager and an agent. The agent keeps performance information in a database. The manager has access to the values in the database.

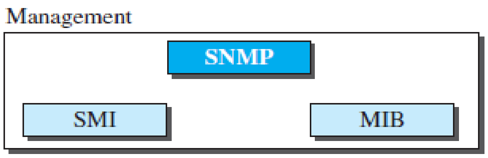
Management with SNMP is based on three basic ideas

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes the management process by warning the manager of an unusual situation.

Management Components

To do management tasks, SNMP uses two other protocols: **Structure of Management Information (SMI)** and **Management Information Base (MIB).** In other words, management on the Internet is done through the cooperation of three protocols: SNMP, SMI, and MIB

Figure 27.3 *Components of network management on the Internet*



Role of SNMP

SNMP has some very specific roles in network management. It defines the format of the packet to be send from a manager to an agent and vice versa. It also interprets the result and creates statistics. The packet exchange contains the object names (variables) and their status (values). SNMP is response for reading and changing these values.

Role of SMI

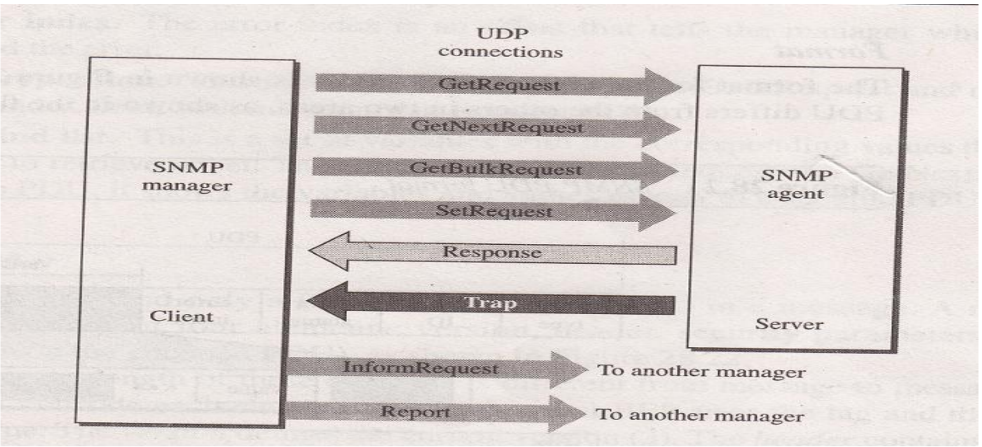
SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

Role of MIB

MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed

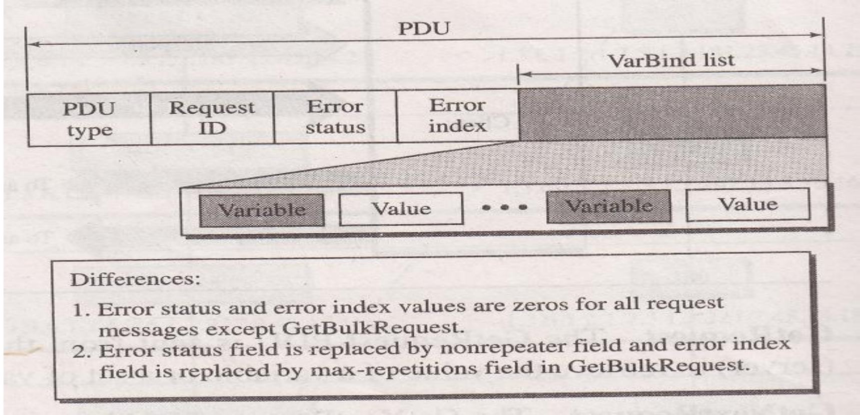
PDU's

SNMP V3 defines 8 types of packets



PDU Type	Name	Description
1	get-request	Get one or more variables .(manager to agent)
2	get-next-request	Get next variable after one or more specified variables. (manager to agent)
3	Get-bulk-request	To retrieve a large amount of data
4	set-request	Set one or more variables. (manager to agent)
5	get-response	Return value of one or More variables. (agent to manager)
6	trap	Notify manager of an event. (agent to manager)
7	Inform request	To get the value of some variable from agents under the control of the remote manager. The remote manager response with a response PDU. (one manager to another remote manager)
8	report	To report some types of errors between managers.

SNMP PDU Format



Differences:
1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by nonrepeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

- ➢ **PDU type -** This field defines the type of the PDU.
- ➢ **Request ID** – This field is a sequence number used by the manager in a request PDU and repeated by the agent in a response. It is used to match a request to a response.
- ➢ **Error status** – This is an integer that is used only in response PDU's to show the types of errors reported by the agent. Its value is zero in request PDU's.

Types of errors:

Error	Name	Description
0	no error	OK
1	too big	Reply does not fit into one message
2	no such name	The variable specified does not exist
3	bad value	Invalid value specified in a set request.
4	read only	The variable to be changed is read only.
5	general error	General error

Non Repeater: This field is used only in get-bulk-request and replaces the error status field which is empty in request PDU's.

- ➢ **Error Index**: Error index is an offset that tells the manager which variable caused the error.

Max-repetition: This field is also used only in get-bulk-request and replaces the error index filed, which is empty in request PDU's

- ➢ **VarBind List**: This is a set of variables with corresponding values the manager wants to retrieve or set. The values or null in get-request and get-next-request.

SNMP messages:

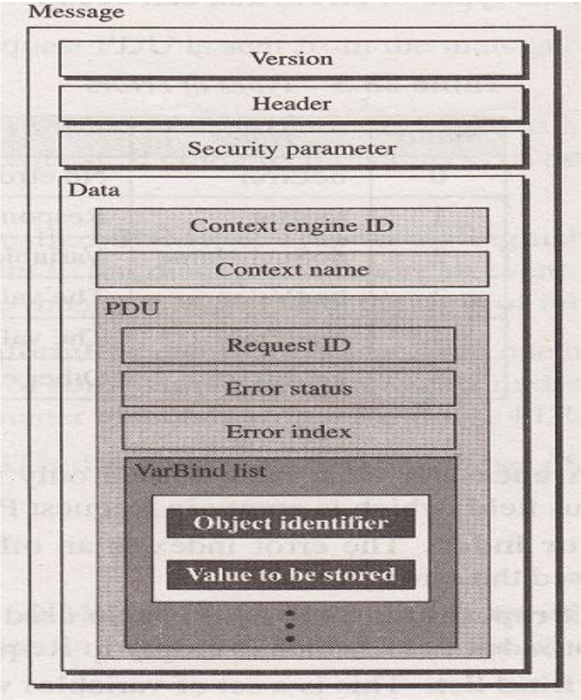
- SNMP does not send only a PDU, it embeds the PDU in a message. A message in SNMPv3 is made of four elements: version, header, security parameter and data.
- The **version**, defines the current version (3)
- The **header** contains values for message identification, maximum message size, message flag and a message security model.
- The message **security parameter** is used to create a message digest.
- The **data** contain the PDU. If the data are encrypted, there is information about the encrypting engine and the encrypting context followed by the encrypted PDU. If the data are not encrypted, the data consist of just the PDU.

UDP Ports:

SNMP uses the services of UDP on two well-known ports, 161 and 162. The well-known port 161 is used by the server (agent), and the well-known port 162 is used by the client (Manager).

Security:

- SNMPv3 provides two types of security: general and specific.
- SNMPv3 provides message authentication, privacy, and manager authorization.
- SNMPv3 allows a manager remotely change the security configuration, which means that the manager does not have to be physically present at the manager station.



9.Expalin the concept of TELNET (8.m)

TELNET is an abbreviation for TErminaL NETwork. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. TELNET general purpose client server application program.

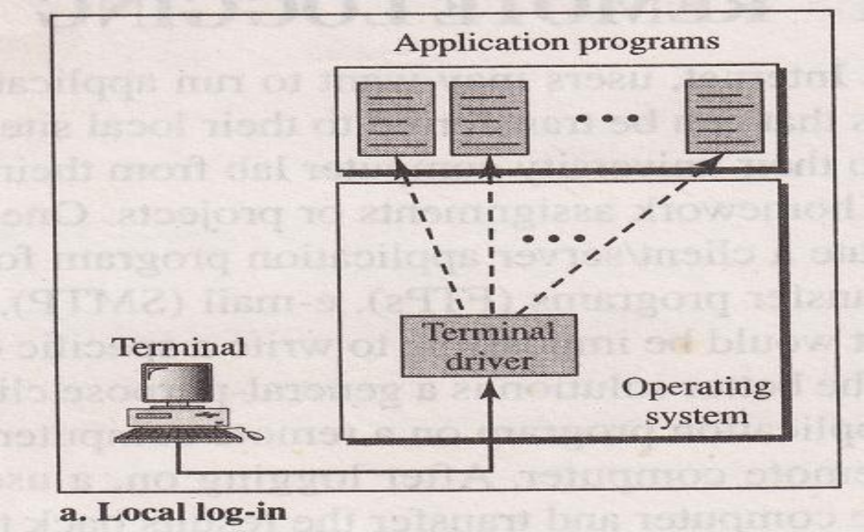
Using the Telnet protocol user on a local host can remote-login and execute commands on another distant host

Time sharing environment:

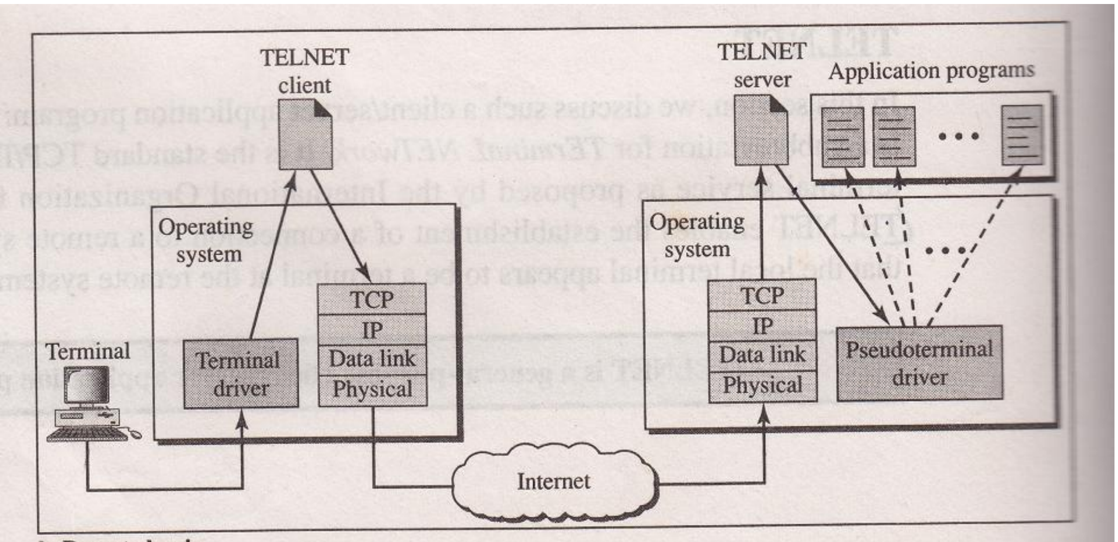
TELNET was designed at a time when most operating systems, such as UNIX, were operating in a time sharing environment. In this environment, a large computer supports multiple users. The interaction between a user and the computer occurs through a terminal, which is usually a combination of keyboard, monitor and mouse.

Logging:

In a time sharing environment, users are the part of the system with some rights to access the resources. To access the system, the authorized user logs in to the system with a user id or login name. This system also includes password checking to prevent an unauthorized users from accessing the resources.



a. Local log-in



b. Remote log-in

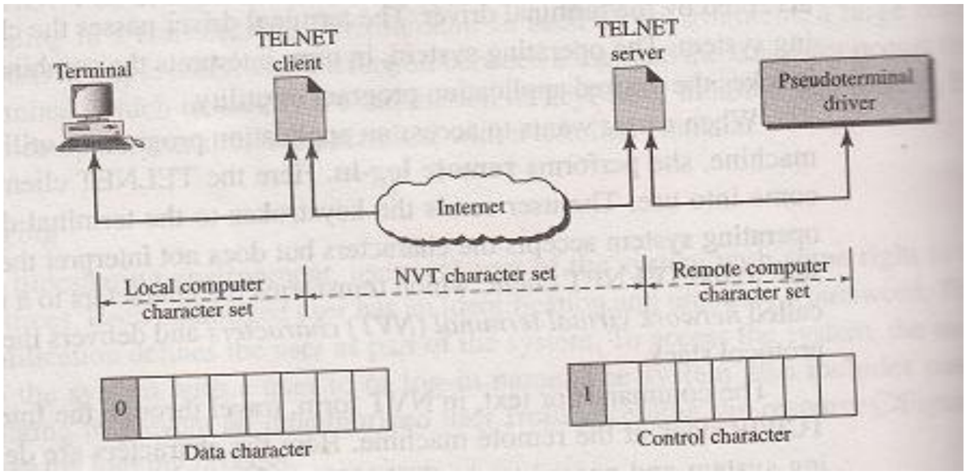
- When a user logs into a local timesharing system, it is called local log-in. As a user types at a terminal the keystrokes are accepted by the terminal deriver. The terminal driver passes the characters to the operating system. The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility.

- When a user wants to access an application program or utility located on a remote machine, she performs remote log-in. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver, where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters to a universal character set called network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack.

- The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. The solution is to add a piece of software called a pseudo terminal driver which pretends that the characters are coming from a terminal. The operating system then passes the characters to the appropriate application program.

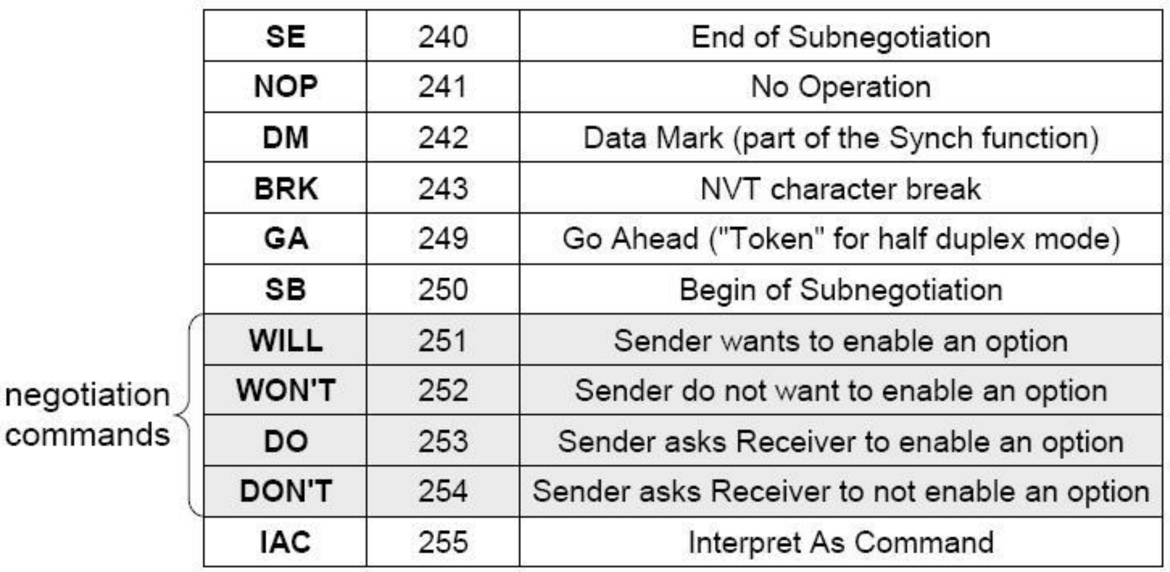
- **Network Virtual Terminal (NVT):**

Network Virtual Terminal, which transforms the characters to a universal character set and delivers them to the local TCP/IP stack.



NVT's Character Set

- NVT uses two sets of characters one for data and other for control.
- NVT generally use the 8 bit character set for both.
- NVT's data character set is the US ASCII 7-bit code.
- NVT can handle the printable characters with ASCII codes 32-126 plus a small set of control characters:



SE	240	End of Subnegotiation
NOP	241	No Operation
DM	242	Data Mark (part of the Synch function)
BRK	243	NVT character break
GA	249	Go Ahead ("Token" for half duplex mode)
SB	250	Begin of Subnegotiation
WILL	251	Sender wants to enable an option
WON'T	252	Sender do not want to enable an option
DO	253	Sender asks Receiver to enable an option
DON'T	254	Sender asks Receiver to not enable an option
IAC	255	Interpret As Command

negotiation commands

Embedding:

TELNET uses only one TCP connection. The same connection is used for sending both data and control characters. TELNET accomplishes this by embedding the control characters in the data stream. However, to distinguish data from control characters, each sequence of control characters is preceded by a special control character called interpret as control (IAC).

Options:

TELNET lets the client and server negotiate options before or during the use of service. Options are extra features available to a user with a more sophisticated terminal. Some common options:

Code	Option	Meaning
0	Binary	Interpret as 8-bit transmission
1	Echo	Echo the data received on one side to the other
3	Suppress go ahead	Suppress go-ahead signals after data
5	Status	Request the status of TELNET
6	Timing mark	Define the timing marks
24	Terminal type	Set the terminal type
32	Terminal speed	Set the terminal speed.
34	Line mode	Change to line mode

Option Negotiation:

To use any of the options mentioned in the previous section first requires option negotiation between the client and the server. In this four control character are used

Character	Decimal	Binary	Meaning
WILL	251	11111011	1. Offering to enable 2. Accepting a request to enable
WONT	252	11111100	1. Rejecting a request to enable 2. Offering to disable 3. Accepting a request to disable
DO	253	11111101	1. Approving an offer to enable 2. Requesting to enable
DON'T	254	11111110	1. Disapproving an offer to enable 2. Approving an offer to disable 3. Requesting to disable.

A party can offer to enable or disable an option if it has the right to do so. The offering can be approved or disapproved by the other party. To offer enabling, the offering party sends the WILL command, which means "Will I enable the option?" The other party sends either the DO command, which means "please do," or the DON'T command, which means "Please don't." To offer disabling, the offering party sends the WONT command, which means "I won't use this option anymore." The answer must be the don't command, which means "Don't use it anymore."

Sub option Negotiation:

Some option requires addition information. To define the type or speed of a terminal, the negotiation includes a string or a number to define the type or speed.

Character	Decimal	Binary	Meaning
SE	240	11110000	Suboption end
SB	250	11111010	Suboption begin

Mode of operation:

TELNET implementations operate in one of three modes. **Default mode**, **Character mode**, or **Line mode**.

Default Mode:

The default mode is used if no other modes are invoked through option negotiation. In this mode the echoing is done by the client. The user types a character, and the client echoes the character on the screen, but does not send it until a whole line is completed.

Character Mode:
In the character mode, each character typed is send by the client to the server. The server normally echoes the character back to be displayed on the client screen. In this mode the echoing of the character can be delayed with the transmission time is long.
Line Mode:
A new mode has been proposed to compensate for the deficiencies of the default mode and character mode. In this mode line editing is done by the client. The client then sends the whole line to the server.

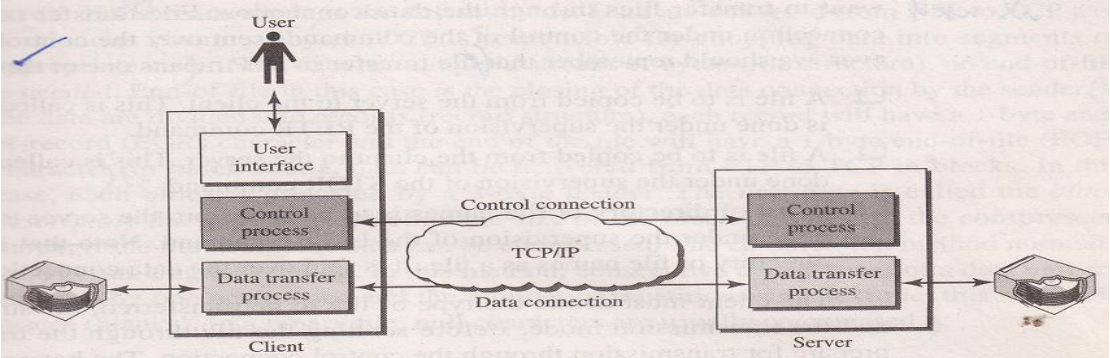
10.Discuss the various commands used in FTP (12) (MAY/JUNE 2009) (or) Discuss FTP with suitable diagram (Apr /may2011) (8)

FTP (File Transfer Protocol)

- FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straight forward.
- FTP differs from other client server applications, in that it establishes to connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). The control connection uses very simple rules of communications. We need to transfer only a line of command or a line of response at a time. The data connection needs more complex rules, due to the variety of data types transferred.
- FTP uses the services of the TCP. It needs two TCP connections, the port 21 is used for control connection and the port 20 is used for data connection.

Basic Model of FTP:

- ➢ The client has three components: **user interface**, **client control process** and the **client data transfer process.**
- ➢ The server has two components: the **server control process** and the **server data transfer process**.
- ➢ The control connection is need between the control processes. The data connection is made between the data transfer processes.



The control connection remains, connected during the entire interactive FTP session.
The data connection is opened and then closed for each file transferred.

Communication over Control Connection:
FTP uses the 7 bit ASCII character set to communicate across the control connection. Communication is achieved through commands and responses. In this, send one command or response at a time. Each command are response is only one short line, so need not worry about file format or file structure. Each line is terminated with a two character end of line token.

Communication over Data Connection:

It is used to transfer files through the data connection. File transfer occurs over the data connection under the control of the commands send over the control connection. File transfer in FTP means one of three things:

1. A file is to be copied from the server to the client. This is called **retrieving a file**. It is done under the supervision of the RETR command.
2. A file is to be copied from the client to the server. This is called **storing a file**. It is done under the supervision of STOR command.
3. A list of directories or file names is to be sending from the server to the client. This is done under the supervision of LIST command. FTP treats a list of directory or file names as a file. It is send over the data connection.

The client must define the **type of file to be transferred**, the **structure of the data** and **the transmission mode**. Before sending the file through the data connection, prepare for transmission for the control connection.

File Type:

FTP can transfer one of the following file types across the data connection: an ASCII file, EBCDIC file or IMAGE file.

- The **ASCII file** is the default format for transferring text files. Each character is encoded using 7-bit ASCII.
- A file can be transferred using **EBCDIC file.** Abbreviation of **E**xtended **B**inary-**C**oded **D**ecimal **I**nterchange **C**ode. EBCDIC is an IBM code for representing characters as numbers.
- The **IMAGE file** is the default format for transferring binary files.

Data Structure:

FTP can transfer a file across the data connection by using one of the following interpretations about the structure of the data: **file structure**, **record structure** and **page structure**.

- In the **file structure** format, the file is a continuous stream of bytes.
- In the **record structure** format, the file is divided in to records. This can be used only with text files.
- In the **page structure** format, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly and sequentially.

Transmission Mode:

FTP can transfer a file across the data connection by using one of the following three transmission modes: **stream mode**, **block mode** and **compressed mode**.

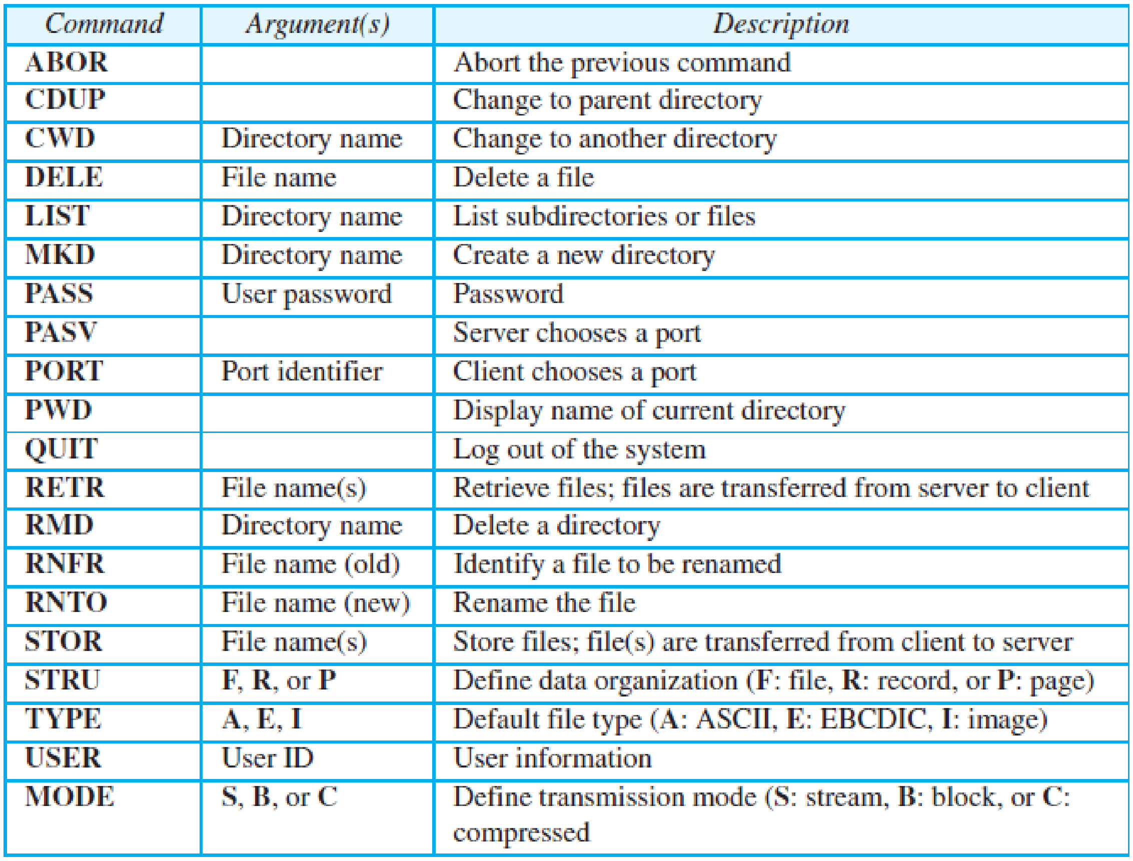
In **stream mode**, the data are delivered from FTP to TCP as a continuous stream of bytes. TCP is responsible for chopping data into segments of appropriate sizes. If the data are divided in to records, each record will have a one byte end of record (EOR) character and end of the file will have a one byte EOF character.

In **block mode**, the data can delivered from FTP to TCP blocks; in this case each block is preceded by a three byte header. The first byte is called the block descriptor; the next two bytes define the size of the block in bytes.

In the **compressed mode**, if the file is big the data can be compressed. The compressed method normally used is run length encoding. In this method, consecutive appearances of a data unit are replaced by one occurrence and the no of repetitions. In a text file this is usually spaces. In a binary null characters are compressed.

FTP Commands

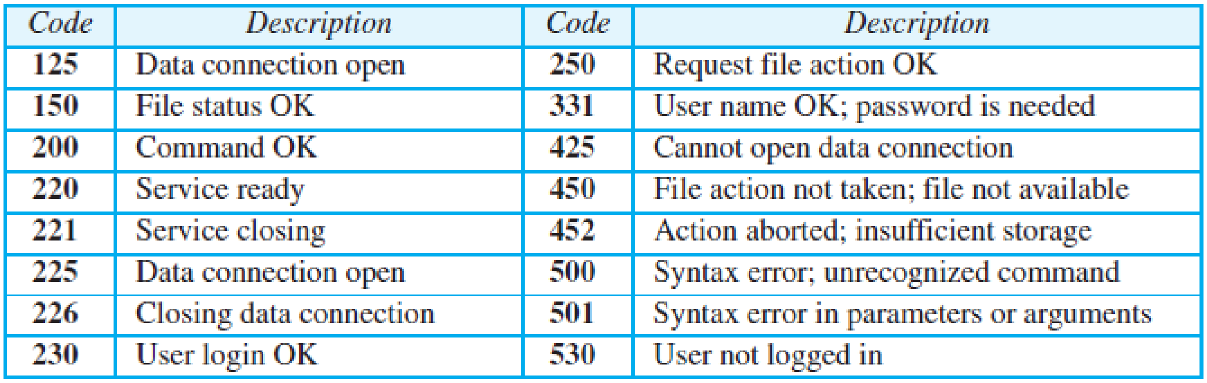
Table 26.4 *Some FTP commands*



Command	*Argument(s)*	*Description*
ABOR		Abort the previous command
CDUP		Change to parent directory
CWD	Directory name	Change to another directory
DELE	File name	Delete a file
LIST	Directory name	List subdirectories or files
MKD	Directory name	Create a new directory
PASS	User password	Password
PASV		Server chooses a port
PORT	Port identifier	Client chooses a port
PWD		Display name of current directory
QUIT		Log out of the system
RETR	File name(s)	Retrieve files; files are transferred from server to client
RMD	Directory name	Delete a directory
RNFR	File name (old)	Identify a file to be renamed
RNTO	File name (new)	Rename the file
STOR	File name(s)	Store files; file(s) are transferred from client to server
STRU	**F**, **R**, or **P**	Define data organization (**F**: file, **R**: record, or **P**: page)
TYPE	**A**, **E**, **I**	Default file type (**A**: ASCII, **E**: EBCDIC, **I**: image)
USER	User ID	User information
MODE	**S**, **B**, or **C**	Define transmission mode (**S**: stream, **B**: block, or **C**: compressed

Every FTP command generates at least one response. A response has two parts: a three-digit number followed by text. The numeric part defines the code; the text part defines needed parameters or further explanations. The first digit defines the status of the command. The second digit defines the area in which the status applies. The third digit provides additional information.

Table 26.5 *Some responses in FTP*

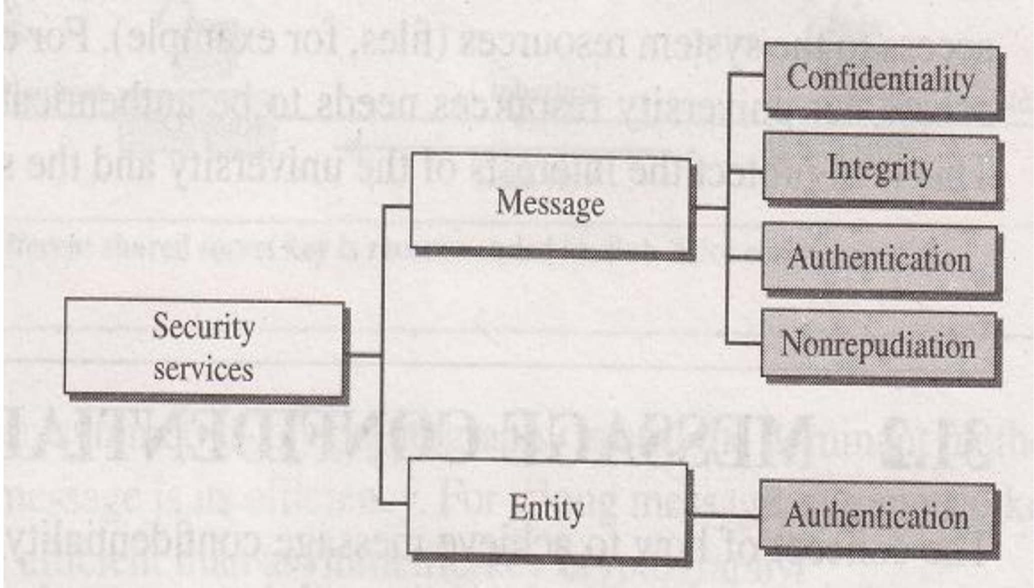


Code	*Description*	*Code*	*Description*
125	Data connection open	**250**	Request file action OK
150	File status OK	**331**	User name OK; password is needed
200	Command OK	**425**	Cannot open data connection
220	Service ready	**450**	File action not taken; file not available
221	Service closing	**452**	Action aborted; insufficient storage
225	Data connection open	**500**	Syntax error; unrecognized command
226	Closing data connection	**501**	Syntax error in parameters or arguments
230	User login OK	**530**	User not logged in

11. Write notes on Security protocol SSH in detail

Security in networking is based on cryptography (secret writing), the science and art of transforming messages to make them secure and immune to attack. Cryptography can provide confidentiality, integrity, authentication and non repudiation of messages.

Network Security can provide one of the 5 services.



- ***Message confidentiality:*** *Message confidentiality or privacy means that the sender and receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.*
- ***Message integrity:*** *Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidently nor maliciously.*
- ***Message Authentication:*** *Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.*
- ***Message Non repudiation:*** *Message Non repudiation means that a sender must not be able to deny sending a message that he or she did sent. The burden of proof falls on the receiver.*

Entity Authentication: *In entity authentication or user authentication, the entity or user is verified prior to access to the system resources.*

<u>PGP (Pretty Good Privacy)</u>

It is a protocol to provide security at the application layer. PGP is designed to create authenticated and confidential emails.

<u>SSH (Secure Shell)</u>

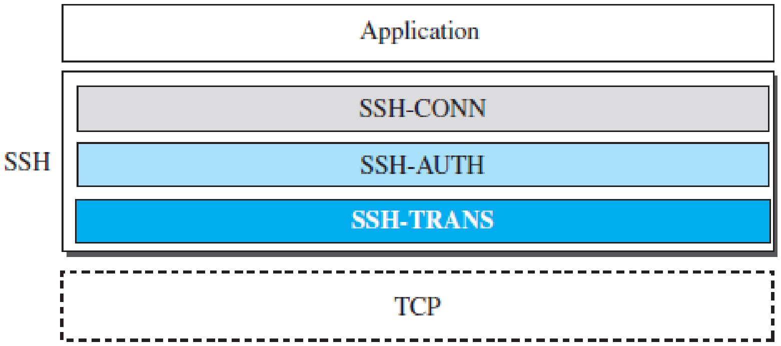
- SSH is a protocol for secure remote login and other secure network services over an insecure network. The Secure Shell (SSH) provides a remote login service and is intended to replace the less secure Telnet and rlogin programs used in the early days of the Internet.

- SSH is most often used to provide strong client/server authentication—where the SSH client runs on the user's desktop machine and the SSH server runs on some remote machine that the user wants to log into—but it also supports message integrity and confidentiality. Telnet and rlogin provide none of these capabilities.
- SSH provides a way to encrypt the data sent over these connections and to improve the strength of the authentication mechanism they use to login.

Major SSH components

- SSH Transport Layer Protocol
  - provides server authentication, confidentiality, and integrity services
  - it may provide compression
  - runs on top of any reliable transport layer (e.g., TCP)
- SSH User Authentication Protocol
  - provides client-side user authentication
  - runs on top of the SSH Transport Layer Protocol
- SSH Connection Protocol
  - multiplexes the secure tunnel provided by the SSH Transport Layer and User Authentication Protocols into several logical channels

Figure 26.25 *Components of SSH*



SSH security features

- Strong algorithms
  - uses well established strong algorithms for encryption, integrity, key exchange, and public key management
- Large key size
  - requires encryption to be used with at least 128 bit keys
  - supports larger keys
- Algorithm negotiation
  - encryption, integrity, key exchange, and public key algorithms are negotiated
  - it is easy to switch to some other algorithm without modifying the base protocol

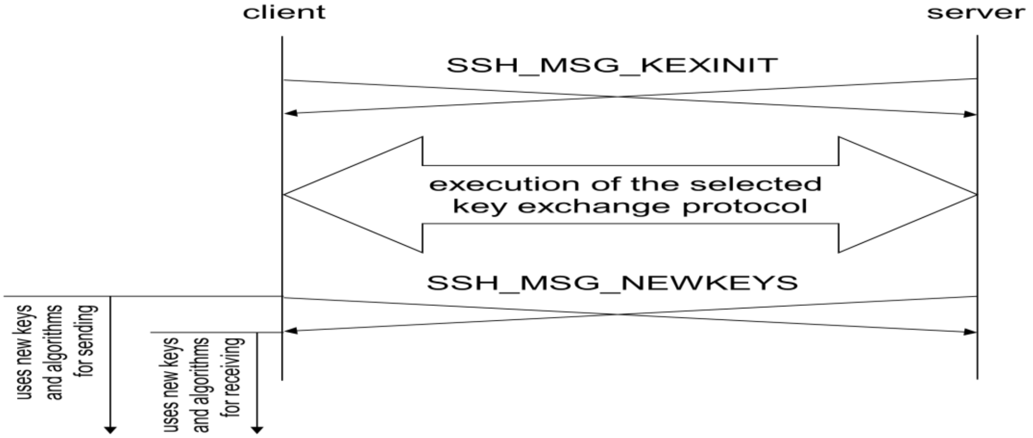
Transport Layer Protocol

- Client initiates connection to the server
- Identification string exchange
- Algorithms exchange
- Key exchanges include host key sent to client
  - Diffie-Hellman key exchange
  - Client selects a random session key

Connection setup and version string exchange

- SSH works over any 8-bit binary transport protocol, e.g., TCP
- Client initiates the connection on the port 22 on the server
- Underlying transport protocol should provide protection against transmission errors, e.g., TCP provides reliable byte stream service.
- Once the connection has been established, both client and server send a version exchange id string of the form "SSH-proto version-software version comments" followed by carriage return & new line character.
- Before the id string is sent, the server might send other strings with useful information to the client.
- The client should be capable of handling these strings and may/may not display it to the user.
- These are used by TCP wrappers to display an error message before disconnecting.
- Key exchange begins after the initial client-server version string exchange.

Key exchange – Overview


client
server
SSH_MSG_KEXINIT
execution of the selected key exchange protocol
SSH_MSG_NEWKEYS
uses new keys and algorithms for sending
uses new keys and algorithms for receiving

User Authentication Protocol

- the protocol assumes that the underlying transport protocol provides integrity and confidentiality (e.g., SSH Transport Layer Protocol)
- the protocol has access to the session ID
- the server should have a timeout for authentication and disconnect if the authentication has not been accepted within the timeout period
  - recommended value is 10 minutes
- the server should limit the number of failed authentication attempts a client may perform in a single session
  - recommended value is 20 attempts
- three authentication methods are supported
  - public key
  - password
  - host based

Connection Protocol

- provides
  - interactive login sessions
  - remote execution of commands
  - forwarded TCP/IP connections
- all these applications are implemented as "channels"
- all channels are multiplexed into the single encrypted tunnel provided by the SSH Transport Layer Protocol
- channels are identified by channel numbers at both ends of the connection
- channel numbers for the same channel at the client and server sides may differ

Anna university question paper

B.E/B.TECH NOVEMBER/DECEMBER 2014

2 MARKS

1. State the difference between SMTP and MIME. (Q.NO 3)
2. List down the key lengths supported by PGP (Q.NO 28)

16 MARKS

1. Write notes on URLS (16) (Q.NO 4)
2. (i) Discuss the advantages of DNS (8) (Q.NO 6)
   (ii) Explain Telnet in detail (8) (Q.NO 9)

B.E/B.Tech April May 2015

2 MARKS

1. Define SMTP (Q.NO 1)
2. What are the groups of HTTP header? (Q.NO 29)

16 MARKS

1. .i.Explain the message transfer using Simple Mail Transfer Protocol.(8) (Q.NO 2)
ii.Explain the final delivery of email to the end user using POP3.(8) (Q.NO 4)
2.Write short notes on. i.Web services (Q.NO 8) ii.SNMP(Q.NO 7)

B.E/B.Tech Nov-Dec 2015

2 MARKS

1. Mention the types of HTTP messages. (Q.NO 32)
2. What is SMTP? (Q.NO 1)

16 MARKS

1. Explain in detail about domain name system (Q.NO 6)
2. Write short notes onEmail&HTTP (Q.NO 1 &5)

B.E/B.Tech April-May 2016

2 MARKS

1. Define URL. (Q.NO 30)
2. Mention the different levels in domain name space. (Q.NO 31)

16 MARKS

1. a)Describe how SMTP protocol is used in E-mail applications. (Q.NO1,2)
   b) Explain HTTP with an example (Q.NO 5)
2. Explain in detail about Web service architecture (Q.NO 8)

B.E/B.Tech Nov-Dec 2016

2 MARKS

1. Expand POP3 and IMAP4. (Q.NO 13 & 14)
2. What is persistent HTTP. (Q.NO 16)

16 MARKS

1.Give a detailed note on DNS operation (Q.NO 6)

2. a)Explain in detail about SNMP messages. (Q.NO 7)
   b)Illustrate the role of POP3 in Electronic mail Applicatons (Q.NO 4)

B.E/B.Tech Apr-May 2017

PART A

1.State the usage of conditional get in HTTP(Q.No 33)

2.Present the information contained in a DNS resource record?(Q.No 34)

PART B

1. i) Describe how SMTP transfer message from one host to another with suitable illustration?(Q.No 2)
   ii) Explain IMAP with its state transition diagram.?(Q.No 4)
2. i) What is Domain Name System(DNS)?Explain(Q.No 6)
   ii) Brief about the importance of Simple Network Management Protocol(SNMP) (Q.No 7)

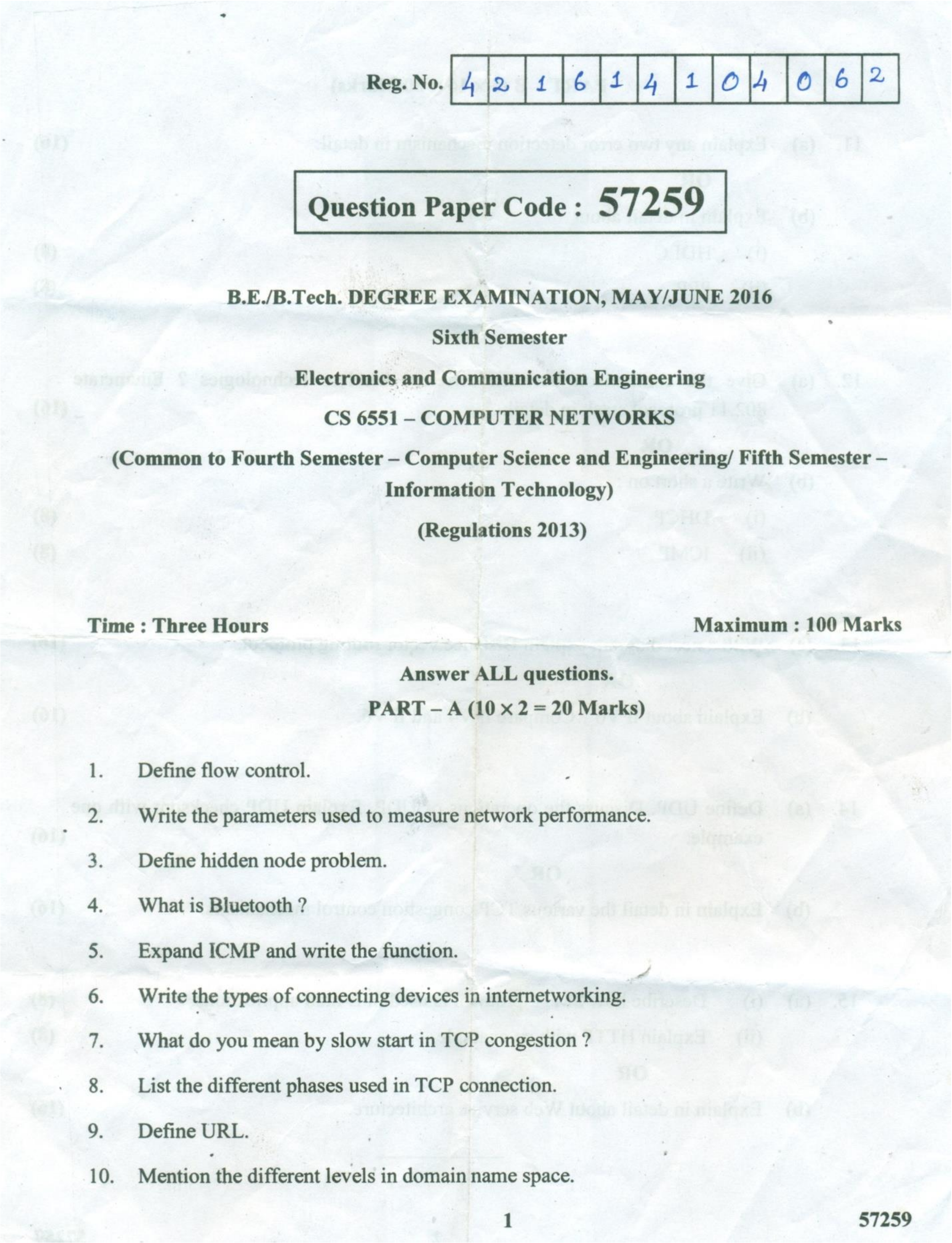
B.E/B.TechNov-Dec 2017

PART A

1. Write the use of HTTP (Q.No 35)
2. What do you meant by web services description language(WSDL)?(Q.No25)

PART B

1. i) Explain the functions of IMAP with a state transition diagram. (Q.No 4)
   ii) List and Explain the various HTTP request operations (Q.No 5)
2. i)List the element of network management and explain the operation of SNMP protocol in detail? (Q.No 7)
   ii) Discuss the function performed by of DNS . Give example. (Q.No6)



Reg. No. 4 2 1 6 1 4 1 0 4 0 6 2

Question Paper Code : 57259

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2016

Sixth Semester

Electronics and Communication Engineering

CS 6551 – COMPUTER NETWORKS

(Common to Fourth Semester – Computer Science and Engineering/ Fifth Semester – Information Technology)

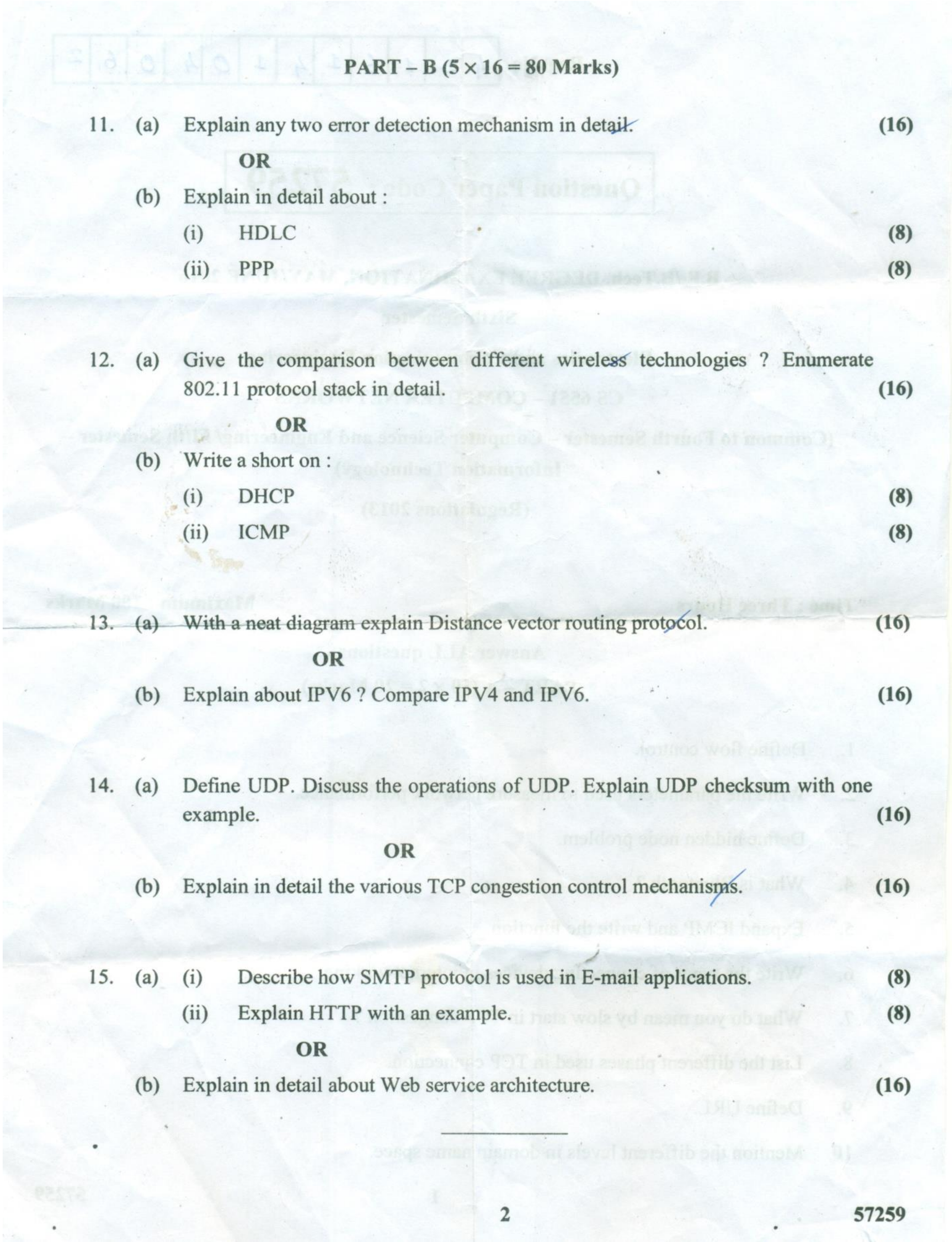
(Regulations 2013)

Time : Three Hours **Maximum : 100 Marks**

Answer ALL questions.

PART – A (10 × 2 = 20 Marks)

1. Define flow control.
2. Write the parameters used to measure network performance.
3. Define hidden node problem.
4. What is Bluetooth ?
5. Expand ICMP and write the function.
6. Write the types of connecting devices in internetworking.
7. What do you mean by slow start in TCP congestion ?
8. List the different phases used in TCP connection.
9. Define URL.
10. Mention the different levels in domain name space.



PART – B (5 × 16 = 80 Marks)

11. (a) Explain any two error detection mechanism in detail. **(16)**

OR

(b) Explain in detail about :

(i) HDLC **(8)**

(ii) PPP **(8)**

12. (a) Give the comparison between different wireless technologies ? Enumerate 802.11 protocol stack in detail. **(16)**

OR

(b) Write a short on :

(i) DHCP **(8)**

(ii) ICMP **(8)**

13. (a) With a neat diagram explain Distance vector routing protocol. **(16)**

OR

(b) Explain about IPV6 ? Compare IPV4 and IPV6. **(16)**

14. (a) Define UDP. Discuss the operations of UDP. Explain UDP checksum with one example. **(16)**

OR

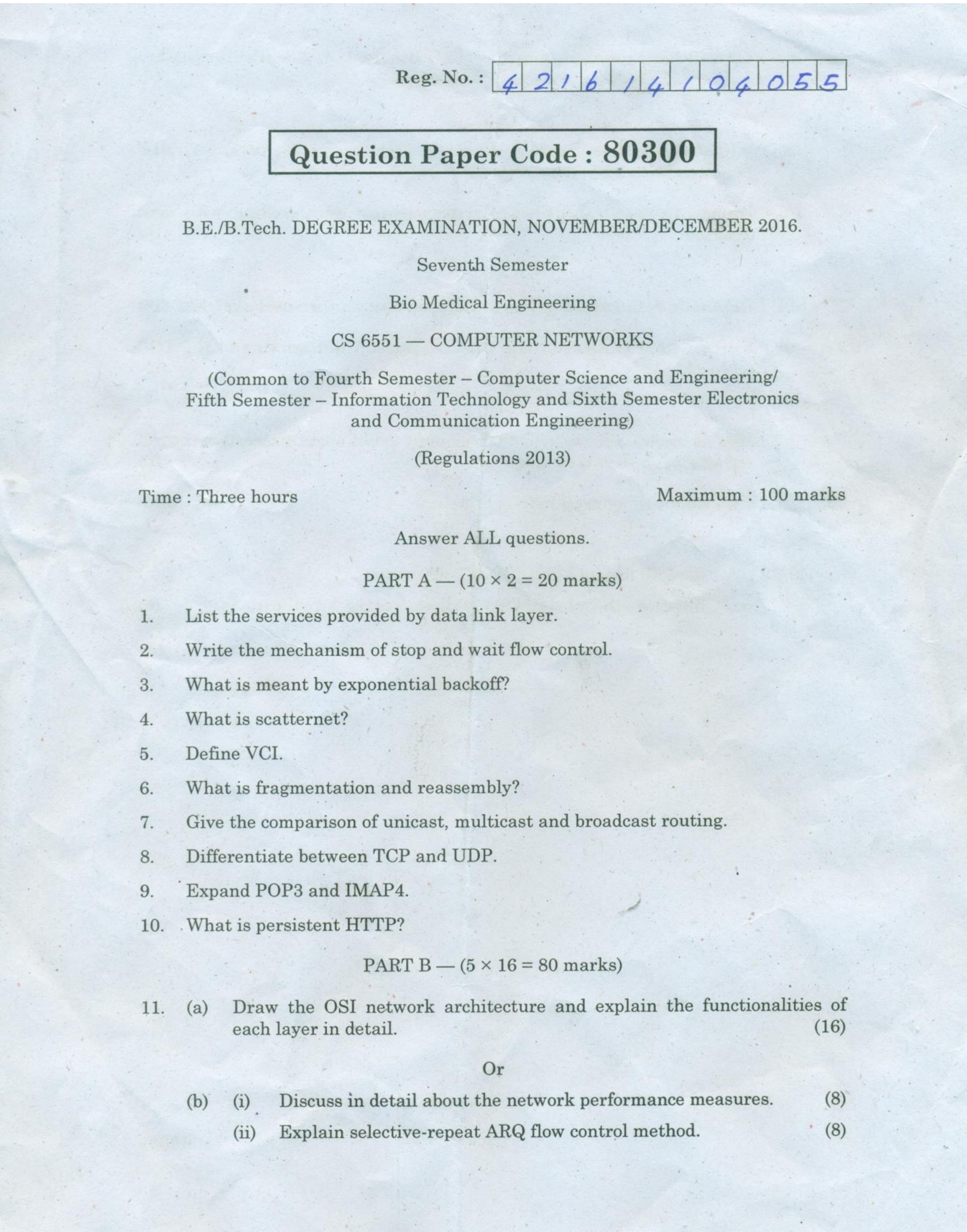
(b) Explain in detail the various TCP congestion control mechanisms. **(16)**

15. (a) (i) Describe how SMTP protocol is used in E-mail applications. **(8)**

(ii) Explain HTTP with an example. **(8)**

OR

(b) Explain in detail about Web service architecture. **(16)**



Reg. No. : 4 2 1 6 1 4 1 0 4 0 5 5

Question Paper Code : 80300

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Bio Medical Engineering

CS 6551 — COMPUTER NETWORKS

(Common to Fourth Semester – Computer Science and Engineering/
Fifth Semester – Information Technology and Sixth Semester Electronics
and Communication Engineering)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. List the services provided by data link layer.
2. Write the mechanism of stop and wait flow control.
3. What is meant by exponential backoff?
4. What is scatternet?
5. Define VCI.
6. What is fragmentation and reassembly?
7. Give the comparison of unicast, multicast and broadcast routing.
8. Differentiate between TCP and UDP.
9. Expand POP3 and IMAP4.
10. What is persistent HTTP?

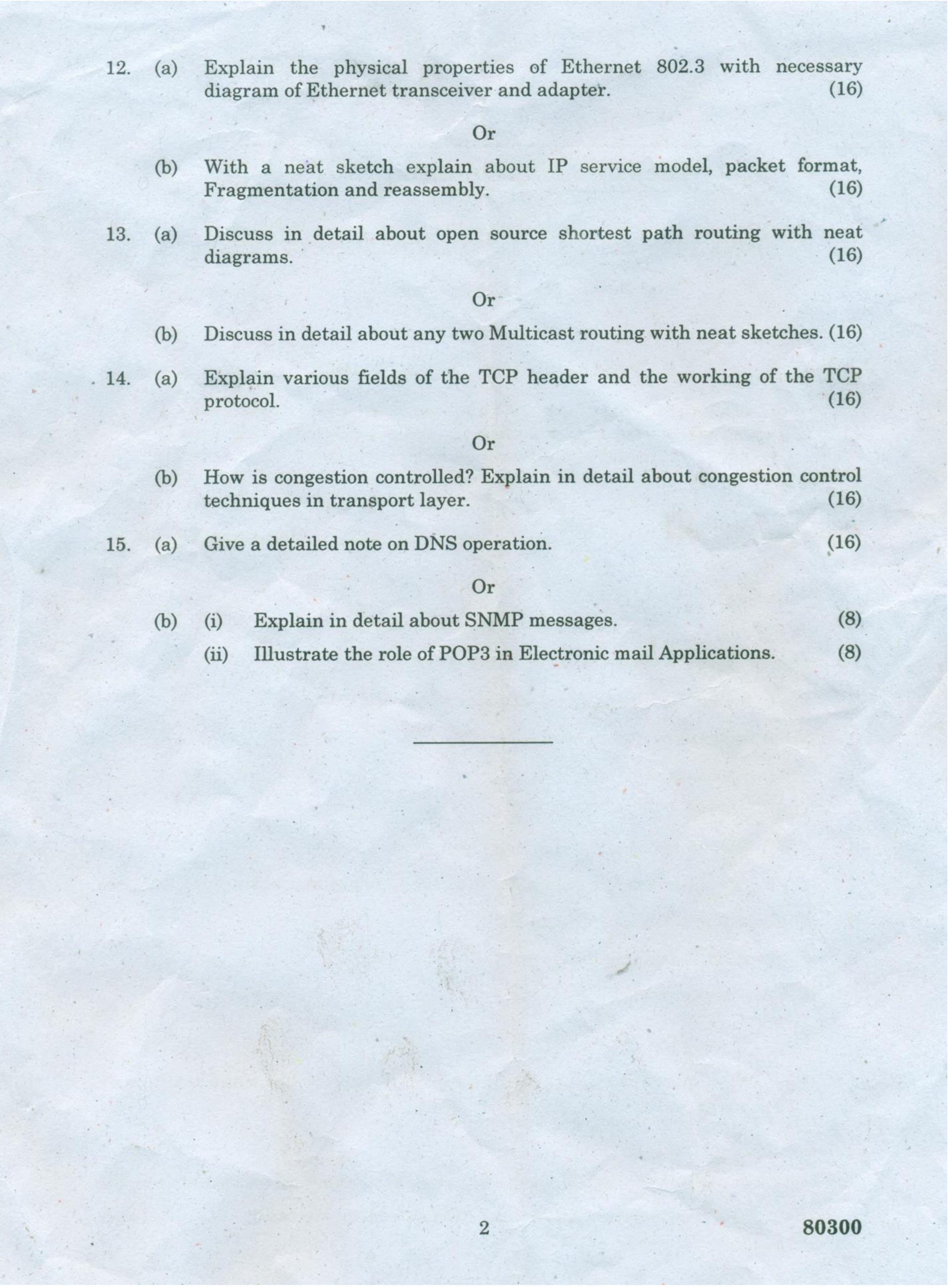
PART B — (5 × 16 = 80 marks)

11. (a) Draw the OSI network architecture and explain the functionalities of each layer in detail. (16)

Or

(b) (i) Discuss in detail about the network performance measures. (8)

(ii) Explain selective-repeat ARQ flow control method. (8)



12. (a) Explain the physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver and adapter. (16)

Or

(b) With a neat sketch explain about IP service model, packet format, Fragmentation and reassembly. (16)

13. (a) Discuss in detail about open source shortest path routing with neat diagrams. (16)

Or

(b) Discuss in detail about any two Multicast routing with neat sketches. (16)

14. (a) Explain various fields of the TCP header and the working of the TCP protocol. (16)

Or

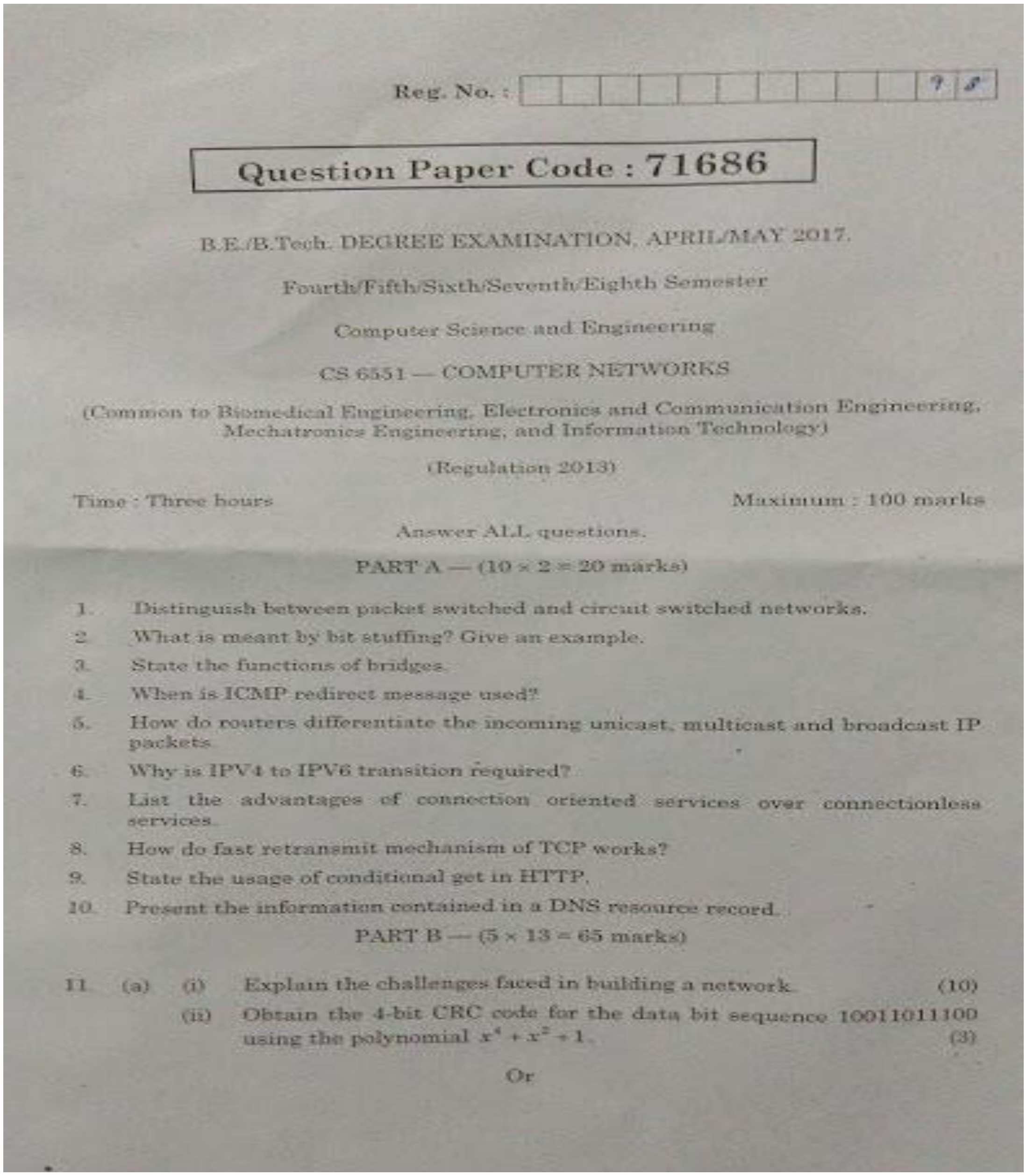
(b) How is congestion controlled? Explain in detail about congestion control techniques in transport layer. (16)

15. (a) Give a detailed note on DNS operation. (16)

Or

(b) (i) Explain in detail about SNMP messages. (8)

(ii) Illustrate the role of POP3 in Electronic mail Applications. (8)



Reg. No. : 7 8

Question Paper Code : 71686

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2017.

Fourth/Fifth/Sixth/Seventh/Eighth Semester

Computer Science and Engineering

CS 6551 — COMPUTER NETWORKS

(Common to Biomedical Engineering, Electronics and Communication Engineering, Mechatronics Engineering, and Information Technology)

(Regulation 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

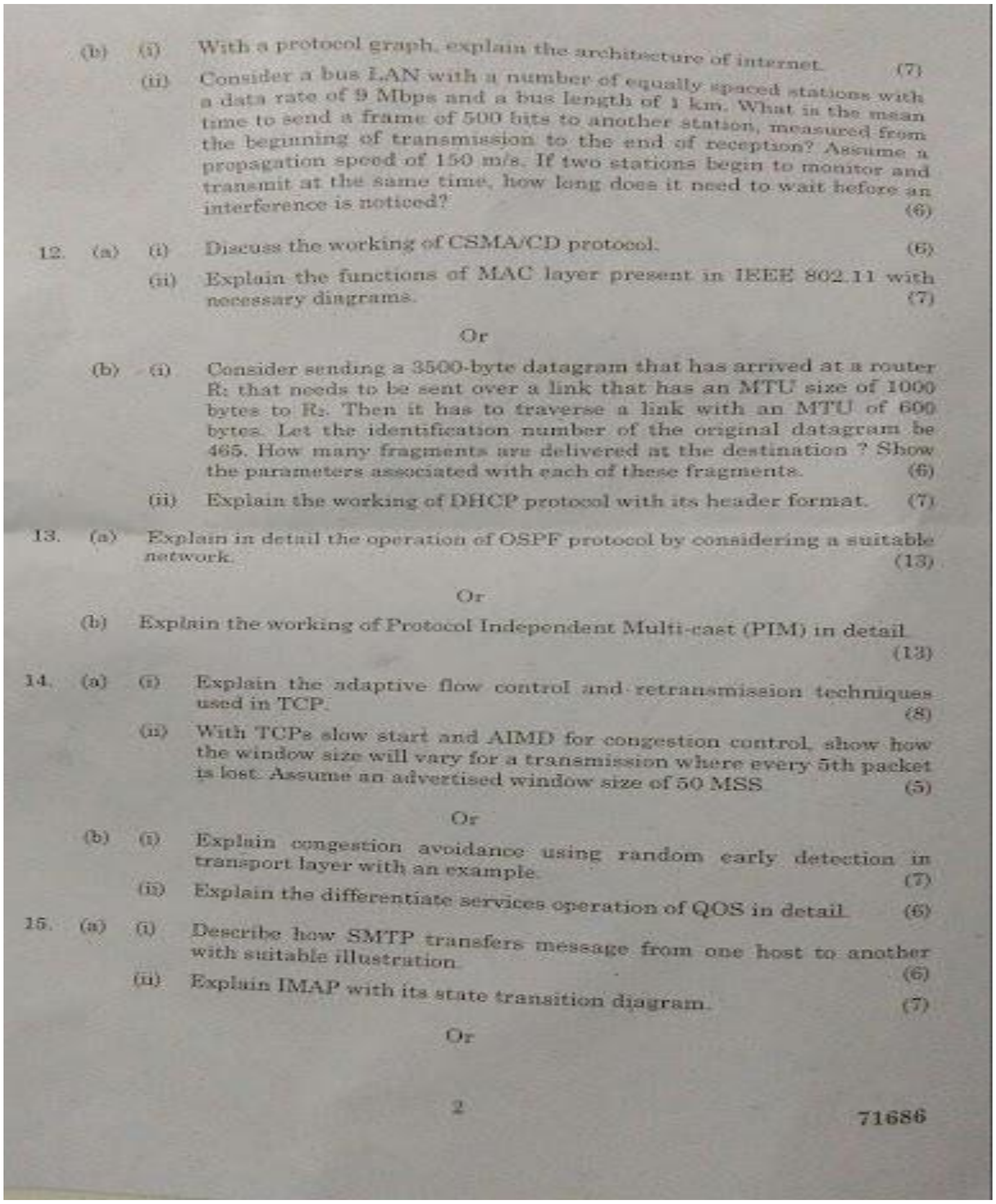
1. Distinguish between packet switched and circuit switched networks.
2. What is meant by bit stuffing? Give an example.
3. State the functions of bridges.
4. When is ICMP redirect message used?
5. How do routers differentiate the incoming unicast, multicast and broadcast IP packets.
6. Why is IPV4 to IPV6 transition required?
7. List the advantages of connection oriented services over connectionless services.
8. How do fast retransmit mechanism of TCP works?
9. State the usage of conditional get in HTTP.
10. Present the information contained in a DNS resource record.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Explain the challenges faced in building a network. (10)

(ii) Obtain the 4-bit CRC code for the data bit sequence 10011011100 using the polynomial $x^4 + x^2 + 1$. (3)

Or



(b) (i) With a protocol graph, explain the architecture of internet. (7)

(ii) Consider a bus LAN with a number of equally spaced stations with a data rate of 9 Mbps and a bus length of 1 km. What is the mean time to send a frame of 500 bits to another station, measured from the beginning of transmission to the end of reception? Assume a propagation speed of 150 m/s. If two stations begin to monitor and transmit at the same time, how long does it need to wait before an interference is noticed? (6)

12. (a) (i) Discuss the working of CSMA/CD protocol. (6)

(ii) Explain the functions of MAC layer present in IEEE 802.11 with necessary diagrams. (7)

Or

(b) (i) Consider sending a 3500-byte datagram that has arrived at a router R_1 that needs to be sent over a link that has an MTU size of 1000 bytes to R_2. Then it has to traverse a link with an MTU of 600 bytes. Let the identification number of the original datagram be 465. How many fragments are delivered at the destination ? Show the parameters associated with each of these fragments. (6)

(ii) Explain the working of DHCP protocol with its header format. (7)

13. (a) Explain in detail the operation of OSPF protocol by considering a suitable network. (13)

Or

(b) Explain the working of Protocol Independent Multi-cast (PIM) in detail. (13)

14. (a) (i) Explain the adaptive flow control and retransmission techniques used in TCP. (8)

(ii) With TCPs slow start and AIMD for congestion control, show how the window size will vary for a transmission where every 5th packet is lost. Assume an advertised window size of 50 MSS. (5)

Or

(b) (i) Explain congestion avoidance using random early detection in transport layer with an example. (7)

(ii) Explain the differentiate services operation of QOS in detail. (6)

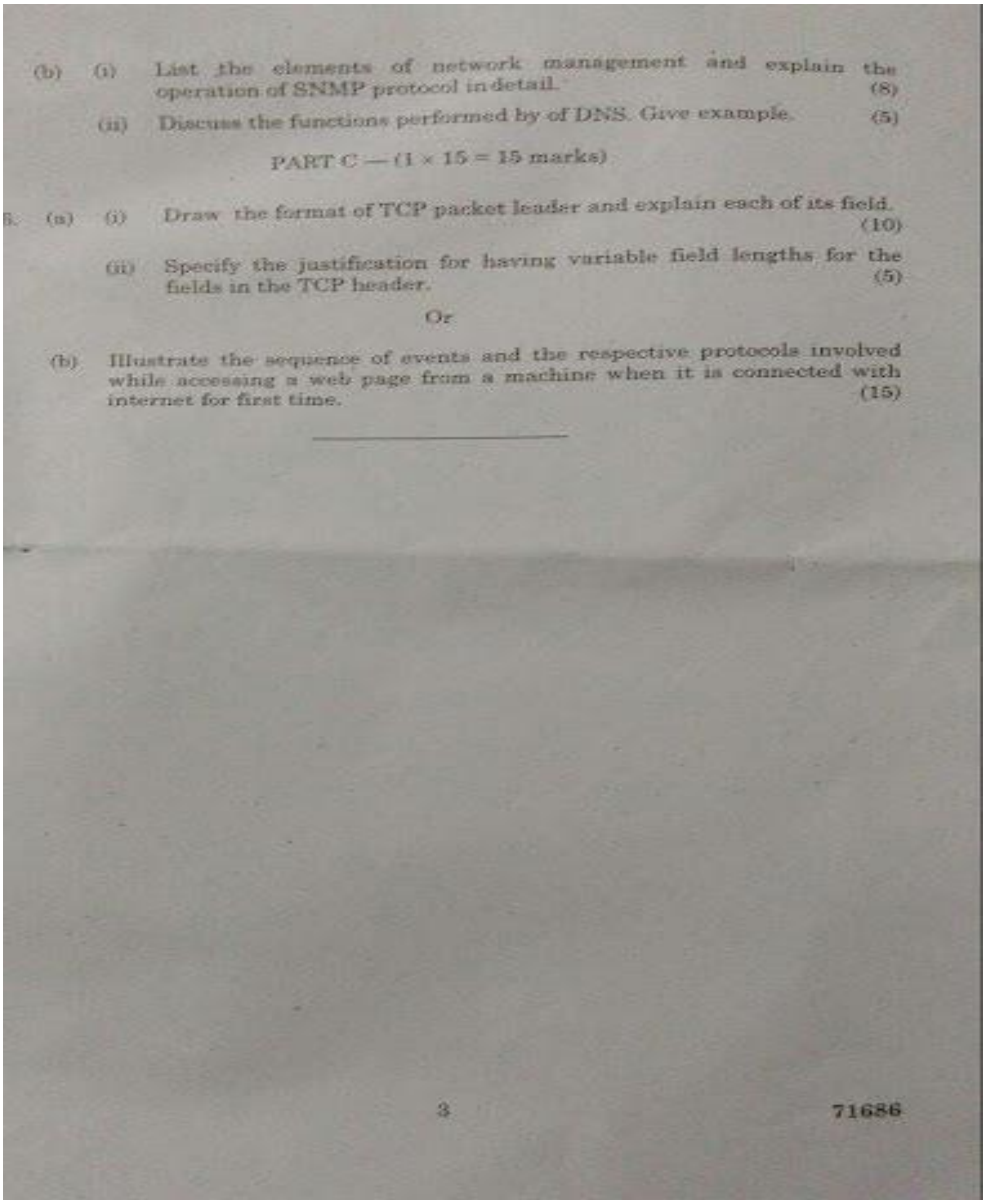
15. (a) (i) Describe how SMTP transfers message from one host to another with suitable illustration. (6)

(ii) Explain IMAP with its state transition diagram. (7)

Or

2

71686



(b) (i) List the elements of network management and explain the operation of SNMP protocol in detail. (8)

(ii) Discuss the functions performed by of DNS. Give example. (5)

PART C — (1 × 15 = 15 marks)

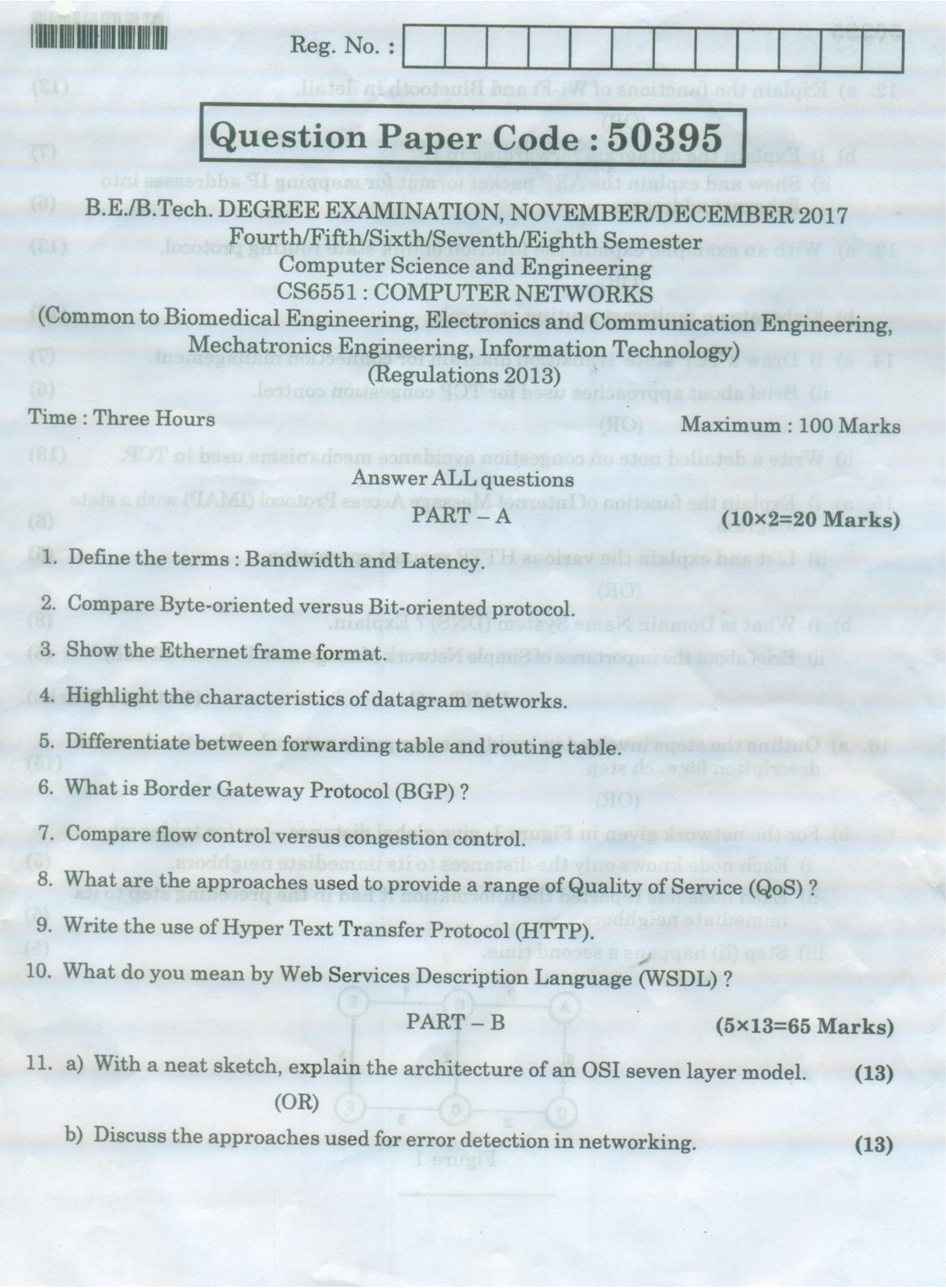
6. (a) (i) Draw the format of TCP packet leader and explain each of its field. (10)

(ii) Specify the justification for having variable field lengths for the fields in the TCP header. (5)

Or

(b) Illustrate the sequence of events and the respective protocols involved while accessing a web page from a machine when it is connected with internet for first time. (15)

3 71686



Reg. No. : □□□□□□□□□□□□

Question Paper Code : 50395

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2017

Fourth/Fifth/Sixth/Seventh/Eighth Semester

Computer Science and Engineering

CS6551 : COMPUTER NETWORKS

(Common to Biomedical Engineering, Electronics and Communication Engineering, Mechatronics Engineering, Information Technology)

(Regulations 2013)

Time : Three Hours Maximum : 100 Marks

Answer ALL questions

PART – A (10×2=20 Marks)

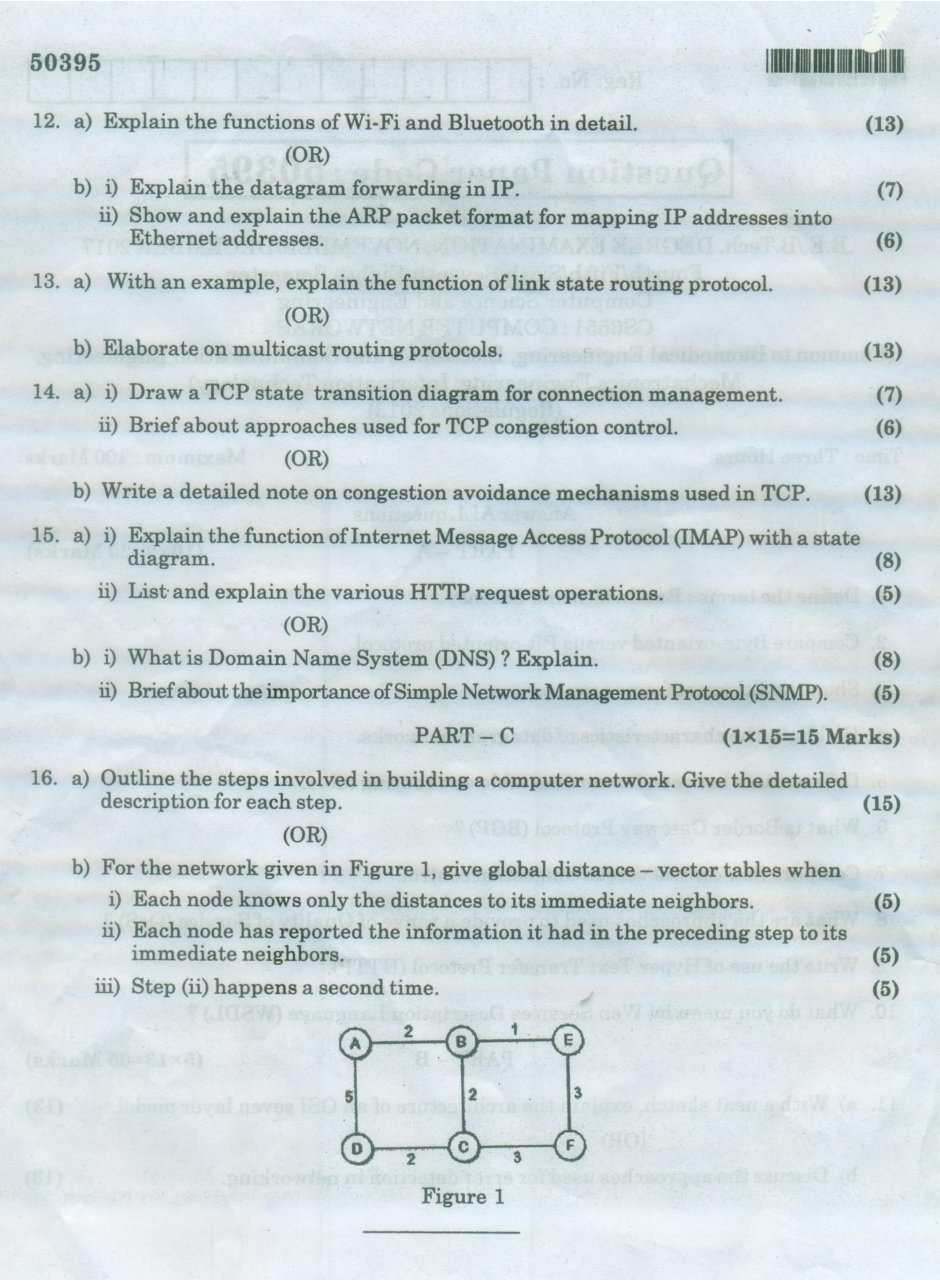
1. Define the terms : Bandwidth and Latency.
2. Compare Byte-oriented versus Bit-oriented protocol.
3. Show the Ethernet frame format.
4. Highlight the characteristics of datagram networks.
5. Differentiate between forwarding table and routing table.
6. What is Border Gateway Protocol (BGP) ?
7. Compare flow control versus congestion control.
8. What are the approaches used to provide a range of Quality of Service (QoS) ?
9. Write the use of Hyper Text Transfer Protocol (HTTP).
10. What do you mean by Web Services Description Language (WSDL) ?

PART – B (5×13=65 Marks)

11. a) With a neat sketch, explain the architecture of an OSI seven layer model. (13)

(OR)

b) Discuss the approaches used for error detection in networking. (13)



50395

12. a) Explain the functions of Wi-Fi and Bluetooth in detail. (13)

(OR)

b) i) Explain the datagram forwarding in IP. (7)

ii) Show and explain the ARP packet format for mapping IP addresses into Ethernet addresses. (6)

13. a) With an example, explain the function of link state routing protocol. (13)

(OR)

b) Elaborate on multicast routing protocols. (13)

14. a) i) Draw a TCP state transition diagram for connection management. (7)

ii) Brief about approaches used for TCP congestion control. (6)

(OR)

b) Write a detailed note on congestion avoidance mechanisms used in TCP. (13)

15. a) i) Explain the function of Internet Message Access Protocol (IMAP) with a state diagram. (8)

ii) List and explain the various HTTP request operations. (5)

(OR)

b) i) What is Domain Name System (DNS) ? Explain. (8)

ii) Brief about the importance of Simple Network Management Protocol (SNMP). (5)

PART – C **(1×15=15 Marks)**

16. a) Outline the steps involved in building a computer network. Give the detailed description for each step. (15)

(OR)

b) For the network given in Figure 1, give global distance – vector tables when

i) Each node knows only the distances to its immediate neighbors. (5)

ii) Each node has reported the information it had in the preceding step to its immediate neighbors. (5)

iii) Step (ii) happens a second time. (5)

Figure 1

UNIT IV - TRANSPORT LAYER

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram Protocol – Transmission Control Protocol – SCTP.

2 Marks

1) List the duties of Transport Layer (TL)

- Packetizing
- Connection Control
- Addressing
- Providing reliability

2) What is the difference between TCP & UDP? (NOV 2014 & 2016)

TCP	**UDP**
Connection Oriented Service	Connection less Service
Reliable	Not much reliable
Not suitable for multimedia, real time applications	used for multimedia and multicasting applications

3) What is socket? Define socket address.

Socket is the end point of a bi-directional communication flow across IP based network (Internet)

Socket address is the combination of an IP address (location of computer) and a port (application program process) into a single entity.

4) What is congestion? How to control congestion?

Congestion in network is the network is the situation in which an increase in data transmission results in a reduction in the throughput.

Throughput-amount of data passes through network congestion can be controlled using two techniques.

- Open-loop congestion control (prevention)
- Closed-loop congestion control(removal)

5) Define jitter

Jitter is the variation in delay for packets belonging to the same flow.

Example: 2ms delay for 1st packet
60ms delay for second packet.

6) What is the use of integrated services?

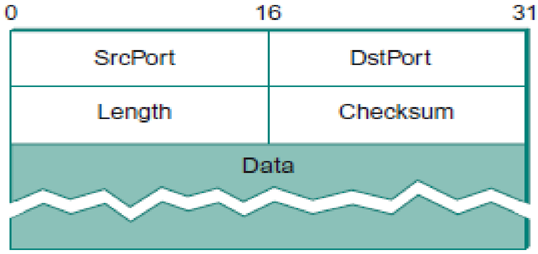
Integrated services (Instserv) is a followed based QoS model where the user creates a flow from source to direction and inform all the routers of the rource requirement.

7). Differentiate between delay and jitter.

Voice over IP (VoIP) is susceptible to network behaviors, referred to as delay and jitter, which can degrade the voice application to the point of being unacceptable to the average user. Delay is the time taken from point-to-point in a network. Delay can be measured in either one-way or round-trip delay.

Jitter is the VARIATION in delay over time from point-to-point. If the delay of transmissions varies too widely in a VoIP call, the call quality is greatly degraded. The amount of jitter tolerable on the network is affected by the depth of the jitter buffer on the network equipment in the voice path. The more jitter buffer available, the more the network can reduce the effects of jitter.

8) Draw UDP header format



9) What is traffic shaping?

Traffic shaping is a mechanism to control the amount and rate of traffic sent to the network.

10) What is the unit of data transfer in UDP and TCP?

In UDP, the Unit of data transfer is called datagram.

In TCP, Unit of data transfer is called segments.

11) List the timers used by TCP.

1) Retransmission timer
2) Persistence timer
3) Keep alive timer
4) Time waited timer

12) Define Sill window syndrome.

Sending less amount of Data (Ex. 1 byte) which is lesser than header size (20 bytes of TCP header +20 bytes of IP header) is called silly window syndrome. Here the capacity of network is used inefficiently.

13. Explain the main idea of UDP? Or Simple Demultiplexer

The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

14. What are the different fields in pseudo header?

- Protocol number
- Source IP address
- Destination IP addresses.

15. Define TCP? Or Reliable byte stream

TCP guarantees the reliable, in order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

16. Define Congestion Control?

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

17. State the two kinds of events trigger a state transition?

- A segment arrives from the peer.
- The local application process invokes an operation on TCP.

18. What is meant by segment?

At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

19. What is meant by segmentation?

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

20. What is meant by Concatenation?

The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

21. What is rate based design?

Rate- based design, in which the receiver tells the sender the rate-expressed in either bytes or packets per second – at which it is willing to accept incoming data.

22. Define Gateway.

A device used to connect two separate networks that use different communication protocols.

23. What are the two categories of QoS attributes?

The two main categories are,

- User Oriented
- Network Oriented

24. What is RED?

Random Early Detection in each router is programmed to monitor its own queue length and when it detects that congestion is imminent, to notify the source to adjust its congestion window.

25. What are the three events involved in the connection?

For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:

- Connection establishment
- Data transfer
- Connection release

26. Give the approaches to improve the QoS

Four common techniques are:

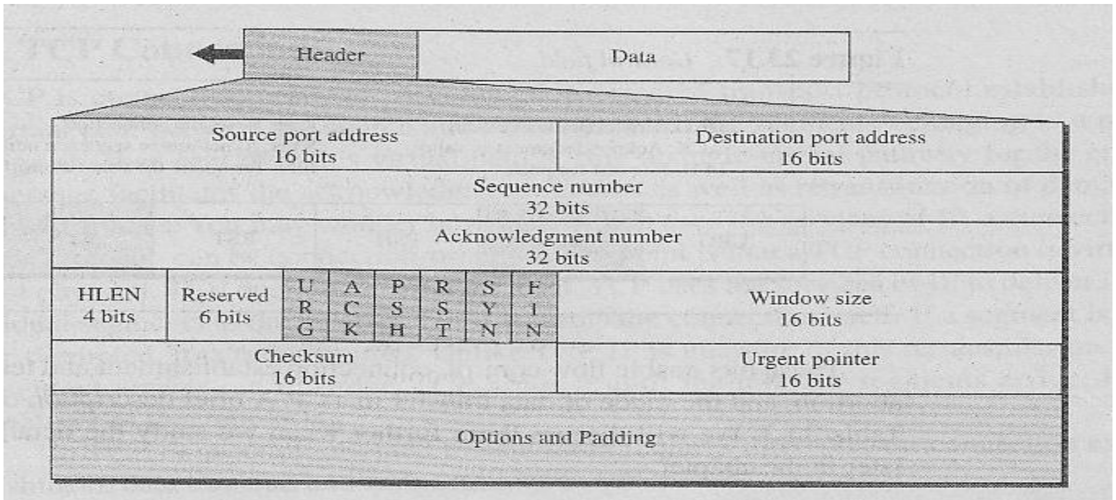
- ➢ Scheduling

- Traffic shaping
- Admission control
- Resource reservation

27. What is the difference between service point address, logical address and physical address? Service point addressing Logical addressing Physical addressing

Service point addressing	**Logical addressing**	**Physical addressing**
The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver.	If the frames are to be distributed to different systems on the network, the data link layer adds the header, which defines the source machine' s address and the destination Machine' s address.

28. Draw TCP header format



29. How will the congestion be avoided?
The congestion may be avoided by two bits
BECN - Backward Explicit Congestion Notification
FECN - Forward Explicit Congestion Notification

30. What is the function of BECN BIT?
The BECN bit warns the sender of congestion in network. The sender can respond to this warning by simply reducing the data rate.

31. What is the function of FECN?

The FECN bit is used to warn the receiver of congestion in the network. The sender and receiver are communicating with each other and are using some types of flow control at a higher level.

32. What is meant by quality of service or QoS? (NOV 2014 & 2015)

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

33. List out the user related attributes?

User related attributes are
SCR – Sustainable Cell Rate
PCR – Peak Cell Rate
MCR- Minimum Cell Rate
CVDT – Cell Variation Delay Tolerance

34. What are the networks related attributes?

The network related attributes are,
Cell loss ratio (CLR)
Cell transfer delay (CTD)
Cell delay variation (CDV)
Cell error ratio (CER)

35. Why is UDP pseudo header included in UDP checksum calculation? What is the effect of an invalid checksum at the receiving UDP?

The UDP checksum is performed over the entire payload, *and* the other fields in the header, *and* some fields from the IP header. A pseudo-header is constructed from the IP header in order to perform the calculation (which is done over this pseudo-header, the UDP header and the payload). The reason the pseudo-header is included is to catch packets that have been routed to the wrong IP address.

If the checksum validation is enabled and it detected an invalid checksum, features like packet reassembling won't be processed.

36. How can the effect of jitter be compensated? What type of application require for this compensation?

Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components.

Jitter is defined as a variation in the delay of received packets. The sending side transmits \ packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant. This variation causes problems for audio playback at the receiving end. Playback may experience gaps while waiting for the arrival of variable delayed packets.

When a router receives an audio stream for VoIP, it must compensate for any jitter that it detects. The playout delay buffer mechanism handles this function. Playout delay is the amount of time that elapses between the time a voice packet is received at the jitter buffer on the DSP and the time a voice packet is played out to the codec.

The playout delay buffer must buffer these packets and then play them out in a steady Stream to the DSPs. The DSPs then convert the packets back into an analog audio stream. The play out delay buffer is also referred to as the dejitter buffer.

37. What is meant by PORT or MAILBOX related with UDP?

Form of address used to identify the target process:

Process can directly identify each other with an OS-assigned process ID(pid) More commonly-processes indirectly identify each other using a port or mailbox Source sends a message to a port and destination receives the message from the port UDP port is 16 bits, so there are 64K possible ports- not enough for all Internet hosts Process is identified as a port on a particular host – a (port, host) pair.

To send a message the process learns the port in the following way:

A client initiates a message exchange with a server process. The server knows the client’s port (contained in message header and can reply to it. Server accepts messages at a well known port.

Examples: DNS at port 53, mail at port 25

38. List out the various features of sliding window protocol.

The key feature of the sliding window protocol is that it permits pipelined communication. In contrast, with a simple stop-and-wait protocol, the sender waits for an acknowledgment after transmitting every frame. As a result, there is at most a single outstanding frame on the channel at any given time, which may be far less than the channel's capacity. For maximum throughput, the amount of data in transit at any given time should be equal to (channel bandwidth) X (channel delay).

39. What is the function of a router?

- Connect network segment together
- Router forwards the packet to the right path

40. What is the advantage of using UDP over TCP?

- UDP can send data in a faster way than TCP
- UDP is suitable for sending multicasting and multimedia applications

41. What is the difference between congestion control and flow control? Nov 2015 ,Nov/Dec 2017

Congestion control

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

Flow control

The amount of data flowed from source to destination should be restricted. The source can send one byte at a time, but it will take long time to transmit n bytes

42. List the mechanisms used in TCP congestion control mechanism

- Additive Increase/Multiplicative Decrease
- Slow Start
- Fast Retransmit and Fast Recovery

43. List the mechanisms used in TCP congestion avoidance

- DEC bit
- RED(Random Early Detection)
- Source-based Congestion Avoidance

44. Define DEC bit

Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur. This notification is implemented by setting a binary congestion bit in the packets that flow through the router, hence the name *DEC bit*.

45. What is meant by Source-Based Congestion Avoidance?

The general idea of these techniques is to watch for some sign from the network that some router's queue is building up and that congestion will happen soon if nothing is done about it

46. List the approaches to QoS support or what are the approaches used to provide range of Quality of services Nov/Dec 2017

***Fine-grained* approaches**, which provide QoS to individual applications or flows
***Coarse-grained* approaches,** which provide QoS to large classes of data or aggregated traffic

47. List the types of application requirements in QoS

- Real-time
- Non-real-time

48. List some of the Quality of service parameters of transport layer (May 2015)

- Reliability
- Delay
- Jitter
- Bandwidth

49. How does transport layer perform duplication control? (May 2015)

Duplication can be controlled by the use of sequence number & acknowledgment number

50. What do you mean by slow start in TCP congestion? (May 2016)

The sender starts with a very slow rate of transmission but increases the rate rapidly to reach a threshold

51. List the different phases used in TCP connection

- ✓ Connection establishment and Data transfer
- ✓ Connection termination

52. List out the advantages of connection oriented services over connectionless services. (APR 2017)

Advantage of connection oriented:

(i) In connection oriented virtual circuit,buffers can be reversed in advance
(ii) Sequencing can be guaranteed
(iii)Short-headers can be used
(iv)Troubles caused by delayed duplicate packets can be avoided

Advantage of connectionless:

(i) It can be used over subnets that do not use virtual circuit inside

(ii) No circuit setup time required
(iii) It is higher robust in the face of router failure
(iv) It is best for connectionless transport protocol because it does not impose unnecessary overhead

53. How do fast retransmit mechanism of TCP works. (APR 2017)

The transmission rate will be increases with slow start algorithm until either a loss is detected, or the receiver's advertised window (rwnd) is limiting factor, or when the slow start threshold (ssthresh) is reached.

<u>16 MARKS</u>

1. Discuss in detail about transport layer & its services

INTRODUCTION

The transport layer is located between the application layer and the network layer. It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host. Communication is provided using a logical connection, which means that the two application layers, which can be located in different parts of the globe, assume that there is an imaginary direct connection through which they can send and receive messages.

Transport-Layer Services

Each protocol provides a different type of service and should be used appropriately.

UDP

UDP is an unreliable connectionless transport-layer protocol used for its simplicity and efficiency in applications where error control can be provided by the application-layer process.

TCP

TCP is a reliable connection-oriented protocol that can be used in any application where reliability is important.

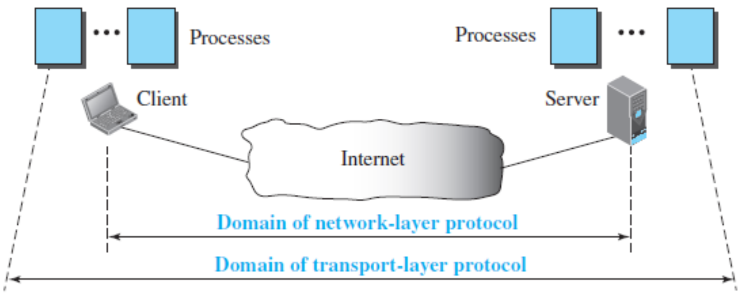
SCTP

SCTP is a new transport-layer protocol that combines the features of UDP and TCP.

Process-to-Process Communication

The first duty of a transport-layer protocol is to provide **process-to-process communication.** A process is an application-layer entity (running program) that uses the services of the transport layer. A transport-layer protocol is responsible for delivery of the message to the appropriate process

Figure 23.2 *Network layer versus transport layer*


Processes
Processes
Client
Server
Internet
Domain of network-layer protocol
Domain of transport-layer protocol

Addressing: Port Numbers

Although there are a few ways to achieve process-to-process communication, the most common is through the **client-server paradigm**. A process on the local host, called a *client*, needs services from a process usually on the remote host, called a *server*.

The local host and the remote host are defined using IP addresses. To define the processes, we need second identifiers, called ***port numbers.*** The client program defines itself with a port number, called the ***ephemeral port number.*** The word *ephemeral* means "short-lived" and is used because the life of a client is normally short. An ephemeral port number is recommended to be greater than 1023 for some client/server programs to work properly.

Figure 23.3 *Port numbers*

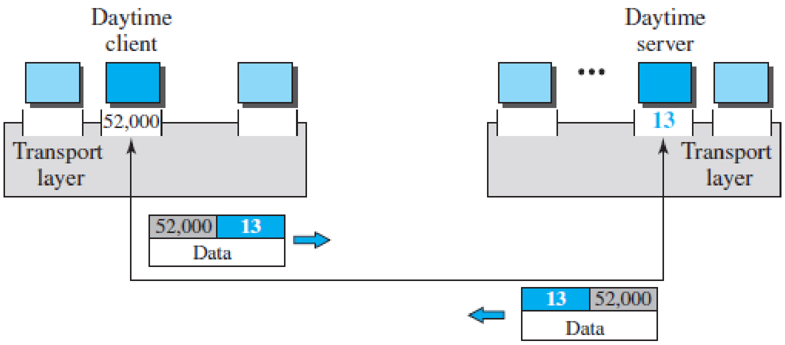
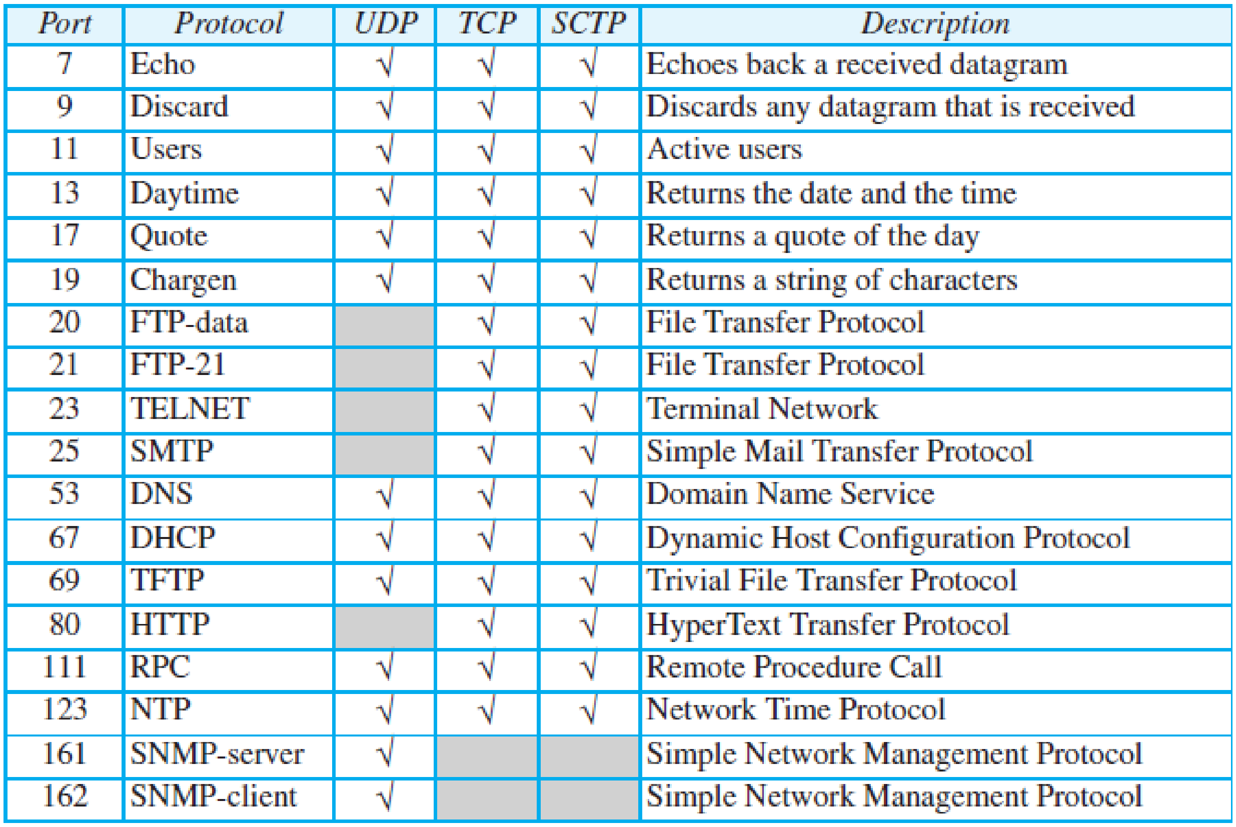


Table 24.1 *Some well-known ports used with UDP and TCP*



Port	*Protocol*	*UDP*	*TCP*	*SCTP*	*Description*
7	Echo	√	√	√	Echoes back a received datagram
9	Discard	√	√	√	Discards any datagram that is received
11	Users	√	√	√	Active users
13	Daytime	√	√	√	Returns the date and the time
17	Quote	√	√	√	Returns a quote of the day
19	Chargen	√	√	√	Returns a string of characters
20	FTP-data		√	√	File Transfer Protocol
21	FTP-21		√	√	File Transfer Protocol
23	TELNET		√	√	Terminal Network
25	SMTP		√	√	Simple Mail Transfer Protocol
53	DNS	√	√	√	Domain Name Service
67	DHCP	√	√	√	Dynamic Host Configuration Protocol
69	TFTP	√	√	√	Trivial File Transfer Protocol
80	HTTP		√	√	HyperText Transfer Protocol
111	RPC	√	√	√	Remote Procedure Call
123	NTP	√	√	√	Network Time Protocol
161	SNMP-server	√			Simple Network Management Protocol
162	SNMP-client	√			Simple Network Management Protocol

ICANN Ranges

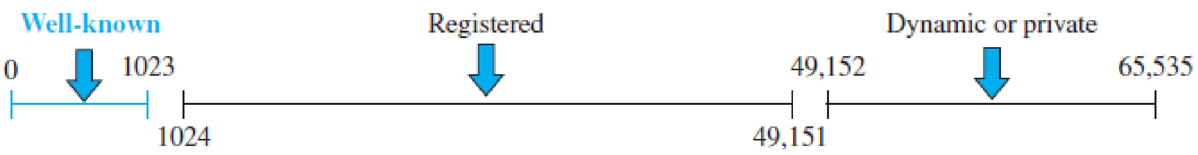
ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private), as shown in Figure 23.5

❑ ***Well-known ports.*** The ports ranging from 0 to 1023 are assigned and controlled by ICANN. These are the well-known ports.

❑ ***Registered ports.*** The ports ranging from 1024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

❑***Dynamic ports.*** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.

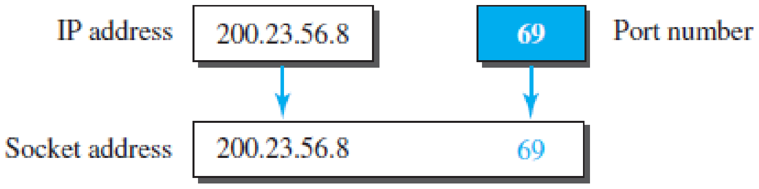
Figure 23.5 *ICANN ranges*



Socket Addresses

A transport-layer protocol in the TCP suite needs both the IP address and the port number, at each end, to make a connection. The combination of an IP address and a port number is called a ***socket address.*** The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely

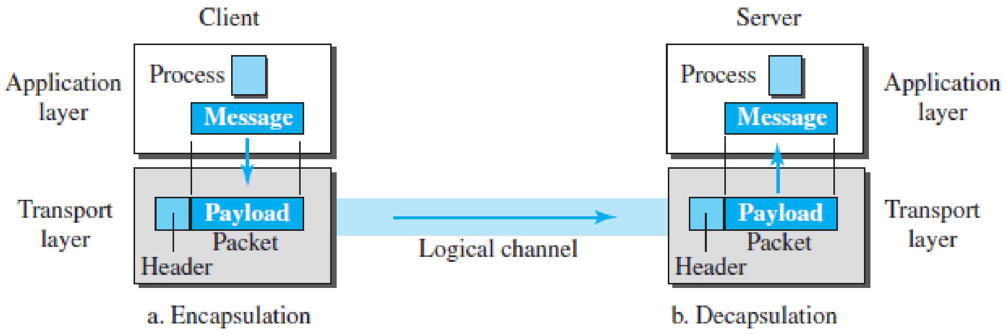
Figure 23.6 *Socket address*



Encapsulation and Decapsulation

To send a message from one process to another, the transport-layer protocol encapsulates and decapsulates messages.

Figure 23.7 *Encapsulation and decapsulation*



Multiplexing and Demultiplexing

Whenever an entity accepts items from more than one source, this is referred to as ***multiplexing*** (many to one); whenever an entity delivers items to more than one source, this is referred to as ***demultiplexing*** (one to many). The transport layer at the source performs multiplexing; the transport layer at the destination performs demultiplexing

Flow Control

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates

Error Control

Error control at the transport layer is responsible for

1. Detecting and discarding corrupted packets.
2. Keeping track of lost and discarded packets and resending them.
3. Recognizing duplicate packets and discarding them.
4. Buffering out-of-order packets until the missing packets arrive.

Congestion Control

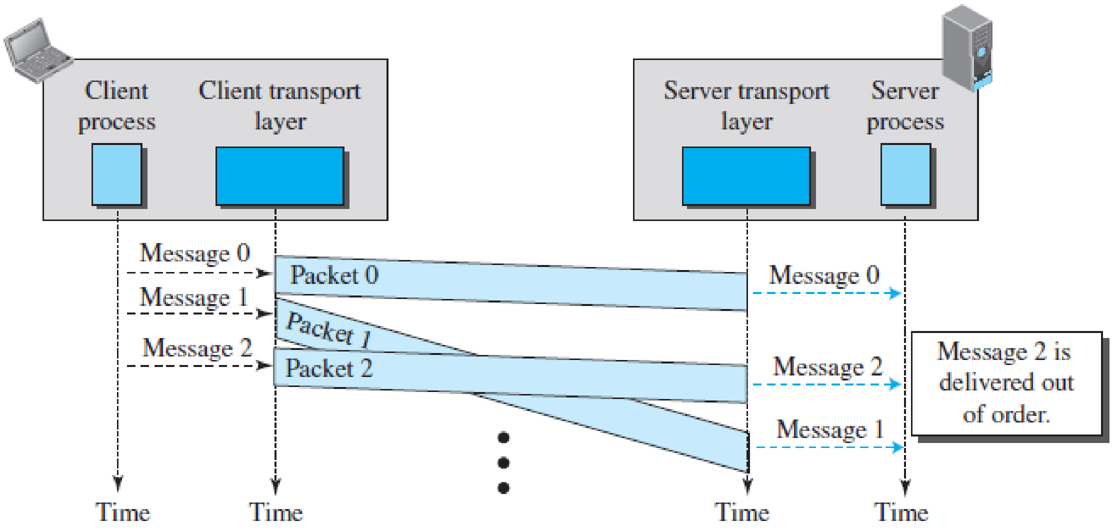
Congestion control refers to the mechanisms and techniques that control the congestion and keep the load below the capacity

Connectionless and Connection-Oriented Protocols

Connectionless Service

In a connectionless service, the source process (application program) needs to divide it message into chunks of data of the size acceptable by the transport layer and deliver them to the transport layer one by one

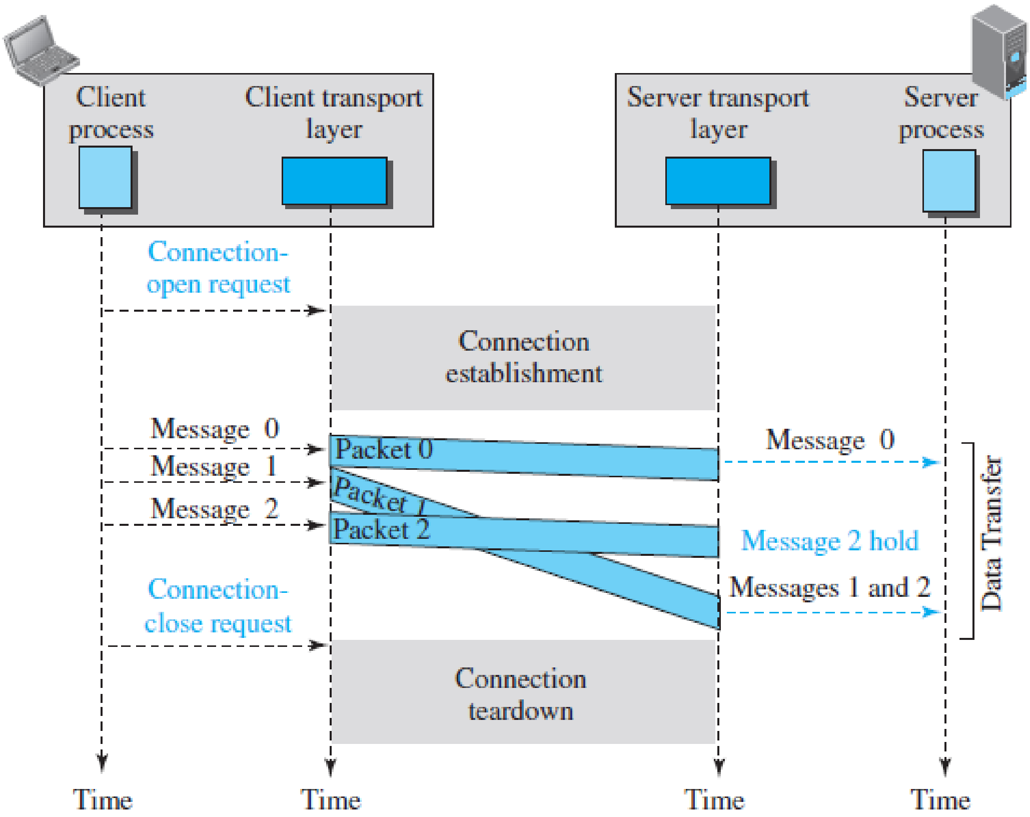
Figure 23.14 *Connectionless service*



Connection-Oriented Service

In a connection-oriented service, the client and the server first need to establish a logical connection between themselves. The data exchange can only happen after the connection establishment. After data exchange, the connection needs to be torn down

Figure 23.15 *Connection-oriented service*



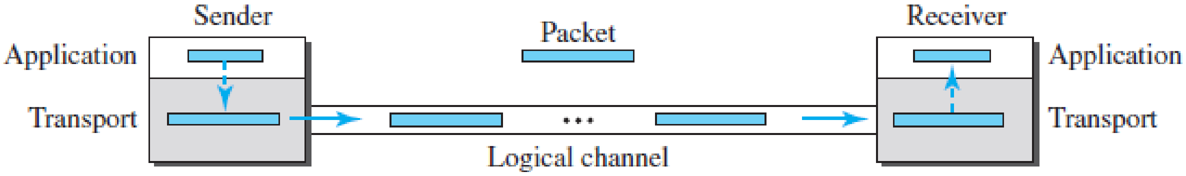
2. List & explain the protocols used in transport layer.

- Simple Protocol
- Stop-and-Wait Protocol
- Go-Back-*N* Protocol (GBN)
- Selective-Repeat Protocol
- Bidirectional Protocols: Piggybacking

Simple Protocol

Our first protocol is a simple connectionless protocol with neither flow nor error control. We assume that the receiver can immediately handle any packet it receives. In other words, the receiver can never be overwhelmed with incoming packets.

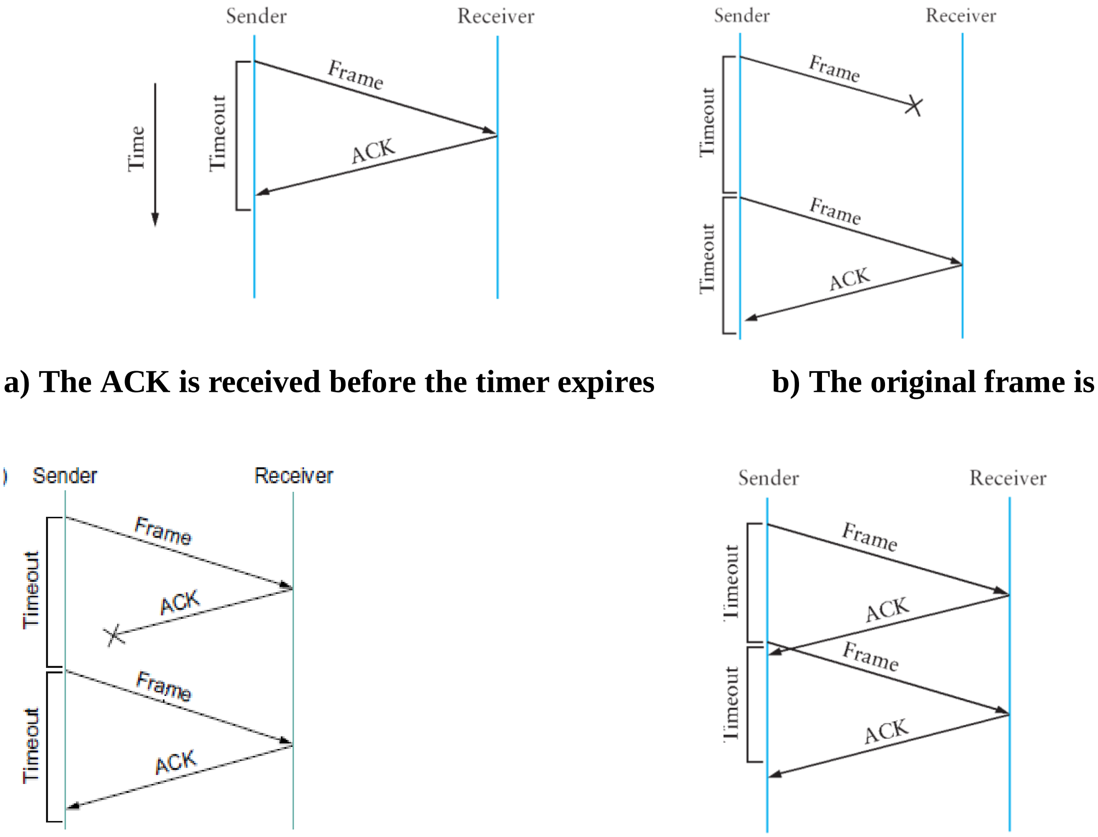
Figure 23.17 *Simple protocol*



Stop and Wait Protocol

➢ After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.

➢ If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.



a) The ACK is received before the timer expires

b) The original frame is lost

c) The ACK is lost

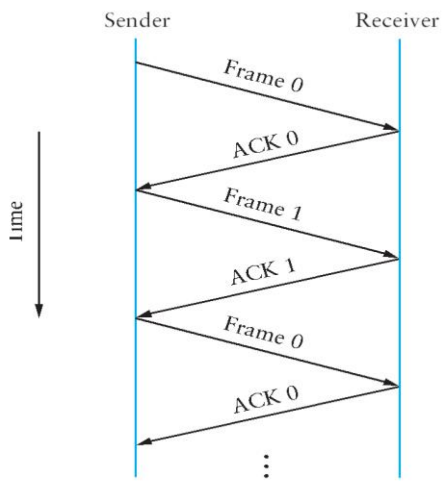
d)The timeout fires too soon

Fig: illustrates four different scenarios that result from this basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.

➢ In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..

➢ Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.

➢ This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively.



- ➢ The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

Sliding Window Protocol

- ➢ The sender can transmit several frames before needing an acknowledgement.
- ➢ Frames can be sent one right after another meaning that the link can carry several frames at once and it s capacity can be used efficiently.
- ➢ The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames
- ➢ Sliding Window refers to imaginary boxes at both the sender and the receiver.
- ➢ Window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- ➢ Frames are numbered modulo-n which means they are numbered from o to n-1
- ➢ For eg. If n=8 the frames are numbered 0,1,2,3,4,5,6,7. i.e the size of the window is n -1.
- ➢ When the receiver sends ACK it includes the number of the next frame it expects to receive.
- ➢ When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

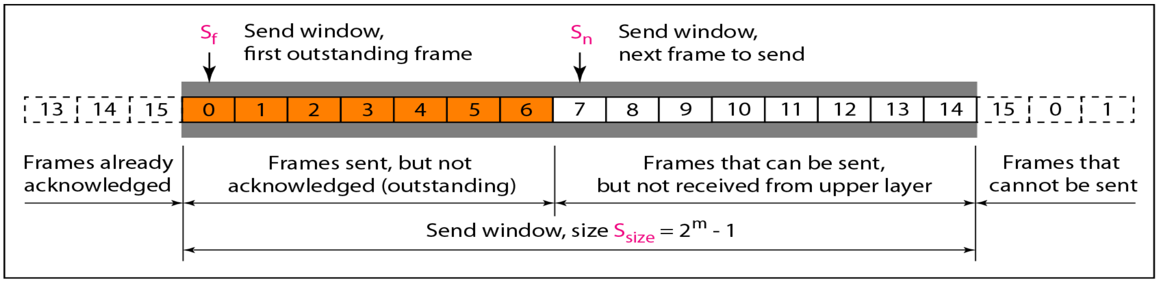
There are two methods to retransmit the lost frames

- ➢ GO-Back N
- ➢ Selective Repeat

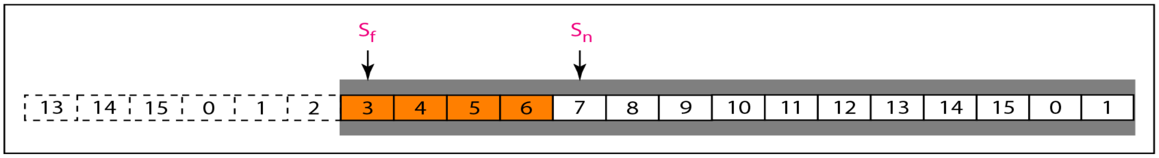
Go – Back N Protocol

Sender Window

- ➢ At the beginning of transmission, the sender window contains n-1 frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window
- ➢ If size of window is W if three frames have been transmitted since the last acknowledgement then the number of frames left in the window is w -3.
- ➢ Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by that ACK.


S_f
Send window, first outstanding frame
S_n
Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size $S_{size} = 2^m - 1$

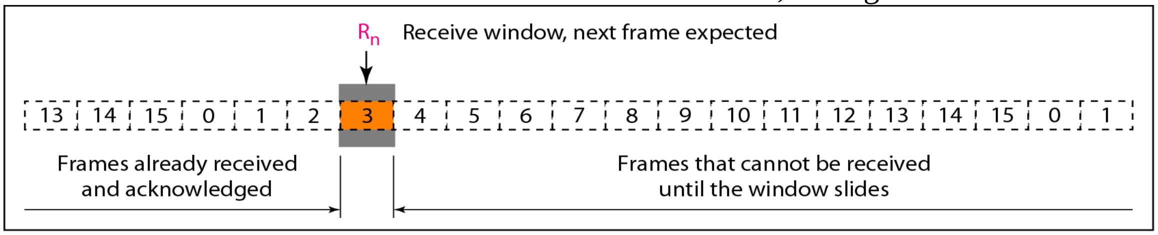
a. Send window before sliding



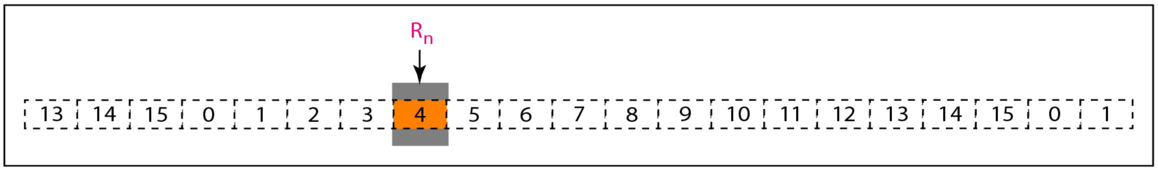
b. Send window after sliding

Receiver Window

- ➢ The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.
- ➢ The window slides when a correct frame has arrived, sliding occurs one slot at a time.


R_n
Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received and acknowledged
Frames that cannot be received until the window slides

a. Receive window

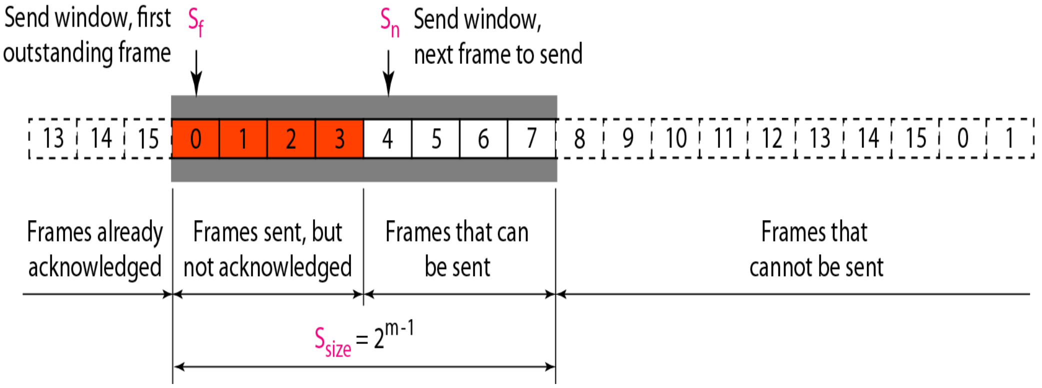


b. Window after sliding

When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4,5, and 6 again. That is why the protocol is called *Go-Back-N*.

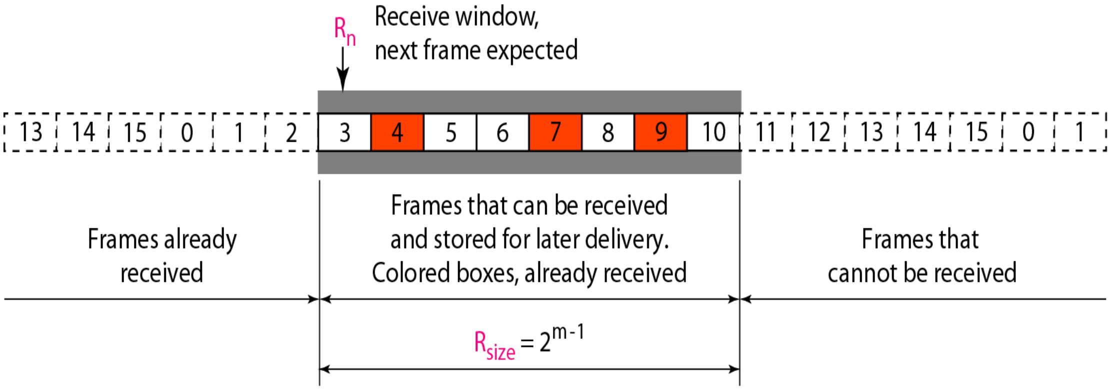
Selective Repeat Protocol

Sender Window


Send window, first outstanding frame
S_f
S_n
Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged
Frames that can be sent
Frames that cannot be sent
$S_{size} = 2^{m-1}$

Receiver window

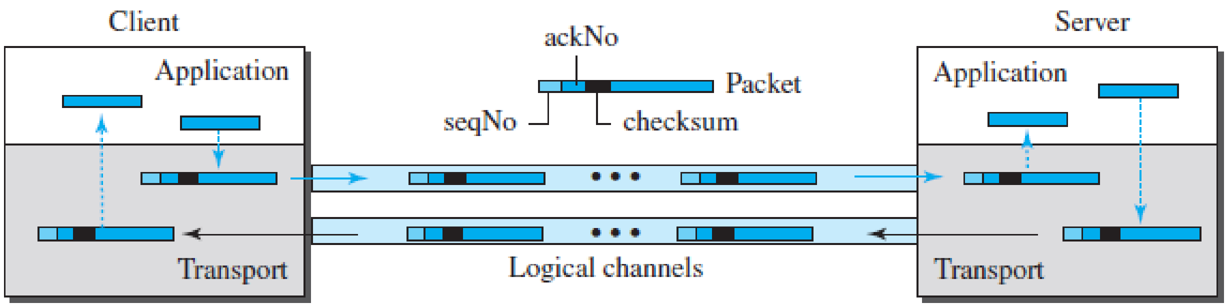
- The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer.
- Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered.
- If any frame lost, sender has to retransmit only that lost frames.


R_n
Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received
Frames that can be received and stored for later delivery. Colored boxes, already received
Frames that cannot be received
$R_{size} = 2^{m-1}$

Bidirectional Protocols: Piggybacking

The four protocols we discussed earlier in this section are all unidirectional: data packets flow in only one direction and acknowledgments travel in the other direction. In real life, data packets are normally flowing in both directions: from client to server and from server to client. This means that acknowledgments also need to flow in both directions. A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols. When a packet is carrying data from A to B, it can also carry acknowledgment feedback about arrived packets from B; when a packet is carrying data from B to A, it can also carry acknowledgment feedback about the arrived packets from A.

Figure 23.37 *Design of piggybacking in Go-Back-N*



3. Explain the working of USER DATAGRAM PROTOCOL (UDP) or Simple Demultiplexer (May 2016)

The UDP is called a connection less, unreliable transport protocol. The purpose of UDP is to break up a stream of data into datagram, add a source and destination port information, a length and a checksum. It is the receiving application's responsibility to detect and recover lost or damaged packets, as UDP doesn't take care of this.

Advantages:

- It is a very simple protocol using a minimum of overhead.
- If a process wants to send a small message and doesn't care much about reliability, it can use UDP.
- It is a convenient protocol for multimedia and multicasting applications.
- Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP.

Basic Properties of UDP (services):

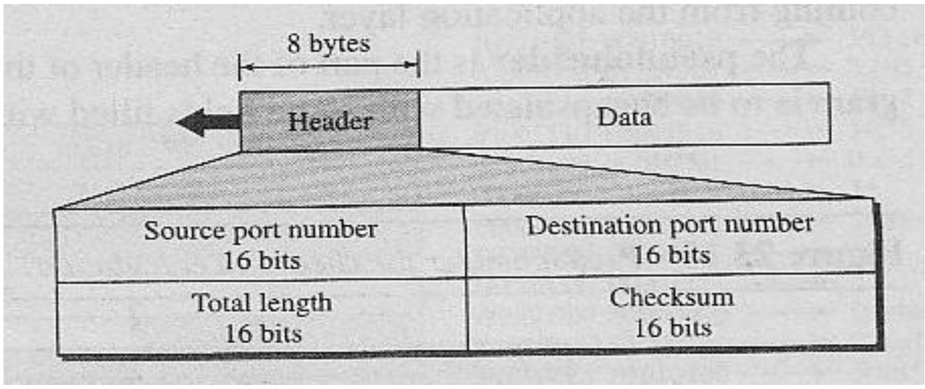
- UDP is a connectionless transport protocol.
  - A UDP application sends messages without establishing and then closing a connection.
  - UDP has a smaller overhead then TCP, especially when the total size of the messages is small.
- UDP does not guarantee reliable data delivery.
  - UDP messages can be lost or duplicated, or they may arrive out of order; and they can arrive faster than the receiver can process them.
  - The application programmers using UDP have to consider and tackle these issues themselves.
  - Not buffered -- UDP accepts data and transmits immediately (no buffering before transmission)
  - Full duplex -- concurrent transfers can take place in both directions
- UDP has no mechanism for flow control.
- Multiplexing and Demultiplexing
  - This is many to one relationship used in sender side.
  - The protocol accepts messages from different processes, differentiated by their assigned port numbers.
  - Demultiplexing is one to many relationship used in receiver side.
- Encapsulation and Decapsulation
  - To send a message from one processes to another, the UDP protocol encapsulate and decapsulate messages in an IP datagram
  - Encapsulate each UDP message in an IP datagram, and use IP to deliver this datagram across the internet.

UDP Message Format

User Datagram:

- UDP packets called user datagram which has a fixed size header of 8 bytes.

Format of User Datagram:



User datagram has the following fields.

- **Source Port Number**

  The source port number used by the processes running on the source host (local computer). It is 16 bits long, which means that the port number can range from 0 to 65535. If the source host is the client, the port number requested by the processes and chosen by the UDP software running on the source host.

- **Destination Port Number**

  This is the port number used by the processes running on the destination host. It is also 16 bits long. The Destination port is usually a 'well known port number' such as 69 for trivial file transfer protocol, or 53 for DNS. These port numbers allow the remote machine to recognize a request for a particular type of service. If the destination host is a client, the server copies the port number it has received in the request packet.

- **Length**

  This is a 16 bits field that defines the total length of the user data gram, header plus data. The 16 bits can defined a total length of 0 to 65535 bytes.

- **Checksum**

  This field is used to detect errors over the entire user datagram. The calculation of checksum and its inclusion in the user datagram are optional.

Process communication in UDP

The next issue is how a process learns the port for the process to which it wants to send the message.

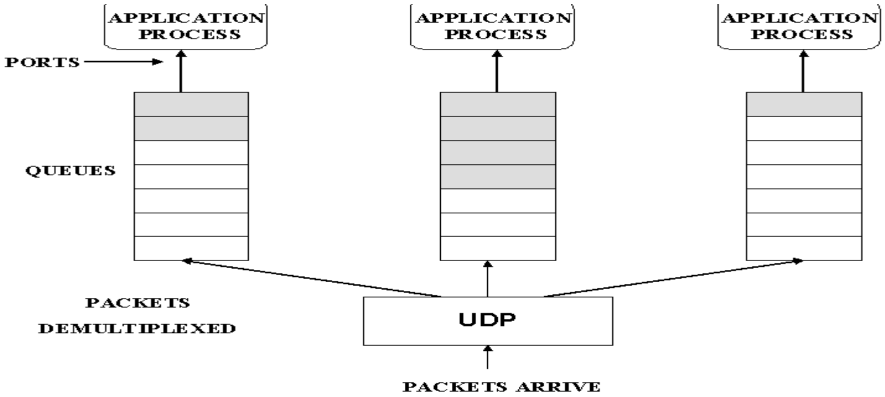
Typically a client process initiates a message exchange with a server process. Once a client has contacted a server, the server knows the client’s port (it was contained in the message header) and can reply to it.

The real problem, therefore, is how the client learns the server’s port in the first place. A common approach is for the server to accept messages at a well known port.

That is, each server receives its messages at some fixed port that is widely published, much like the emergency telephone service available at the well-known number 911.

In the Internet, for example, the domain name server (DNS) receives messages at well-known port 53 on each host, the mail service listens of messages at port 25,and the Unix talk program accepts messages at well known port 517,and so on.

UDP Message queue



This mapping is published periodically in an RFC and is available on the most Unix systems in file /etc/services. Sometimes a well-known port to agree on some other port that they will use for subsequent communication leaving the well-known port free for other clients.

A port is purely an abstraction. Exactly how it is implemented differs from system to system, or more precisely, from OS to OS.

For example, the socket API is an example implementation of ports. Typically, a port is implemented by a message queue.

When a message arrives, the protocol l(eg.UDP) appends the message to the end of the queue. Should the queue be full, the message is discarded.

There is no flow-control mechanism that tells the sender to slow down. When an application process wants to receive a message, one is removed from the front of the queue. If the queue is empty, the process blocks until a message becomes available.

Uses or applications of UDP

- UDP is used for process with simple request-response communication with little concern for and error control.
- UDP is suitable for a process with internal flow and error control mechanism.
- UDP is suitable for multicasting. Multicasting capabilities are embedded in UDP software but not in TCP software.
- UDP is used for some route updating protocols, such as routing information protocol (RIP).
- UDP is used for management processes such as SNMP.

4. Describe in detail about TCP segment (Header) format (NOV 2013, 2014)(May & Nov 2015) or Draw the format of TCP Packet header and explain each of its field and Specify the justification for having variable field length for the field in TCP header. Apr 2017

A Packet in TCP is called a segment. The below diagram shows the format of the segment.
The segment consists of a 20 to 60 byte header, followed by data from the application program.
The header is 20 bytes if there are no options and up to 60 bytes if it contains options.

- *__Header__*

– The header is composed of a 20-byte fixed part and an optional part with a variable length. The total size of the header (in 32-bit words) is specified in HLEN.

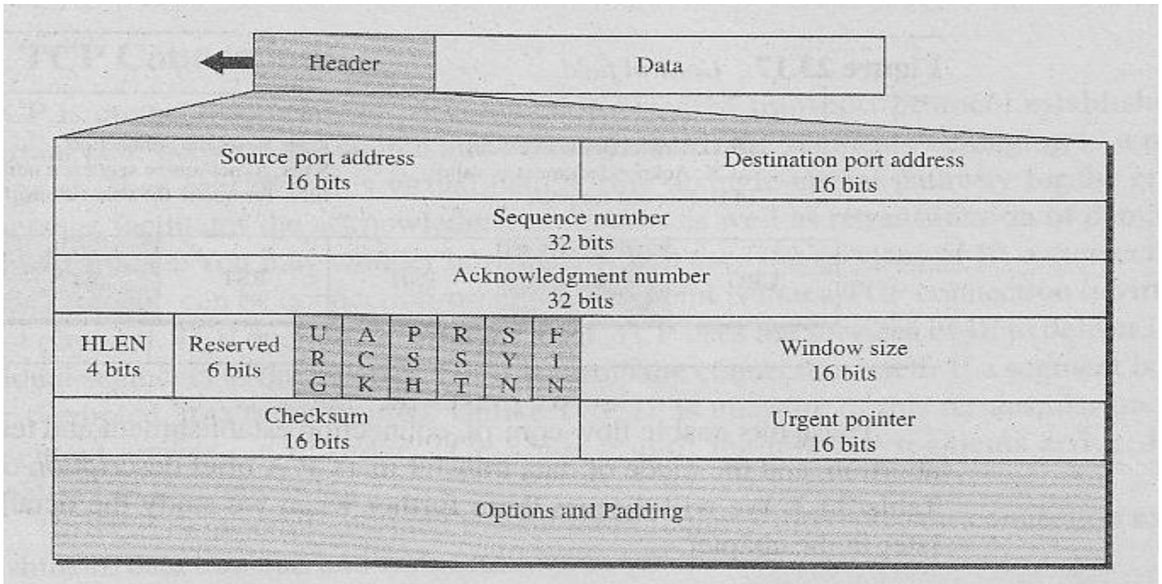
➢ <u>*Data -*</u> The data can have a variable size, which can be up to 65535 – 20 = 65515 bytes.

➢ <u>*Source port number (16 bits)*</u>

– The *SOURCE PORT* field identifies the *TCP process* which sent the datagram.

➢ <u>*Destination port number (16 bits)*</u>

The *DESTINATION PORT* field identifies the *TCP process* which is receiving the datagram



➢ <u>*Sequence number (32 bits*</u>)

– The *SEQUENCE NUMBER* field identifies the first byte of the outgoing data. The receiver uses this to re-order segments arriving out of order and to compute an acknowledgement number.

➢ <u>*Acknowledgement number (32 bits)*</u>

– Contains the next sequence number that the sender of the acknowledgement expects to receive which is the sequence number plus 1 (plus the number of bytes received in the last message). This number is used only if the ACK flag is on. The *ACKNOWLEDGEMENT NUMBER* field identifies the sequence number of the incoming data that is expected next.

➢ <u>*Header Length*</u>

– This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes.

➢ <u>*Reserved*</u>

– This is a 6-bit field reserved for future use.

➢ <u>*Code bits*</u>

– The *CODE BITS* (or *FLAGS*) field contains one or more 1-bit flags

– Control bits to indicate end of stream, acknowledgement field being valid, connection reset, urgent pointer field being valid, etc.

[CONTROL]: URG (1)-	Urgent Bit validates the Urgent Pointer field.
[CONTROL]: ACK (1)-	Acknowledge Bit, set if the Acknowledge Number field is being used.
[CONTROL]: PSH (1)-	Push Bit tells the sender that a higher throughput is required.
[CONTROL]: RST (1)-	Reset Bit resets the connection when there's conflicting sequence numbers.
[CONTROL]: SYN (1)-	Sequence Number Synchronization. Used in 3 types of segments: connection request, connection confirmations (with ACK) and confirmation termination (with FIN) in 3 types of segments: terminal request, terminal confirmation (with ACK) and acknowledgement of terminal confirmation (with ACK).
[CONTROL]: FIN (1)-	Used with SYN to confirm termination of connections

- *Window Size*(16 bit)
  - The *WINDOW* field identifies how much buffer space is available for incoming data.
  - During piggybacking, how much data a receiver is willing to accept.

Note: The process of sending data along with the acknowledgment is called piggybacking

- *Checksum*(16 bit)
  - The *CHECKSUM* field contains a simple checksum over the TCP segment header and data.
- *Urgent Pointer* (16 bit)
  - This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.
- *Options*
  - There can be up to 40 bytes of optional information in the TCP header.

5. Explain in detail about TCP connection establishment & termination (TCP Connection Management) (NOV 2013) (May & Nov 2015) Nov 2017

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgement process as well as retransmission of damaged or lost frames. TCP, which uses the services of IP, a connection-less protocol, can be connection-oriented. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted.

In TCP connection-oriented transmission requires two phases:

- ✓ Connection establishment and Data transfer
- ✓ Connection termination

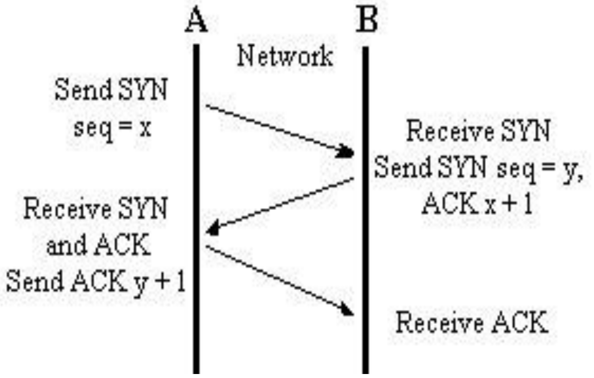
Connection establishment:

TCP transmits data in full-duplex mode. When two TCP’s in two machines or connected, they are able to send segments to each other simultaneously.

Three-way handshaking.

The connection establishment in TCP is called three way handshaking. The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open.

The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process. Each segment has the sequence number the acknowledgement number, the control flags, and the window size, if not empty.



The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. A SYN segment cannot carry data, but it consumes one sequence number.

2. The server sends the second segment, a SYN + ACK segment, with 2 flag bits set: SYN and ACK. This segment has a dual pupose. It is a SYN segment for communication in the other direction and serves as the acknowledgement for the SYN segment. It consumes one sequence number.

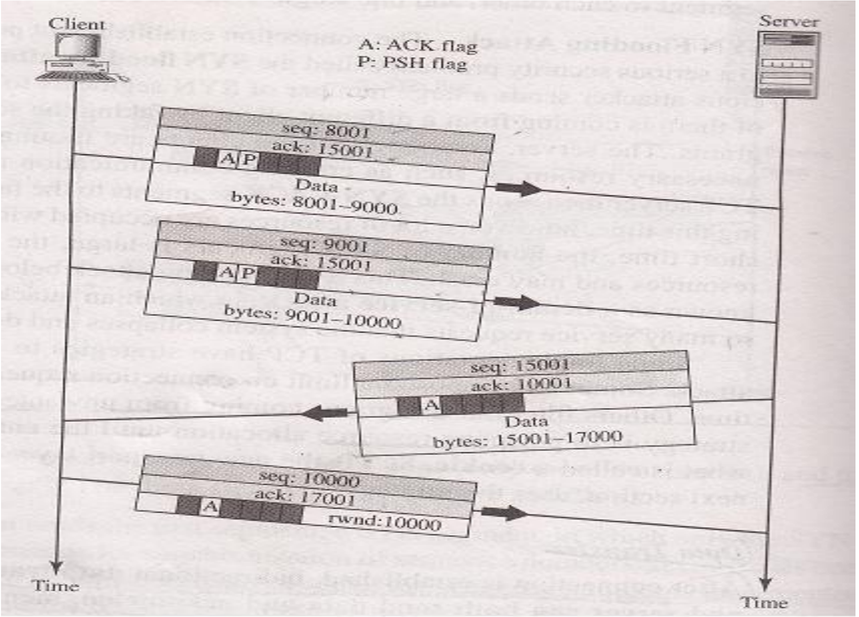
3. The client sends the third segment. This is just an ACK segment. It acknowdeges the receipt of the second segmant with the ACK flag and acknowledgment number field.

Data Transfer

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgements.

The below figure shows an example. In this example, after connection is established, the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment. The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgement because there are no more data to be sent.

The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.



Pushing Data: The sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

The application program at the sending site can request a push operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

TCP Connection Release (or) Connection Termination

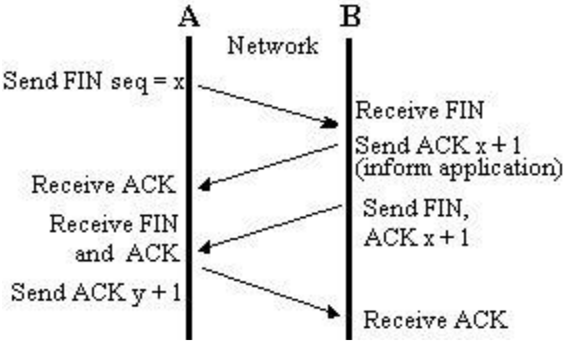
Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

Three-way handshaking

In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. The FIN segment consumes one sequence number if it does not carry data.

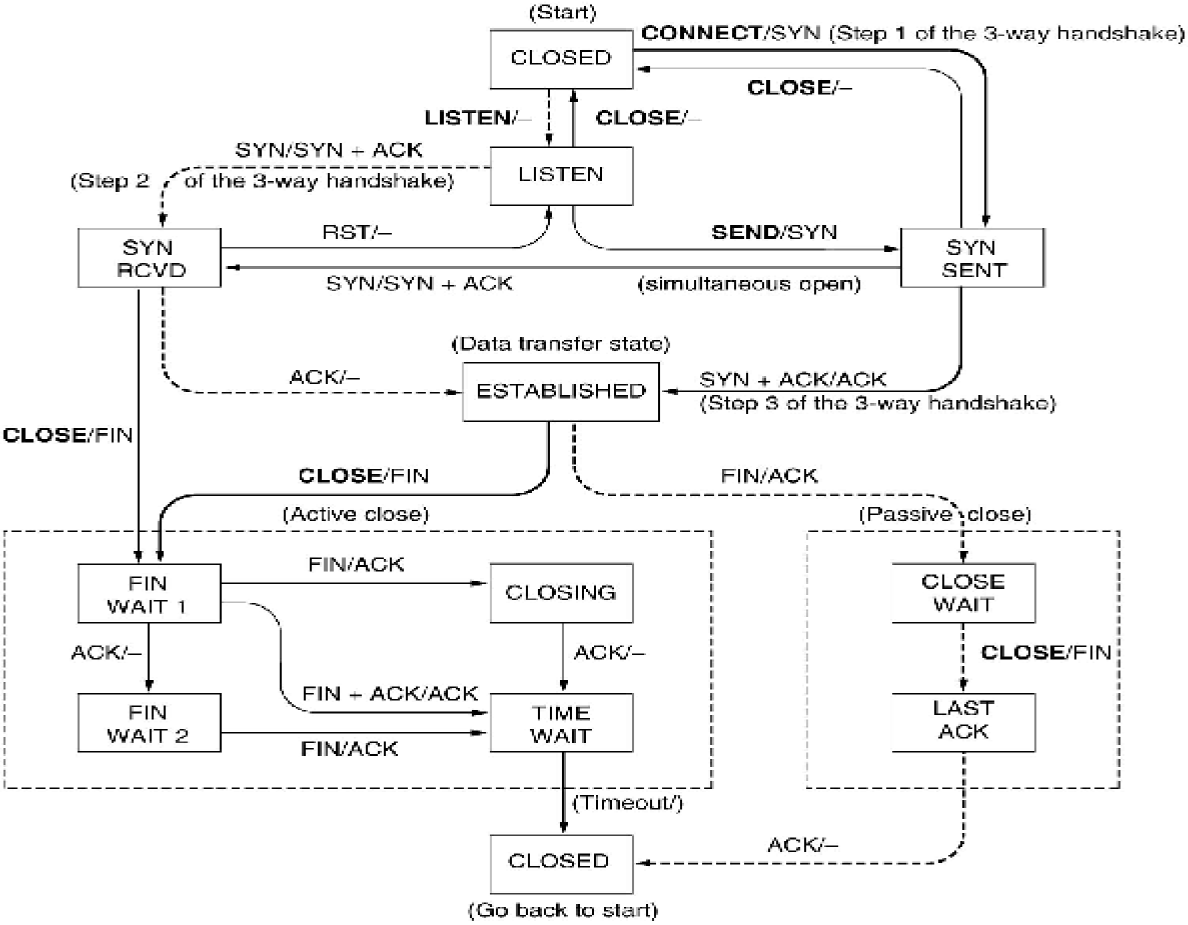
1. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN + ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. The FIN + ACK segment consumes one sequence number if it does not carry data.

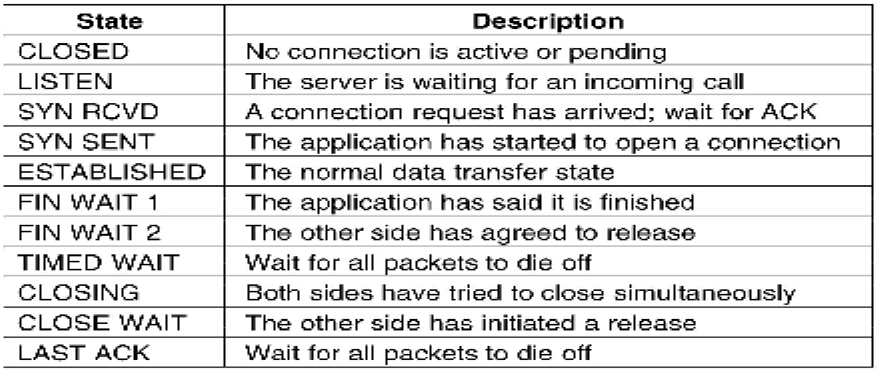
2. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgement number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence number.



TCP Connection Management (State transition diagram) (NOV/DEC 2013)

The steps to manage a TCP connection can be represented in a finite state machine with the eleven states listed in Figure





State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

Client Diagram:

- The client TCP starts in the CLOSED state.
- While in this state, the client TCP can receive an active open request from the client application program. It sends a SYN segment to the server TCP and goes to the SYN-SENT state.
- While in this state, the client TCP can receive a SYN + ACK segment from other TCP. It sends an ACK segment to the other TCP and goes to the ESTABLISHED state. This is the data transfer state. The client remains in this state as long as it is sending and receiving data.
- While in this state, the client TCP can receive a close request from the client application program. It sends a FIN segment to the other TCP and goes to the FIN-WAIT1 state.
- While in this state, the client TCP waits to receive an ACK from the server TCP. When ACK is received, it goes to the FIN-WAIT2 state. Now the connection is closed in one direction.
- The client remains in this state, waiting for the server to close the connection. If it receives a FIN segment, it sends an ACK segment and goes to the TIME-WAIT state.
- When the client is in this state, it starts a timer and waits until this timer goes off. After the time-out, the client goes to the CLOSED state, where it began.

Server Diagram:

- The server TCP starts in the CLOSED state.
- While in this state, the server TCP can receive an open request from the server application program, it goes to the LISTEN state.
- While in this state, the server TCP can receive a SYN segment. It sends a SYN + ACK segment to the client and goes to the SYN-RCVD state.
- While in this state, the server TCP receives an ACK and goes to ESTABLISHED state. This is the data transfer state. The server remains in this state as long as it is receiving and sending data.
- While in this state, the server TCP can receive a FIN segment from the client. It can send an ACK and goes to the CLOSE-WAIT state.
- While in this state, the server waits until it receives a close request from the server program. It then sends a FIN segment and goes to LAST-ACK state.
- While in this state, the server waits for the last ACK segment and goes to the CLOSED state.

6. Discuss TCP Services & Features

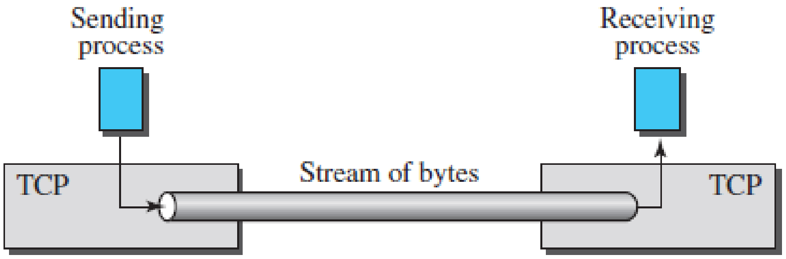
Transmission Control Protocol (TCP) is a connection-oriented, reliable protocol.
TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service

TCP Services

Process-to-Process Communication
As with UDP, TCP provides process-to-process communication using port numbers

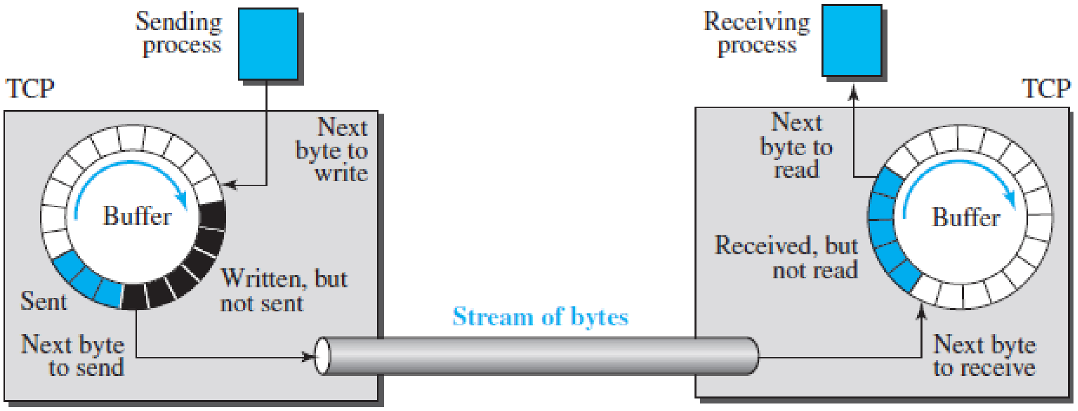
Stream Delivery Service

Figure 24.4 *Stream delivery*



Sending and Receiving Buffers

Figure 24.5 *Sending and receiving buffers*



Full-Duplex Communication
TCP offers *full-duplex service*, where data can flow in both directions at the same time.
Each TCP endpoint then has its own sending and receiving buffer, and segments move in both directions

Multiplexing and Demultiplexing
Like UDP, TCP performs multiplexing at the sender and demultiplexing at the receiver.

However, since TCP is a connection-oriented protocol, a connection needs to be established for each pair of processes.

Connection-Oriented Service

TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send to and receive data from another process at site B, the following three phases occur:
1. The two TCP's establish a logical connection between them.
2. Data are exchanged in both directions.
3. The connection is terminated.

Reliable Service

TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

TCP Features

- *Numbering System*
- *Byte Number*
- *Sequence Number*
- *Acknowledgment Number*

Windows in TCP:

Send Window

The sender maintains three variables:

- ✓ The *send window size*, denoted SWS, gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
- ✓ LAR denotes the sequence number of the *last acknowledgment received*; and
- ✓ LFS denotes the sequence number of the *last frame sent*.

The sender also maintains the following invariant:

$$\boxed{\mathbf{LFS - LAR \leq SWS}}$$

When an acknowledgment arrives, the sender moves LAR to the right, thereby allowing the sender to transmit another frame. Also, the sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received. Notice that the sender has to be willing to buffer up to SWS frames since it must be prepared to retransmit them until they are acknowledged.

Receive Window

The receiver maintains the following three variables:

- ✓ The *receive window size*, denoted RWS, gives the upper bound on the number of outof- order frames that the receiver is willing to accept;
- ✓ LAF denotes the sequence number of the *largest acceptable frame*; and
- ✓ LFR denotes the sequence number of the *last frame received.*

The receiver also maintains the following invariant

$$\mathbf{LAF - LFR \leq RWS}$$

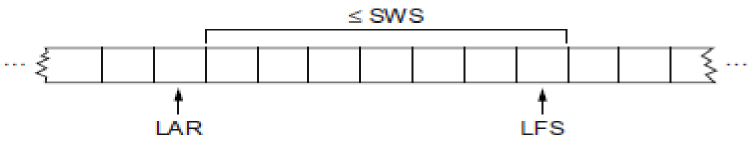


FIGURE 2.20 Sliding window on sender.

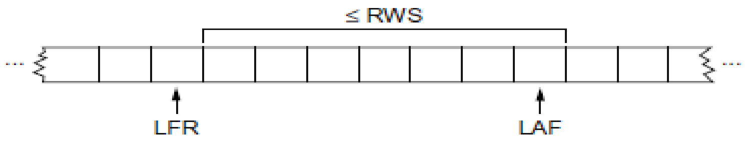


FIGURE 2.21 Sliding window on receiver.

When a frame with sequence number SeqNum arrives, the receiver takes the following action. If SeqNum ≤ LFR or SeqNum > LAF, then the frame is outside the receiver's window and it is discarded. If LFR < SeqNum ≤ LAF, then the frame is within the receiver's window and it is accepted.
Now the receiver needs to decide whether or not to send an ACK. Let SeqNumToAck denote the largest sequence number not yet acknowledged, such that all frames with sequence numbers less than or equal to SeqNumToAck have been received.
The receiver acknowledges the receipt of SeqNumToAck, even if higher numbered packets have been received. This acknowledgment is said to be cumulative. It then sets LFR = SeqNumToAck and adjusts LAF = LFR+RWS.

7. Explain in detail about TCP flow control OR TCP Adaptive flow control (NOV/DEC 2013, 2014) APR 2017

TCP uses a sliding *window* mechanism to control the flow of data. When a connection is established, each end of the connection allocates a buffer to hold incoming data, and sends the size of the buffer to the other end. As data arrives, the receiver sends acknowledgements together with the amount of buffer space available called a *window advertisement.*

Sliding window algorithm serves several purposes.

1. It guarantees the reliable delivery of data
2. It ensures that data is delivered in order.
3. It enforces flow control between, the sender and the receiver.

Reliable and Ordered Delivery

To see how the sending and receiving sides of TCP interact with each other to implement reliable and ordered delivery, consider the situation illustrated in Figure 5.8. TCP on the sending side maintains a send buffer. This buffer is used to store data that has been sent but not yet acknowledged, as well as data that has been written by the sending application but not transmitted. On the receiving side, TCP maintains a receive buffer. This buffer holds data that arrives out of order, as well as data that is in the correct order (i.e., there are no missing bytes earlier in the stream) but that the application process has not yet had the chance to read.

To make the following discussion simpler to follow, we initially ignore the fact that both the buffers and the sequence numbers are of some finite size and hence will eventually wrap around. Also, we do not distinguish between a pointer into a buffer where a particular byte of data is stored and the sequence number for that byte

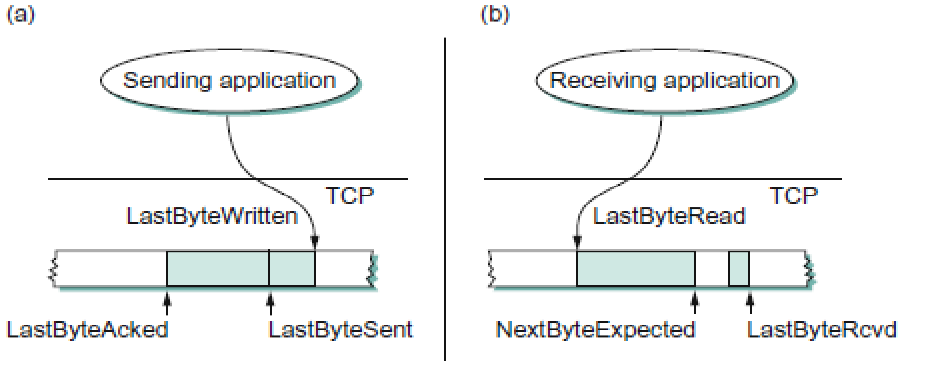


FIGURE 5.8 Relationship between TCP send buffer (a) and receive buffer (b).

Looking first at the sending side, three pointers are maintained into the send buffer, each with an obvious meaning: LastByteAcked, LastByteSent, and LastByteWritten. Clearly

LastByteAcked ≤ LastByteSent

since the receiver cannot have acknowledged a byte that has not yet been sent, and

LastByteSent ≤ LastByteWritten

since TCP cannot send a byte that the application process has not yet written. Also note that none of the bytes to the left of LastByteAcked need to be saved in the buffer because they have already been acknowledged, and none of the bytes to the right of LastByteWritten need to be buffered because they have not yet been generated.

A similar set of pointers (sequence numbers) are maintained on the receiving side: LastByteRead, NextByteExpected, and LastByteRcvd. The inequalities are a little less intuitive, however, because of the problem of out-of-order delivery. The first relationship

LastByteRead < NextByteExpected

is true because a byte cannot be read by the application until it is received *and* all preceding bytes have also been received. NextByteExpected points to the byte immediately after the latest byte to meet this criterion. Second,

NextByteExpected ≤ LastByteRcvd+1

since, if data has arrived in order, NextByteExpected points to the byte after LastByteRcvd, whereas if data has arrived out of order, then NextByteExpected points to the start of the first gap in the data, as in Figure 5.8.Note that bytes to the left of LastByteRead need not be buffered because they have already been read by the local application process, and bytes to the right of LastByteRcvd need not be buffered because they have not yet arrived.

Flow Control

Recall that in a sliding window protocol, the size of the window sets the amount of data that can be sent without waiting for acknowledgment from the receiver. Thus, the receiver throttles the sender by advertising a window that is no larger than the amount of data that it can buffer. Observe that TCP on the receive side must keep

$$\text{LastByteRcvd}-\text{LastByteRead} \leq \text{MaxRcvBuffer}$$

to avoid overflowing its buffer. It therefore advertises a window size of

$$\text{AdvertisedWindow} = \text{MaxRcvBuffer}-((\text{NextByteExpected}-1) -\text{LastByteRead})$$

which represents the amount of free space remaining in its buffer. As data arrives, the receiver acknowledges it as long as all the preceding bytes have also arrived. In addition, LastByteRcvd moves to the right (is incremented), meaning that the advertised window potentially shrinks. Whether or not it shrinks depends on how fast the local application process is consuming data. If the local process is reading data just as fast as it arrives (causing LastByteRead to be incremented at the same rate as LastByteRcvd), then the advertised window stays open (i.e., AdvertisedWindow = MaxRcvBuffer). If, however, the receiving process falls behind, perhaps because it performs a very expensive operation on each byte of data that it reads, then the advertised window grows smaller with every segment that arrives, until it eventually goes to 0.

TCP on the send side must then adhere to the advertised windowit gets from the receiver. This means that at any given time, it must ensure that

$$\text{LastByteSent}-\text{LastByteAcked} \leq \text{AdvertisedWindow}$$

Said another way, the sender computes an *effective* window that limits how much data it can send:

$$\text{EffectiveWindow} = \text{AdvertisedWindow}-(\text{LastByteSent}-\text{LastByteAcked})$$

All the while this is going on, the send side must also make sure that the local application process does not overflow the send buffer—that is, that

$$\text{LastByteWritten}-\text{LastByteAcked} \leq \text{MaxSendBuffer}$$

If the sending process tries to write y bytes to TCP, but

$$(\text{LastByteWritten}-\text{LastByteAcked})+y > \text{MaxSendBuffer}$$

then TCP blocks the sending process and does not allow it to generate more data.

8. Discuss TCP adaptive retransmission APR 2017

TCP ADAPTIVE RETRANSISSION

TCP copies with the loss of packets using a technique called *retransmission*. When TCP data arrives an *acknowledgement* is sent back to the sender. Whenever a TCP segment is transmitted, a copy of it is also placed on the retransmission queue. When TCP data is sent, a timer is started this starts from a particular value and counts down to zero. If the timer expires before an acknowledgement arrives, TCP retransmits the data.

Three algorithm of adaptive retransmission

- ✓ Simple algorithm (Original algorithm)
- ✓ Kern/Partridge algorithm
- ✓ Jacobson/Karels algorithm

Original Algorithm

We begin with a simple algorithm for computing a timeout value between a pair of hosts. This is the algorithm that was originally described in the TCP specification—and the following description presents it in those terms—but it could be used by any end-to-end protocol.

The idea is to keep a running average of the RTT and then to compute the timeout as a function of this RTT. Specifically, every time TCP sends a data segment, it records the time. When an ACK for that segment arrives, TCP reads the time again, and then takes the difference between these two times as a SampleRTT. TCP then computes an EstimatedRTT as a weighted average between the previous estimate and this new sample. That is,

$$\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT}$$

The parameter _ is selected to *smooth* the EstimatedRTT. A small _ tracks changes in the RTT but is perhaps too heavily influenced by temporary fluctuations. On the other hand, a large α is more stable but perhaps not quick enough to adapt to real changes. The original TCP specification recommended a setting of α between 0.8 and 0.9. TCP then uses EstimatedRTT to compute the timeout in a rather conservative way:

$$\textbf{TimeOut = 2×EstimatedRTT}$$

Karn/Partridge Algorithm

After several years of use on the Internet, a rather obvious flaw was discovered in this simple algorithm. The problem was that an ACK does not really acknowledge a transmission; it actually acknowledges the receipt of data. In other words, whenever a segment is retransmitted and then an ACK arrives at the sender, it is impossible to determine if this ACK should be associated with the first or the second transmission of the segment for the purpose of measuring the sample RTT.

It is necessary to know which transmission to associate it with so as to compute an accurate SampleRTT. As illustrated in Figure 5.10, if you assume that the ACK is for the original transmission but it was really for the second, then the SampleRTT is too large (a); if you assume that the ACK is for the second transmission but it was actually for the first, then the SampleRTT is too small (b).

The solution, which was proposed in 1987, is surprisingly simple. Whenever TCP retransmits a segment, it stops taking samples of the RTT; it only measures SampleRTT for segments that have been sent only once. This solution is knownas the Karn/Partridge algorithm, after its inventors.

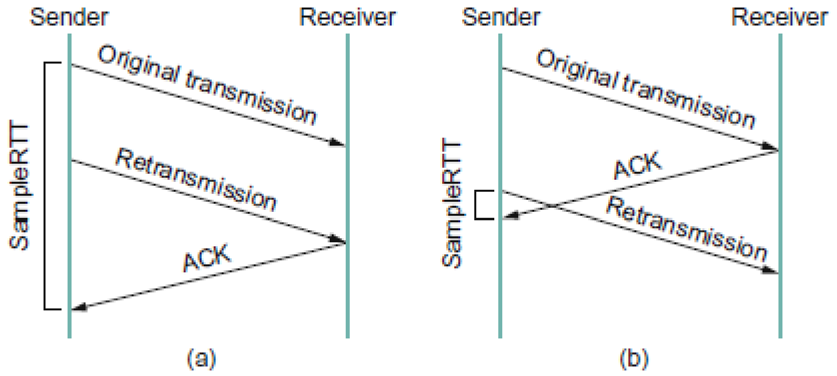


FIGURE 5.10 Associating the ACK with (a) original transmission versus (b) retransmission.

Their proposed fix also includes a second small change to TCP's timeout mechanism. Each time TCP retransmits, it sets the next timeout to be twice the last timeout, rather than basing it on the last EstimatedRTT. That is, Karn and Partridge proposed that TCP use exponential backoff, similar to what the Ethernet does. The motivation for using exponential backoff is simple: Congestion is the most likely cause of lost segments, meaning that the TCP source should not react too aggressively to a timeout. In fact, the more times the connection times out, the more cautious the source should become

Jacobson/Karels Algorithm

The Karn/Partridge algorithm was introduced at a time when the Internet was suffering from high levels of network congestion. Their approach was designed to fix some of the causes of that congestion, but, although it was an improvement, the congestion was not eliminated. The following year (1988), two other researchers—Jacobson and Karels—proposed a more drastic change to TCP to battle congestion. The bulk of that proposed change is described in Chapter 6. Here, we focus on the aspect of that proposal that is related to deciding when to time out and retransmit a segment.

As an aside, it should be clear how the timeout mechanism is related to congestion—if you time out too soon, you may unnecessarily retransmit a segment, which only adds to the load on the network. As we will see in Chapter 6, the other reason for needing an accurate timeout value is that a timeout is taken to imply congestion, which triggers a congestion-control mechanism. Finally, note that there is nothing about the Jacobson/Karels timeout computation that is specific to TCP. It could be used by any endto- end protocol.

The main problem with the original computation is that it does not take the variance of the sample RTTs into account. Intuitively, if the variation among samples is small, then the EstimatedRTT can be better trusted and there is no reason for multiplying this estimate by 2 to compute the timeout. On the other hand, a large variance in the samples suggests that the timeout value should not be too tightly coupled to the EstimatedRTT.

In the new approach, the sender measures a new SampleRTT as before. It then folds this new sample into the timeout calculation as follows:

$$\text{Difference} = \text{SampleRTT} - \text{EstimatedRTT}$$

$$\text{EstimatedRTT} = \text{EstimatedRTT} + (\delta \times \text{Difference})$$

$$\text{Deviation} = \text{Deviation} + \delta(|\text{Difference}| - \text{Deviation})$$

where δ is a fraction between 0 and 1. That is, we calculate both the mean RTT and the variation in that mean.

TCP then computes the timeout value as a function of both Estimated- RTT and Deviation as follows:

$$\text{TimeOut} = \mu \times \text{EstimatedRTT} + \phi \times \text{Deviation}$$

where based on experience, μ is typically set to 1 and $\phi$is set to 4. Thus, when the variance is small, TimeOut is close to EstimatedRTT; a large variance causes the Deviation termto dominate the calculation.

9. Explain in detail about TCP congestion control mechanisms OR Brief about approaches used for TCP congestion control (NOV 2013, 2014, 2015, 2016,2017) OR With TCPs slow start and AIMD for congestion control,show how the window size will vary for a transmission where every 5TH Packet is lost.Assume an advertised window size of 50 MSS (APR 2017)

Congestion, in a network may occur if the load on the network – the number of packets sent to the network is greater than the capacity of the network – the number of packets a network can handle.

- Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity that can either prevent congestion before it happens or remove congestion, after it has happened.
- There are two categories of congestion control
  - **Open-loop congestion control (prevention):** are applied to prevent congestion before it happens. In this, congestion control is handled by either the source or the destination.
  - **Closed-loop congestion control (removal):** try to remove congestion after it happens.

TCP CONGESTION CONTROL

Too many sources sending too much data too fast for network to handle. TCP uses congestion control to avoid congestion or remove congestion in the network.

Factors of congestion:

- Two senders, two receivers
- One router, infinite buffers
- No retransmission
- One router, finite buffers, reliable data transfer
- Sender retransmission of lost packet

Congestion Window

The sender’s window size is determined by the receiver and also by congestion in the network. The sender has two pieces of information:

i) The receiver – advertised window size (rwnd)
ii) The congestion window size (cwnd)

The actual size of the window is the minimize of these two
Max window = min (Congestion window, advertised window)
Effective window = Max window – (LastByteSend – LastByteAcked)
LastByteSend – LastByteAcked <= CongWin

Congestion Policy:
TCP handles congestion is based on three phases

i) Slow start (Exponential Increase)
ii) Additive Increase / Multiplicative Decrease
iii) Fast Retransmit and Fast Recovery

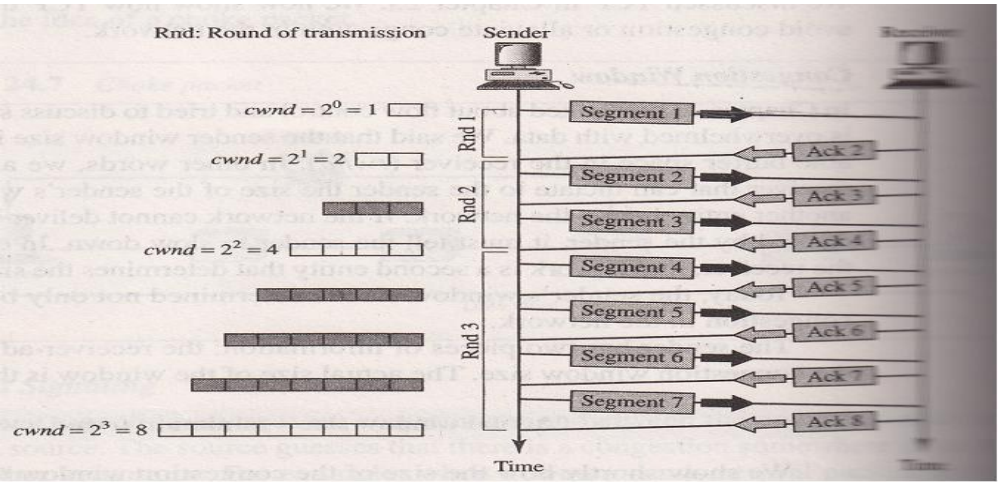
i) Slow Start

In this, the sender starts with a very slow rate of transmission but increases the rate rapidly to reach a threshold.

Slow start adds another window to the sender's TCP: the congestion window, called "cwnd". When a new connection is established with a host on another network, the congestion window is initialized to one segment. Each time an ACK is received, the congestion window is increased by one segment. The sender can transmit up to the minimum of the congestion window and the advertised window. The congestion window is flow control imposed by the sender, while the advertised window is flow control imposed by the receiver. The former is based on the sender's assessment of perceived network congestion; the latter is related to the amount of available buffer space at the receiver for this connection.

The sender starts by transmitting one segment and waiting for its ACK. When that ACK is received, the congestion window is incremented from one to two, and two segments can be sent. When each of those two segments is acknowledged, the congestion window is increased to four. This provides an exponential growth, although it is not exactly exponential because the receiver may delay its ACKs, typically sending one ACK for every two segments that it receives.

At some point the capacity of the internet can be reached, and an intermediate router will start discarding packets. This tells the sender that its congestion window has gotten too large.



Early implementations performed slow start only if the other end was on a different network. Current implementations always perform slow start.

- The source starts with cwnd = 1.
- Every time an ACK arrives, cwnd is incremented.
- Two slow start situations:
  - At the very beginning of a connection **{cold start**}.
  - When the connection goes dead waiting for a timeout to occur (i.e, the advertized window goes to zero!)
- However, in the second case the source has more information. The current value of cwnd can be saved as a **congestion threshold.**
- This is also known as the "slow start threshold" **ssthresh**.

When the size of window in bytes reaches this threshold, slow start stops and the next phase starts.

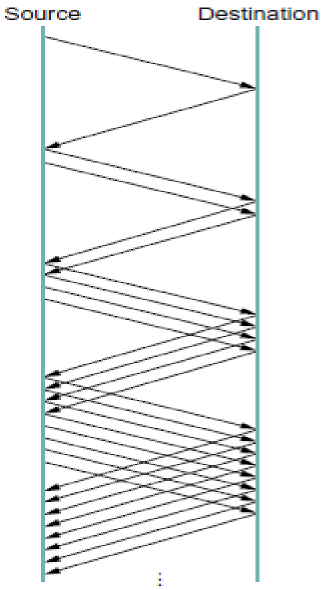
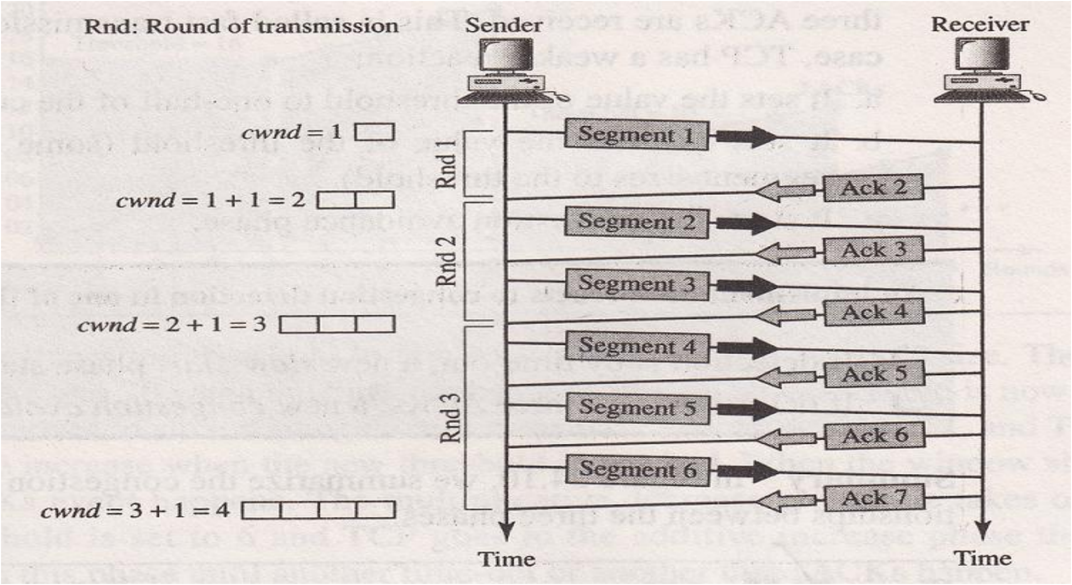


FIGURE 6.10 Packets in transit during slow start.

ii) Additive Increase (Congestion avoidance) / Multiplicative Decrease

To avoid congestion before it happens, one must slow down the exponential growth. When the size of the congestion window reaches the slow start threshold, the slow start phase steps and the additive phase begins. In this, each time the whole window of segments is acknowledged, the size of the congestion window is increased by 1.



After the sender has received acknowledgements for a complete window size of segments, the size of the congestion window increases additively until congestion is detected.
The congestion window is incremented as follows each time an ACK arrives:

Increment = MSS X (MSS / congestion window)
Congestion Window += Increment
Where MSS – Message Segment Size.

Multiplicative Decrease

If congestion occurs, the congestion window size must be decreased. Retransmission can occur in one of two cases, when a timer times out (or) when three ACKS are received. In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease.

TCP implementations have two reactions:

1. If a time-out occurs, there is a stronger possibility of congestion, a segment has probably been dropped in the network, and there is no news about the sent segments. In this, TCP reacts the following
    a. It sets the value of the threshold to one-half of the current window size.
    b. It sets cwnd to the size of one segment.
    c. It starts the slow-start phase again.
2. If three ACK's are received, there is a weaker possibility of congestion, a segment may have been dropped, but some segments after that may have arrived safely since three ACKs are received. This is called fast transmission and fast recovery.

    In this, TCP reacts the following:

a. It sets the value of the threshold to one-half of the current window size.
b. It sets cwnd to the value of the threshold.
c. It starts the congestion avoidance phase

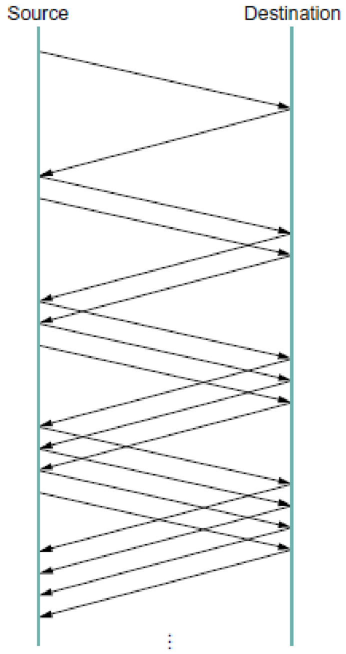


FIGURE 6.8 Packets in transit during additive increase, with one packet being added each RTT.

iii)Fast Retransmit & Fast Recovery

Every time a data packet arrives at the receiving side, the receiver responds with an acknowledgement. When a packet arrives out of order, TCP resends the same acknowledgement is sent the last time. This second transmission of the same acknowledgement is called a duplicate ACK.

When the sending side sees a duplicate ACK, it knows that the other side must have received a packet out of order. The sender waits until it sees some no. of duplicate ACK's and then retransmit the missing packet. TCP waits until it has seen three duplicate ACK's before retransmitting the packet.

In this diagram, the destination receives packets 1 & 2, but packet 3 is lost in the network. Thus the destination will send a duplicate ACK for packet 2 when packet 4 arrives, again when packet 5 arrives & so on. When the sender sees the third duplicate ACK for packet 2, the receiver had gotten packet 6, it retransmits packet s. When the retransmitted copy of packet 3 arrives at the destination, the receiver then sends a cumulative ACK for everything up to and including packet 6 back to the sends.

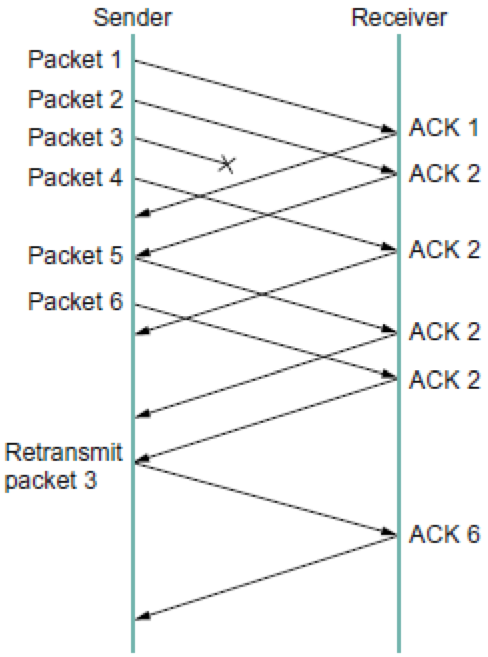


FIGURE 6.12 Fast retransmit based on duplicate ACKs.

Fast Recovery

After fast retransmit sends what appears to be the missing segment, congestion avoidance, but not slow start is performed. This is the fast recovery algorithm. It is an improvement that allows high throughput under moderate congestion, especially for large windows.

The reason for not performing slow start in this case is that the receipt of the duplicate ACKs tells TCP more than just a packet has been lost. Since the receiver can only generate the duplicate ACK when another segment is received, that segment has left the network and is in the receiver's buffer. That is, there is still data flowing between the two ends, and TCP does not want to reduce the flow abruptly by going into slow start.

The fast retransmit and fast recovery algorithms are usually implemented together as follows.

1. When the third duplicate ACK in a row is received, set ssthresh to one-half the current congestion window, cwnd, but no less than two segments. Retransmit the missing segment. Set cwnd to ssthresh plus 3 times the segment size. This inflates the congestion window by the number of segments that have left the network and which the other end has cached.

2. Each time another duplicate ACK arrives, increment cwnd by the segment size. This inflates the congestion window for the additional segment that has left the network. Transmit a packet, if allowed by the new value of cwnd.

3. When the next ACK arrives that acknowledges new data, set cwnd to ssthresh (the value set in step 1). This ACK should be the acknowledgment of the retransmission from step 1, one round-trip time after the retransmission. Additionally, this ACK should acknowledge all the intermediate segments sent between the lost packet and the receipt of

the first duplicate ACK. This step is congestion avoidance, since TCP is down to one-half the rate it was at when the packet was lost.

When fast retransmit detects three duplicate ACKs, start the recovery process from congestion avoidance region and use ACKs in the pipe to pace the sending of packets.

10. Write a detailed note on congestion avoidance mechanism used in TCP. NOV 2017
Or Explain congestion avoidance using random early detection in transport layer with example APR 2017

1. DEC Bit, 2. RED & 3. Source based Congestion Avoidance

DECbit

It is a first mechanism

- The idea here is to more evenly split the responsibility for congestion control between the routers and the end nodes.

- Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur.

- This notification is implemented by setting a **binary congestion bit** in the packets that flow through the router: hence the name DECbit.

- The destination host then copies this congestion bit into the ACk it sends back to the source.

- Finally, the source adjusts its sending rate so as to avoid congestion.

How it is functioning:

- A single congestion bit is added to the packet header. A router sets this bit in a packet if its average queue length is grater than or equal to 1 at the time the packet arrives.

- This average queue length is measured over a time interval that distance the last bust + idle cycle, plus the current busy cycle. (The router is busy when it is transmitting and idles when it is not).

- The above figure shows the queue length at a router as a function of time. Essentially, the router calculates the area under the curve and divides this value by the time interval to compute the average queue length

If less than 50% of the packets had the bit set, then the source increases its congestion window by one packet. If 50% or more of the last window's worth of packets had the congestion bit set, the source decreases its congestion window to 0.875 times the previous value.

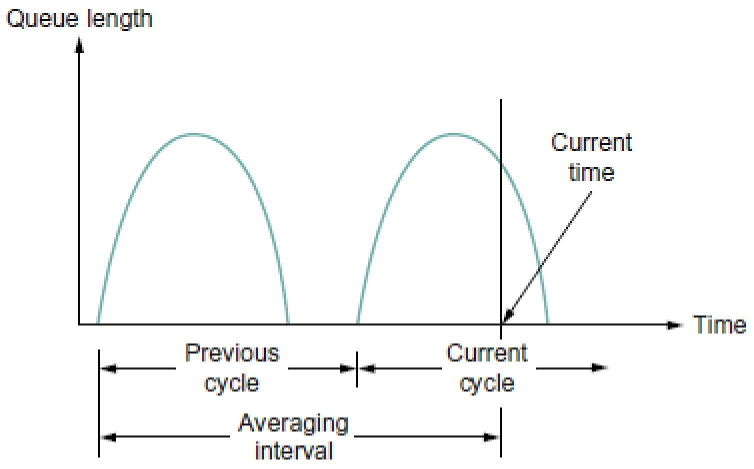


FIGURE 6.14 Computing average queue length at a router.

Random Early Detection (RED)

A second mechanism, called random early detection (RED), is similar to the DECbit scheme in that each router is programmed to monitor its own queue length, and when it detects that congestion is imminent (forthcoming), to notify the source to adjust its congestion window.

- The first is that rather than explicitly sending a congestion notification message to the source, RED is most commonly implemented such that it implicitly notifies the source of congestion by dropping one of its packets.
- The source is, effectively notified by the subsequent timeout or duplicates ACK. In case you haven't already guessed, RED is designed to be used in conjunction with TCP, which currently detects congestion by means of timeouts.
- As the "early" part of the RED acronym suggests, the gateway drops the packet earlier than it would have to, so as to notify the source that it should decrease its congestion window sooner than it would normally have.
- In other words, the router drops a few packets before it has exhausted its buffer space completely, so as to cause the source to slow down, with the hope that this will mean it does not have to drop lots of packets later on.
- Note that RED could easily be adapted to work with an explicit feedback scheme simply by marking a packet instead of dropping it, as discussed in the sidebar on Explicit Congestion Notification.

Source-Based Congestion Avoidance

- A strategy for detecting the initial stages of congestion – before losses occur – from the end hosts.

- The general idea of these techniques is to watch for some sign from the network that some router's queue is building up and that congestion will happen soon if nothing is done about it.

- A **first Scheme** the congestion window normally increases as in TCP, but every two round-trip delays the algorithm checks to see if the current RTT is greater than the average of the minimum and maximum RTT's seen so far. If it is, then the algorithm decreases the congestion window by one-eighth.

- A **second algorithm** is the decision as to whether or not to change the current window size is based on changes to both the RTT and the window size. The window is adjusted once every two round-trip delays based on the product

  (CurrentWindow – OldWindow) X (CurrentRTT – OldRTT)

  If the result is positive, the source decreases the window size by one-eighth; if the result is negative or 0, the source increases the window by one maximum packet size.
- A **third scheme**, Every RTT, it increases the window size by one packet and compares the throughput achieved to the throughput when the window was one packet smaller. If the difference is less than one-half the throughput achieved when only one packet was in transit. If the difference is greater than the algorithm decreases the window by one packet. This scheme calculates the throughput by dividing the number of bytes outstanding in the network by the RTT.

- A **fourth mechanism**, it looks at changes in the throughput rate, or more specifically, changes in the sending rate.

  It compares the measured throughput rate with an expected throughput rate. The algorithm, which is called **TCP Vegas**.
  TCP Vegas uses this idea to measure and control the amount of extra data this connection has in transit, where by "extra data" we mean that the source would not have transmitted had it been trying to match exactly the available bandwidth of the network. The goal of TCP Vegas is to maintain the "right" amount of extra data in the network.
  Obviously, if a source is sending too much extra data, it will cause long delays and possibly lead to congestion. Less obviously, if a connection is sending too little extra data, it cannot respond rapidly enough to transient increases in the available network bandwidth.
  - ✓ TCP Vegas sets BaseRTT to the minimum of all measured round-trip times; it is commonly the RTT of the first packet sent by the connection, before the router queues increase due to traffic generated by this flow. If we assume that we are not overflowing the connection, then the expected throughput is give by

    ExpectedRate = CongestionWindow / BaseRTT

    Where CongestinWindow is the TCP congestion window, which we assume (for the purpose of this discussion) to be equal to the number of bytes in transit.
  - ✓ Second TCP Vegas calculates the current sending rate, ActualRate. This is done by recording the sending time for a distinguished packet, recording how many

bytes are transmitted between the time that packet is sent and when its acknowledgment is received, computing the sample RTT for the distinguished packet when its acknowledgment arrives, and dividing the number of bytes transmitted by the sample RTT. This calculation is done once per round-trip time.

- ✓ Third, TCP Vegas compares ActualRate to ExpectedRate and adjusts the window accordingly. We let Diff = ExpectedRate – ActualRate. Note that Diff is positive or 0 by definition, since ActualRate > ExpectedRate implies that we need to change BaseRTT to the latest sampled RTT.

We also define two thresholds, α < β, roughly corresponding to having too little and too much extra data in the network, respectively. When Diff < α, TCP Vegas increases the congestion window linearly during the next RTT, and when Diff > β, TCP Vegas decreases the congestion window linearly during the next RTT. TCP Vegas leaves the congestion window unchanged when α < Diff < β.

11. Explain SCTP (Stream Control Transmission Protocol) in detail

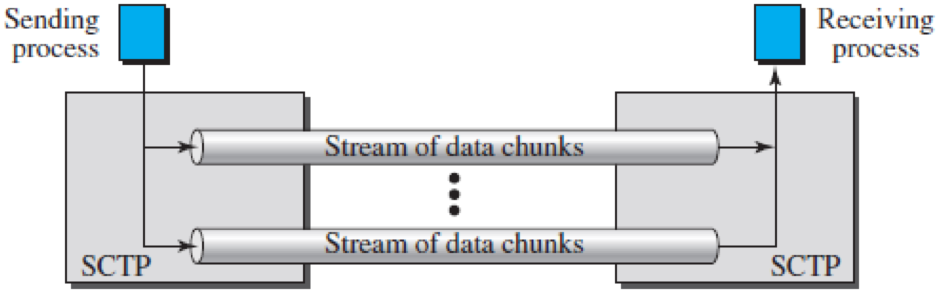
Stream Control Transmission Protocol (SCTP) is a new transport-layer protocol designed to combine some features of UDP and TCP in an effort to create a better protocol for multimedia communication.

SCTP Services

- ***Process-to-Process Communication***
- ***Multiple Streams***

SCTP allows **multistream service** in each connection, which is called ***association*** in SCTP terminology. If one of the streams is blocked, the other streams can still deliver their data.

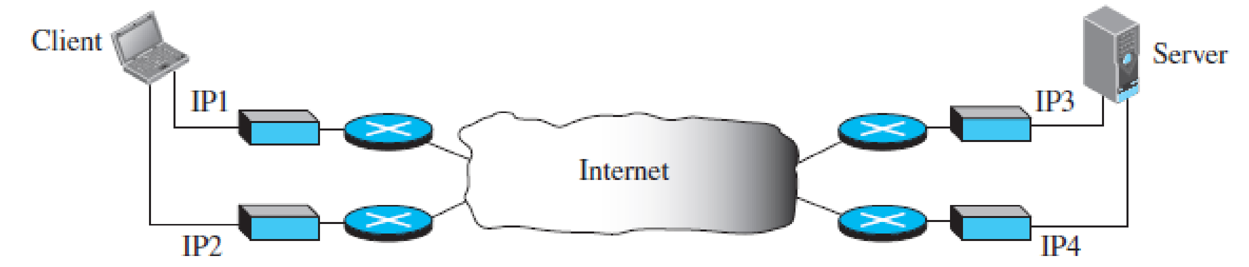
Figure 24.38 *Multiple-stream concept*



- ***Multihoming***

The sending and receiving host can define multiple IP addresses in each end for an association. In this fault-tolerant approach, when one path fails, another interface can be used for data delivery without interruption. This fault-tolerant feature is very helpful when we are sending and receiving a real-time payload such as Internet telephony.

Figure 24.39 *Multihoming concept*



- ***Full-Duplex Communication***
- ***Connection-Oriented Service***
- ***Reliable Service***

SCTP Features

Transmission Sequence Number (TSN)

The unit of data in SCTP is a data chunk, which may or may not have a one-to-one relationship with the message coming from the process because of fragmentation . Data transfer in SCTP is controlled by numbering the data chunks.
SCTP uses a **transmission sequence number (TSN)** to number the data chunks. In other words, the TSN in SCTP plays a role analogous to the sequence number in TCP.

Stream Identifier (SI)

In SCTP, there may be several streams in each association. Each stream in SCTP needs to be identified using a **stream identifier (SI).** Each data chunk must carry the SI in its header so that when it arrives at the destination, it can be properly placed in its stream. The SI is a 16-bit number starting from 0.

Stream Sequence Number (SSN)

When a data chunk arrives at the destination SCTP, it is delivered to the appropriate stream and in the proper order. This means that, in addition to an SI, SCTP defines each data chunk in each stream with a **stream sequence number (SSN).**

Acknowledgment Number

TCP acknowledgment numbers are byte-oriented and refer to the sequence numbers. SCTP acknowledgment numbers are chunk-oriented. They refer to the TSN. A second difference between TCP and SCTP acknowledgments is the control information

SCTP Packet Format

An SCTP packet has a mandatory general header and a set of blocks called chunks. There are two types of chunks: control chunks and data chunks. A control chunk controls and maintains the association; a data chunk carries user data. In a packet, the control chunks come before the data chunks. Figure 24.42 shows the general format of an SCTP packet.

General Header

The *general header* (packet header) defines the end points of each association to which the packet belongs, guarantees that the packet belongs to a particular association, and preserves the integrity of the contents of the packet including the header itself. The format of the general header is shown in Figure 24.43.

There are four fields in the general header. The source and destination port numbers are the same as in UDP or TCP. The verification tag is a 32-bit field that matches a packet to an association. This prevents a packet from a previous association from being mistaken as a packet in this association. It serves as an identifier for the association; it is repeated in every packet during the association. The next field is a checksum. However, the size of the checksum is increased from 16 bits (in UDP, TCP, and IP) to 32 bits in SCTP to allow the use of the CRC-32 checksum.

Figure 24.42 *SCTP packet format*

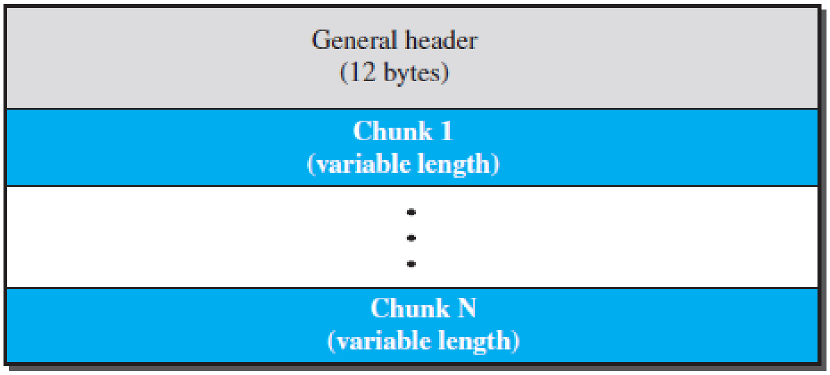
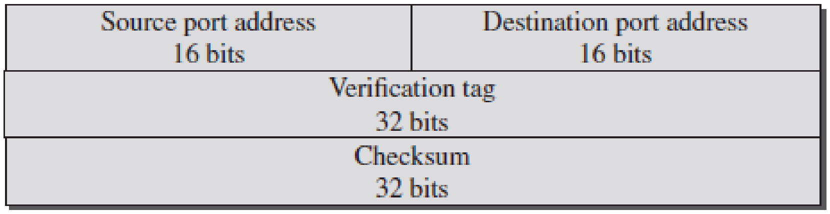


Figure 24.43 *General header*

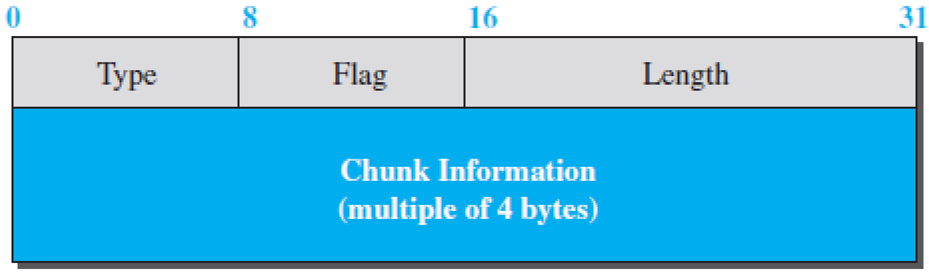


Source port address 16 bits	Destination port address 16 bits
Verification tag 32 bits	
Checksum 32 bits	

Chunks

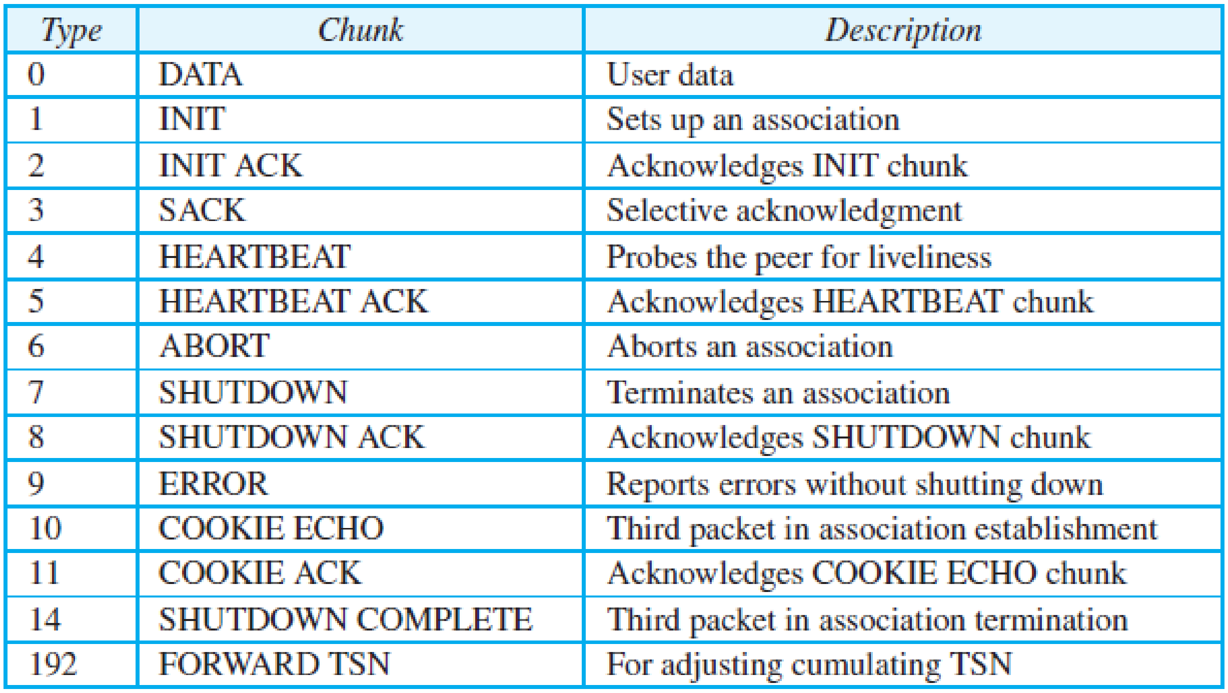
Control information or user data are carried in chunks. Chunks have a common layout, The first three fields are common to all chunks; the information field depends on the type of chunk

Figure 24.44 *Common layout of a chunk*



Types of Chunks
SCTP defines several types of chunks

Table 24.3 *Chunks*



Type	*Chunk*	*Description*
0	DATA	User data
1	INIT	Sets up an association
2	INIT ACK	Acknowledges INIT chunk
3	SACK	Selective acknowledgment
4	HEARTBEAT	Probes the peer for liveliness
5	HEARTBEAT ACK	Acknowledges HEARTBEAT chunk
6	ABORT	Aborts an association
7	SHUTDOWN	Terminates an association
8	SHUTDOWN ACK	Acknowledges SHUTDOWN chunk
9	ERROR	Reports errors without shutting down
10	COOKIE ECHO	Third packet in association establishment
11	COOKIE ACK	Acknowledges COOKIE ECHO chunk
14	SHUTDOWN COMPLETE	Third packet in association termination
192	FORWARD TSN	For adjusting cumulating TSN

An SCTP Association
SCTP, like TCP, is a connection-oriented protocol. However, a connection in SCTP is called an *association* to emphasize multihoming

- ***Association Establishment***
- ***Data Transfer***
  - *Multihoming Data Transfer*
  - *Multistream Delivery*
  - *Fragmentation*
- ***Association Termination***

Figure 24.45 *Four-way handshaking*

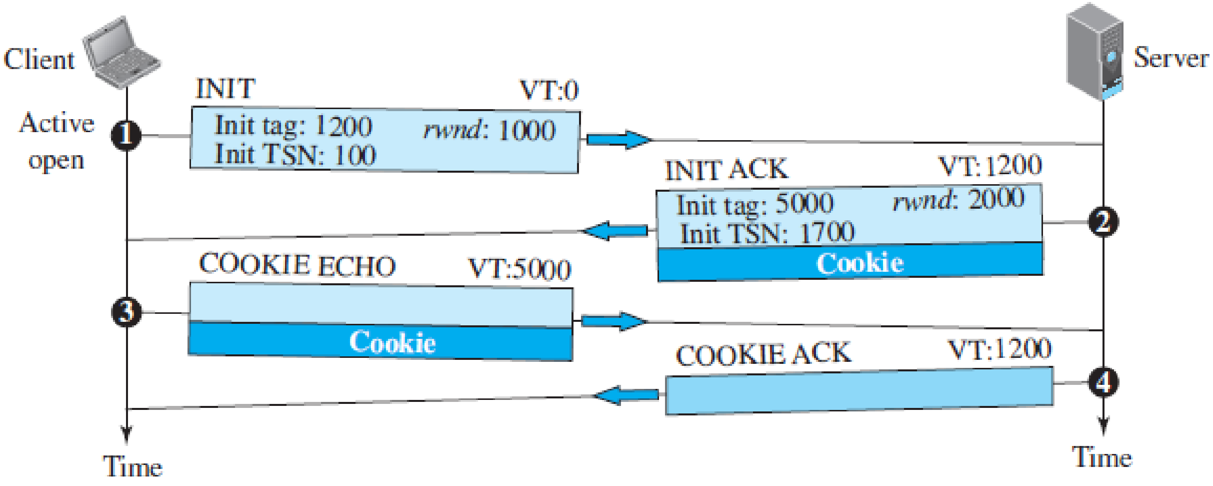
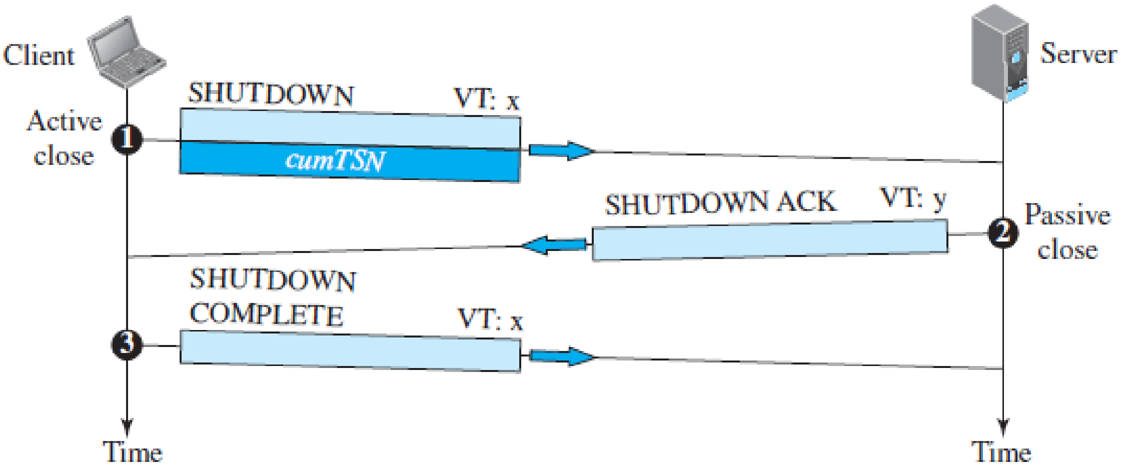


Figure 24.46 *Association termination*



UNIVERSITY QUESTIONS

B.E/B.TECH NOVEMBER/DECEMBER 2014(2008 Regulation)

2 MARKS

1. Differentiate TCP and UDP. (Q.NO. 2)
2. What is QOS? (Q.NO.32)

16 MARKS

1. Explain the following
   (i) TCP header (8) (Q.NO. 2)
   (ii) Adaptive flow control (8) (Q.NO. 4)
2. How is congestion controlled? Explain in detail the TCP congestion control (16)(Q.NO. 6)

B.E/B.Tech April May 2015

2 MARKS

1. List some of the Quality of service parameters of transport layer (Q.NO. 48)
2. How does transport layer perform duplication control? (Q.NO. 49)

16 MARKS

1. Explain the various fields of TCP header and the working of TCP protocol (16) (Q.NO. 2 & 3)

2 (i) i.Explain the three way handshake protocol to establish the transport level connection (8) (Q.NO. 3)

(ii) List the various congestion control mechanisms. Explain any one in detail (8) (Q.NO. 6)

B.E/B.Tech Nov-Dec 2015

2 MARKS

1. What is the difference between congestion control and flow control? (Q.NO 41)
2. What do you mean by QoS? (Q.NO 32)

16 MARKS

1. With a neat architecture, explain TCP in detail (Q.NO 2 & 3)
2. Explain TCP congestion control methods (Q.NO 6)

B.E/B.Tech April-May 2016

2 MARKS

1. What do you mean by slow start in TCP congestion? (Q.NO 50)
2. List the different phases used in TCP connection (Q.NO 51)

16 MARKS

1. Define UDP. Discuss the operations of UDP. Explain UDP checksum withone example. (Q.NO 1)
2. Explain in detail the various TCP congestion control mechanisms (Q.NO 6)

B.E/B.Tech Nov-Dec 2016

2 MARKS

1. Differentiate between TCP and UDP. **(Q.NO 2)**

16 MARKS

1. Explain various fields of TCP header and the working of the TCP protocol **(Q.NO 2)**
2. How is Congestion controlled? Explain in detail about congestion control techniques in transport layer **(Q.NO 6)**

B.E/B.Tech April-May 2017

2 MARKS

1. List out the advantages of connection oriented services over connectionless services. **(Q.NO 52)**
2. How do fast retransmit mechanism of TCP works. **(Q.NO 53)**

16 MARKS

1. (i) Explain the adaptive flow control and retransmission technique used in TCP **(Q.NO 4,5)**
   (ii) With TCPs slow start and AIMD for congestion control, show how the window size will vary for a transmission where every 5th Packet is lost. Assume an advertised window size of 50 MSS. **(Q.NO 6)**
2. (i) Explain congestion avoidance using random early detection in transport layer with example**(Q.NO.7)**
   (ii) Explain the different services operation of QOS in detail. **(Q.NO 9)**

Part-C

1. (i)Draw the format of TCP Packet header and explain each of its field. **(Q.NO 2)**
   (ii)Specify the justification for having variable field length for the field in TCP header.

B.E/B.Tech Nov-Dec 2017

2 MARKS

1. Compare flow control versus congestion control? **(Q.NO 41)**
2. What are the approaches used to provide range of quality of services? **(Q.NO 46)**

16 MARKS

1. (i)Draw the TCP state transition diagram for connection management. **(Q.NO 3)**
   (ii)Brief about approaches used for TCP congestion control. **(Q.NO 6)**
2. Write a detailed note on congestion avoidance mechanism used in TCP. **(Q.NO 7)**

UNIT II - DATA-LINK LAYER & MEDIA ACCESS

Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP - Media Access Control - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices.

PART A

1. What are the functions of MAC?

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

2. What is Ethernet?

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

3. Define Repeater?

A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals. However, no more than four repeaters may be positioned between any pairs of hosts, meaning that an Ethernet has a total reach of only 2,500m.

4. Why Ethernet is said to be a I-*persistent* protocol?

An adaptor with a frame to send transmits with probability ‘1 ‘whenever a busy line goes idle.

5. What is exponential back off? (Nov 2016)

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each transmission attempt is a general technique known as exponential back off.

6. What are the four prominent wireless technologies?

- Bluetooth
- Wi-Fi(formally known as 802.11)
- WiMAX(802.16)
- Third generation or 3G cellular wireless.

7. Define Bluetooth? (May 2016)

Bluetooth fills the niche of very short-range communication between mobile phones, PDAs, notebook computers, and other personal or peripheral devices. For example, Bluetooth can be used to connect mobile phones to a headset, or a notebook computer to a printer.

8. Explain the term handoff?

If the phone is involved in a call at the time , the call must be transferred to the new base station in what is called a hand off.

9. What is the use of Switch?

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

10. What is meant by circuit switching? (NOV/DEC 2010)

Circuit switching is a process that establishes connections on demand and permits exclusive use of those connections until released.

11. What is Spanning tree?

It is for the bridges to select the ports over which they will forward frames. A spanning tree is a subgraph of this graph that covers (spans) all the vertices but contains no cycles. That is, a spanning tree keeps all of the vertices of the original graph but throws out some of the edges

12. What are the three pieces of information in the configuration messages?

1. The ID for the bridge that is sending the message.
2. The ID for what the sending bridge believes to the root bridge.
3. The distance, measured in hops, from the sending bridge to the root bridge.

13. What is broadcast?

Broadcast is simple – each bridge forwards a frame with a destination broadcast address out on each active (selected) port other than the one on which the frame was received.

14. What is multicast?

It can be implemented with each host deciding for itself whether or not to accept the message.

15. How does a given bridge learn whether it should forward a multicast frame over a given port?

It learns exactly the same way that a bridge learns whether it should forward a unicast frame over a particular port- by observing the source addresses that it receives over that port.

16. Differentiate fast Ethernet and gigabit Ethernet. (NOV/DEC 2012)

Fast Ethernet cards connect to networks at a rate of 100 Mbps while Gigabit network cards can connect at speeds up to 1000mb/s. The main difference between the two is speed. A fast Ethernet card can run on bandwidths at 100mb/s while a gigabit Ethernet can run at ten times that speed. However, the existence of FDDIs around made this technology more like a stepping stone to something better – enter the gigabit card. Gigabit networks are made to run the best at Layer 3 switching meaning it has more route functionality than the 100mbs fast Ethernet.

17. What is Transceiver?

Transceiver is a device which connects host adaptor to Ethernet Cable. It receives and sends signal.

18. What is the difference between switch and bridge? (NOV/DEC 2012)

Bridge	**Switch**
A bridge is device which operates at the data link layer. It may be used to join two	A bridge with more than two interface (ports)is also known as a switch

LAN segment(A,B),Constructing a larger LAN	
Bridges receive Ethernet frames then forward all frames, like a repeater	A switch, on the other hand ,forward the frame to only the required interfaces
Bridges learns the association between the system MAC addresses and the interface ports.	The switch reduces the number the number of packets on the other LAN segments, by sending the packet only where it need to go.

.

19. Define bridge and switch. (NOV/DEC 2012)

- Bridges are software based ,while switches are hardware based
- Bridges can only have one spanning –tree instance per bridge, while switches can have many
- Bridges can only have up to 16 ports, whereas a switch can have hundreds.

20. State the difference between token ring and FDDI? (NOV/DEC 2010)

Token ring	FDDI
• It uses shielded twisted pair cables • It uses Manchester encoding • It supports data rate upto 16Mbps • It is implemented as a ring, switch or multistation access unit	It uses fibre optic cables. It uses 4B/5B before NRZ-1 for encoding It supports data rate upto100 Mpbs It is implemented as dual ring, nodes with single attachment station and dual attachment station with concentrator.

21. Define a Bridge. (NOV/DEC 2010)

A network bridge is an abstract device that connects multiple network segments along the data link layer. A concrete example of a bridge in a computer network is the network switch.

22. A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network? (APRIL/MAY 2011)

Throughput= (12,000*10,000)/60=2Mbps.

It is 1/5th of bandwidth.

23. **What is the role of VCI?**

A virtual channel identifier (VCI) distinguishes virtual channels (also known as circuits) created in a packet/cell switched network. A VCI has multiple circuits per communication channel and is primarily used for managing the unique identification of each created circuit.

A VCI is also known as a virtual circuit identifier (VCI).

24. List the two main limitations of bridges.Nov/Dec 2013

- Limited scalability
    - to O(1,000) hosts
    - not to global networks
- Not heterogeneous
    - no translation between frame formats

25. Define source routing. Nov/Dec 2013

Source routing allows a sender of a packet to partially or completely specify the route the packet takes through the network.

Source routing allows easier troubleshooting, improved trace route, and enables a node to discover all the possible routes to a host. It does not allow a source to directly manage network performance by forcing packets to travel over one path to prevent congestion on another.

26. Why should Ethernet frame should be 512 bytes long?

A Valid collision can only happen within the first 512 bits of frame transmission.

The 512 bits include 12 bytes of addresses, plus 2 bytes used in the type/length field ,plus 46 bytes of data,plus 4 bytes of FCS. The preamble is not considered part of the actual frame in these calculations.

27. Define ICMP? (Or) Expand ICMP and write the function (May 2016)

Internet Control Message Protocol is a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully

28. Define Subnetting? (Nov 2015)

Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

29. What is CIDR? (MAY/JUNE2007)

Classless Inter-Domain Routing (**CIDR**) is a methodology of allocating and routing packets. It was introduced in 1993 to replace the prior addressing architecture of design in the with the goal to slow the growth of routing tables on routers across the Internet, and to help slow the rapid of addresses, uses a syntax of specifying IP addresses for IPv4 and IPv6, using the base address of the network followed by a slash and the size of the routing prefix, e.g., 192.168.0.0/16 (IPv4), and 2001:db8::/32 (IPv6).

30. What is (Differ) ARP and RARP? (MAY/JUNE 2009)

ARP stands for Address Resolution Protocol. It is used to convert IP address to Physical address.

RARP stands for Reverse Address Resolution Protocol. It is used to convert Physical address into IP address.

31. What is DHCP? (NOV/DEC 2012)

- Dynamic Host Configuration Protocol (DHCP) is a protocol designed to provide information dynamically.
- It is a client-server program.
- DHCP is used to assign addresses to a host dynamically.
- Basically, DHCP server has two databases.
- The first database is addresses to IP addresses.

32. What are the salient features of IPV6? (NOV/DEC 2012)

- New Packet Format and Header
- Large Address Space
- State full and Stateless IPv6 address
- Multicast
- Integrated

33. Give the CIDR notation for class A, B and C. APR/MAY 2011)

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

34. What is IP addressing?

Internet address or IP address is 32 bit identifier that uniquely and universally defines a host or router connected to the internet.

35. What is the need of subnetting. (NOV/DEC 2013)

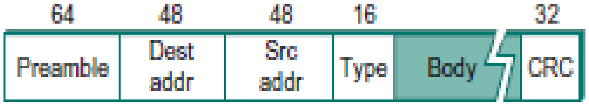
Subnetting is the technique used to break down networks into subnets. With the advent of internet, IP based networks become hugely popular. Due to this available IP addresses depleted at huge rate. To overcome this shortage concept of subnetting was introduced. Subnetting removes the classification of IP addresses according to classes and helps in creating further subnetworks from existing range of a IP network range.
For e.g A class B IP address can be broken down into further smaller networks.

36. What is the need for ARP? (NOV/DEC 2013) (Nov 2015)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long.

In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) 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 protocol rules for making this correlation and providing address conversion in both directions.

37. Draw Ethernet frame format (Dec 2017)



38. Define collision detection?

In Ethernet, all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision detection.

39. What are the four steps involves in scanning?

The technique for selecting an AP is called *scanning* and involves the following four steps:

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points, and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

40. Define Piconet

The basic Bluetooth network configuration, called a *piconet*, consists of a master device and up to seven slave devices

41. Differentiate persistent and non persistent CSMA (Nov/Dec 2014)

In 1-persistent CSMA if the medium is busy, the channel will be sensed until it is idle, then it will transmit immediately. This means that collisions are almost guaranteed to occur.

In non-persistent CSMA if the medium is busy, there will be a random delay for retransmission. This reduces the probability of collisions, but wastes the capacity.

42. State the uses of valid transmission timer (Nov/Dec 2014)

The Valid Transmission Timer (TVX) times the period between correct frame transmissions, therefore is a check for faults on the ring. If it expires then a new claim process begins

43. What do you understand by CSMA protocol? (May 2015)

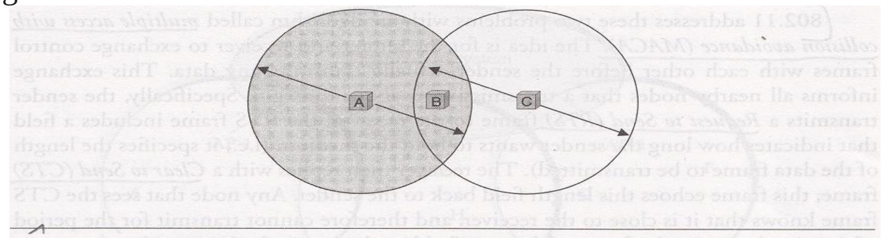
Carrier Sense Multiple Access is a probabilistic Media Access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus.

44. List the functions of bridges (May 2015) (May 2017)

1) Pass data frames between networks using MAC address
2) Break up collision domains
3) Forwards all broadcast messages

45. Define hidden node problem (May 2016)

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP.



The hidden node problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)

46. What is scatternet? (Nov 2016)

The bluetooth network consisting of one or more piconets is known as scatternet. The devices in one piconet type may function as master or slave in another piconet type of the same csatternet

47. Identify the class of the following IP address: (a) 110.34.56.45 (b) 212.208.63.23 (Nov 2015)

110.34.56.45 - Class A
212.208.63.23 - Class C

48. What is fragmentation and reassembly?

IP fragmentation is an Internet Protocol (IP) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transaction unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.

49. When is ICMP redirect message used? (May 2017)

The ICMP Redirect message is generated to inform a local host that it should use a different next hop router for a certain class of traffic

50. Highlights the characteristics of datagram networks (Dec 2017)

A datagram has the following characteristics: Data is transmitted from source to destination without guarantee of delivery. Data is frequently divided into smaller pieces and transmitted without a defined route or guaranteed order of delivery.

51. What are the services offered by data link layer?

Framing, Flow control, Error control, Congestion control

52. Define bit stuffing. Give example (MAY 2011) (May 2017)

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

e.g, Sending side - 011111**0**10

53. Define character stuffing

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by "escaping" the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing

PART B

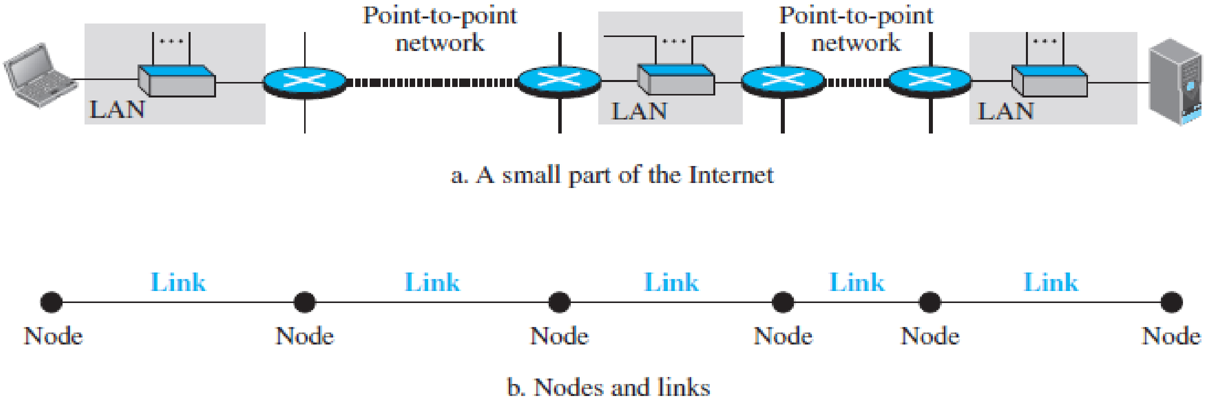
1. Discuss the services offered by data link layer

Introduction

Nodes and Links

Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. Theses LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as ***nodes*** and the networks in between as ***links.*** Figure 9.2 is a simple representation of links and nodes when the path of the data unit is only six nodes.

Figure 9.2 *Nodes and Links*



a. A small part of the Internet

b. Nodes and links

Services

The data-link layer is located between the physical and the network layers. The datalink layer provides services to the network layer; it receives services from the physical layer. Let us discuss services provided by the data-link layer.

The duty scope of the data-link layer is node-to-node. When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path. For this purpose, the data-link layer of the sending node needs to encapsulate the datagram received from the network in a frame, and the data-link layer of the receiving node needs to decapsulate the datagram from the frame.

- ***Framing***

Definitely, the first service provided by the data-link layer is **framing**. The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a **frame** before sending it to the next node. The node also needs to decapsulate the datagram from the frame received on the logical channel.

- ***Flow Control***

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

- ***Error Control***

Error control is used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

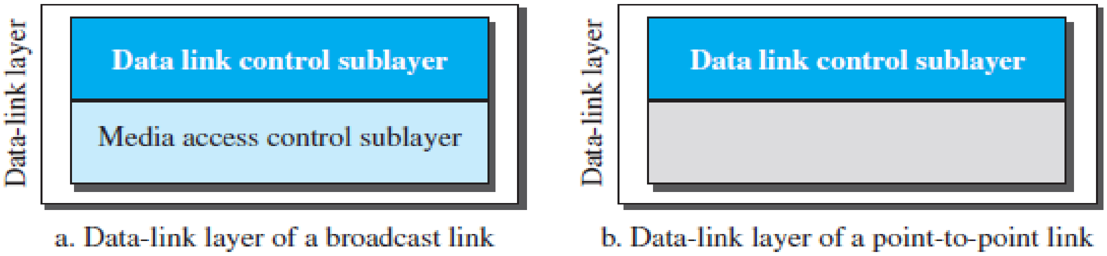
- ***Congestion Control***

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact

Two Sublayers

To better understand the functionality of and the services provided by the link layer, we can divide the data-link layer into two sublayers: **data link control (DLC)** and **media access control (MAC).**

Figure 9.4 *Dividing the data-link layer into two sublayers*


Data-link layer
Data link control sublayer
Media access control sublayer
a. Data-link layer of a broadcast link
Data-link layer
Data link control sublayer
b. Data-link layer of a point-to-point link

2. Discuss in detail about link layer addressing

A *link-layer address* is sometimes called a *link address*, sometimes a *physical address*, and sometimes a *MAC address*

Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer. When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header. These two addresses are changed every time the frame moves from one link to another

Three Types of addresses

- ***Unicast Address***

Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

- ***Multicast Address***

Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication. However, the jurisdiction is local (inside the link).

- ***Broadcast Address***

  Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

Address Resolution Protocol (ARP)

Introduction

- An internet consists of various types of networks and the connecting devices like routers.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognized by their IP addresses.

IP address

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

MAC address

- The packets from source to destination hosts pass through physical networks.
- At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed
- Deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.

Mapping of IP address into a MAC address

- We have seen the need of mapping an IP address into a MAC address.
- Two types of mapping 1) Static mapping and 2) Dynamic mapping

Static Mapping

- In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address.
- If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
- The limitation of static mapping is that the MAC addresses can change.
- To implement static mapping, the static mapping table needs to be updated periodically.

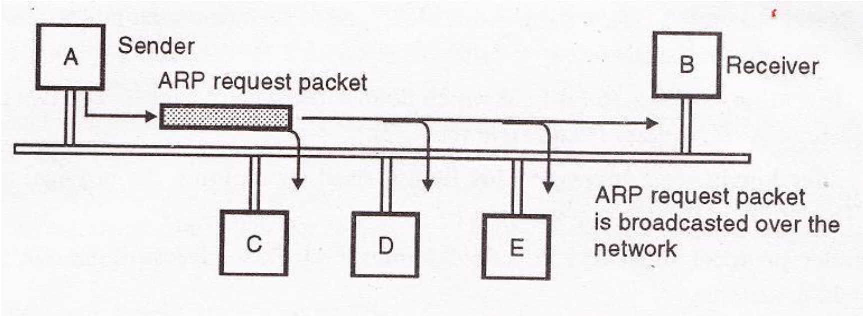
Dynamic mapping

- In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
- There are two type of dynamic mapping available.
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)
- The ARP maps IP address to a MAC address whereas the RARP maps a MAC address to an IP address.

ARP Operation

- ARP is used for associating an IP address to its MAC address.
- For a LAN, each device has its own physical or station address as its identification. This address is imprinted on the NIC.
- Find the MAC address:

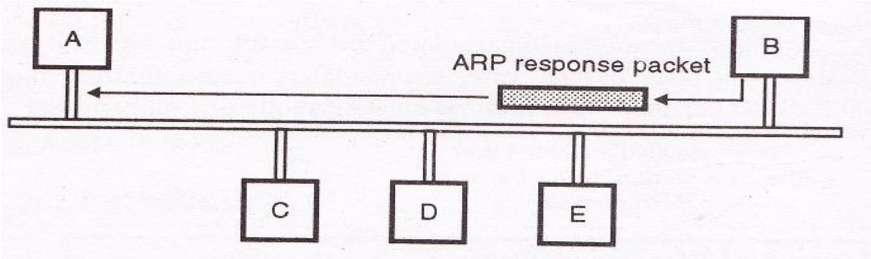
- When a router or a host needs to find the MAC address of another host or network the sequence of events taking place is as follows:
  a. The router or a host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
  b. This request packet is broadcasted over the network as shown the figure.
  c.



ARP request is broadcast

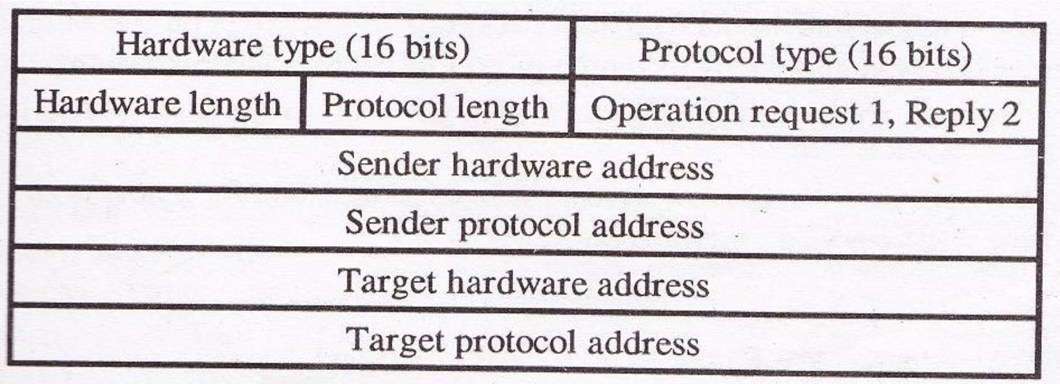
  d. Every host and router on the network receives and processes the ARP request packet. But only the intended receiver (B) recognizes its IP address in the request packet and sends back an ARP response packet.

  e. The ARP response packet contains the IP and physical addresses of the receiver (B). This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in the following figure.



ARP response unicast

ARP Packet Format:



Hardware type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

ARP frame format

HTYPE (Hardware type):
This 16 bit field defines the type of network on which is ARP is being run. ARP can run on any physical network.

PTYPE (Protocol type):
This 16 bit field is used to define the protocol using ARP. Note that ARP can be used with any higher-level protocol such as IPv4.

HLEN (Hardware length):
It is an 8 bit field which is used for defining the length of the physical address in bytes. For example, this value is 6 for Ethernet.

PLEN (Protocol length):
This field is 8 bit long and it defines the length of the IP address in bytes. For IPv4 this value is 4.

OPER (Operation):
It is a 16 bit field which defines the type of packet. The two possible types of packets are:
ARP request (1) and ARP reply (2).

SHA (Sender Hardware Address):
This field is used for defining the physical address of the sender. The length of this field is variable.

SPA (Sender Protocol address):
This field defines the logical address of the sender. The length of this field is variable.

THA (Target hardware address):
It defines the physical address of the target. It is a variable length field. For the ARP request packet, this field contains all zeros because the sender does not know the receivers physical address.

TPA (Target Protocol address):
This field defines the logical address of the target. It is a variable length field.

3. Explain in detail about DLC services with HDLC & PPP

The **data link control (DLC)** deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast. Data link control functions include *framing* and *flow and error control*

Framing

To transmit frames over the node it is necessary to mention start and end of each frame. There are three techniques to solve this frame

- Byte-Oriented Protocols (BISYNC, PPP, DDCMP)
- Bit-Oriented Protocols (HDLC)
- Clock-Based Framing (SONET)

Byte Oriented protocols

In this, view each frame as a collection of bytes (characters) rather than a collection of bits. Such a byte-oriented approach is exemplified by the BISYNC (Binary Synchronous Communication) protocol and the DDCMP (Digital Data Communication Message Protocol)
Sentinel Approach

The BISYNC protocol illustrates the sentinel approach to framing; its frame format is

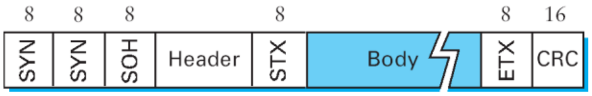


Fig: BISYNC Frame format

- The beginning of a frame is denoted by sending a special SYN (synchronization) character.
- The data portion of the frame is then contained between special sentinel characters: STX (start of text) and ETX (end of text).
- The SOH (start of header) field serves much the same purpose as the STX field.
- The frame format also includes a field labeled CRC (cyclic redundancy check) that is used to detect transmission errors.

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by "escaping" the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing.

Byte-Counting Approach

The number of bytes contained in a frame can he included as a field in the frame header. DDCMP protocol is used for this approach. The frame format is

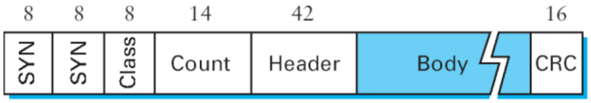
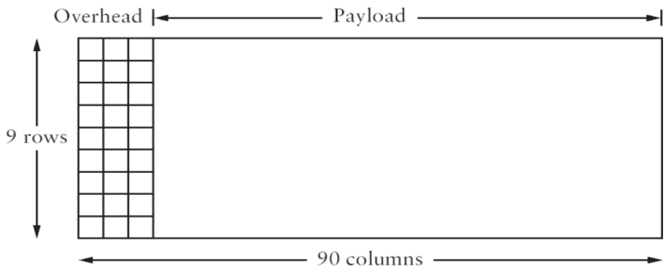


Fig: DDCMP frame format

- COUNT Field specifies how many bytes are contained in the frame's body.
- Sometime count field will be corrupted during transmission, so the receiver will accumulate as many bytes as the COUNT field indicates. This is sometimes called a framing error.
- The receiver will then wait until it sees the next SYN character.

Clock-Based Framing (SONET)

- Synchronous Optical Network Standard is used for long distance transmission of data over optical network.
- It supports multiplexing of several low speed links into one high speed links.
- An STS-1 frame is used in this method.



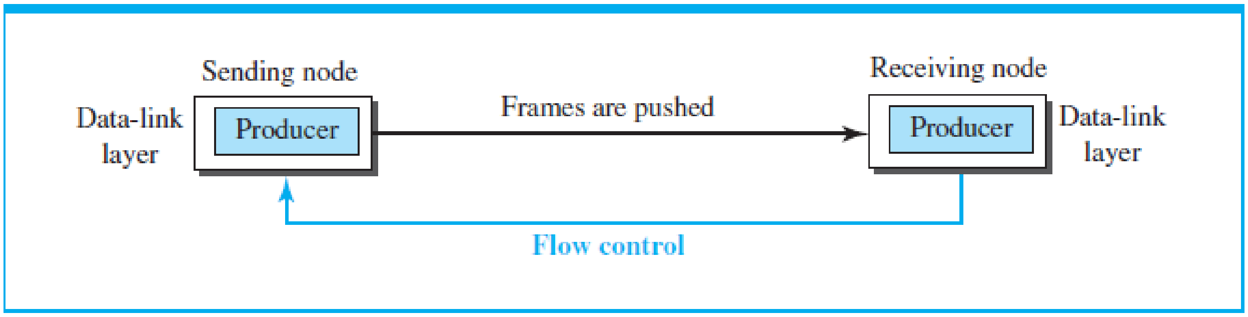
- It is arranged as nine rows of 90 bytes each, and the first 3 bytes of each row are overhead, with the rest being available for data.
- The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to determine where the frame starts.

- The receiver looks for the special bit pattern consistently, once in every 810 bytes, since each frame is 9 x 90 = 810 bytes long.

Flow and Error Control

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates. If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items. If the items are produced more slowly than they can be consumed, the consumer must wait, and the system becomes less efficient. Flow control is related to the first issue. We need to prevent losing the data items at the consumer site.

Figure 11.5 *Flow control at the data-link layer*



The figure shows that the data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node. If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames. Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers

Although flow control can be implemented in several ways, one of the solutions is normally to use two *buffers*; one at the sending data-link layer and the other at the receiving data-link layer. A buffer is a set of memory locations that can hold packets at the sender and receiver. The flow control communication can occur by sending signals from the consumer to the producer. When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

Error Control

Error control at the data-link layer is normally very simple and implemented using one of the following two methods. In both methods, a CRC is added to the frame header by the sender and checked by the receiver.

❑ In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.
❑ In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control) to the sender.

Connectionless and Connection-Oriented

A DLC protocol can be either connectionless or connection-oriented.

Connectionless Protocol

In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent. Note that the term *connectionless* here does not mean that there is no physical connection (transmission medium) between the nodes; it means that there is no *connection* between frames. The frames are not numbered and there is no sense of ordering. Most of the data-link protocols for LANs are connectionless protocols.

Connection-Oriented Protocol

In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase). After all frames that are somehow related to each other are transmitted (transfer phase), the logical connection is terminated (teardown phase). In this type of communication, the frames are numbered and sent in order. If they are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer. Connection oriented protocols are rare in wired LANs, but we can see them in some point-to-point protocols, some wireless LANs, and some WANs.

4. Discuss the protocols used in data link layer .

- Simple Protocol
- Stop-and-Wait Protocol
- Piggybacking

Point-to-Point Protocol (PPP)

The more recent Point-to-Point Protocol (PPP). The format of PPP frame is

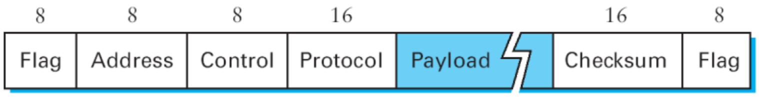


Fig: PPP Frame Format

- ➢ The Flag field has <u>01111110 as starting sequence</u>.
- ➢ The Address and Control fields usually contain default values
- ➢ The Protocol field is used for demultiplexing.
- ➢ The frame payload size can he negotiated, but it is 1500 bytes by default.
- ➢ The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.
- ➢ Negotiation is conducted by a protocol called LCP (Link Control Protocol).
- ➢ LCP sends control messages encapsulated in PPP frames—such messages are denoted by an LCP identifier in the PPP Protocol.

Bit-Oriented Protocols (HDLC)

In this, frames are viewed as collection of bits. High level data link protocol is used. The format is

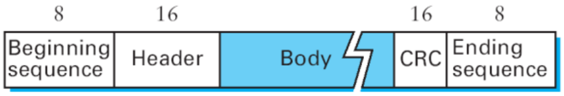


Fig: HDLC Frame Format

➢ HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.

➢ This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing.

➢ On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.

➢ On the receiving side, five consecutive 1's arrived, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five is).

➢ If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true, either this is the end-of-frame marker or an error has been introduced into the bit stream.

➢ By looking at the next bit, the receiver can distinguish between these two cases:

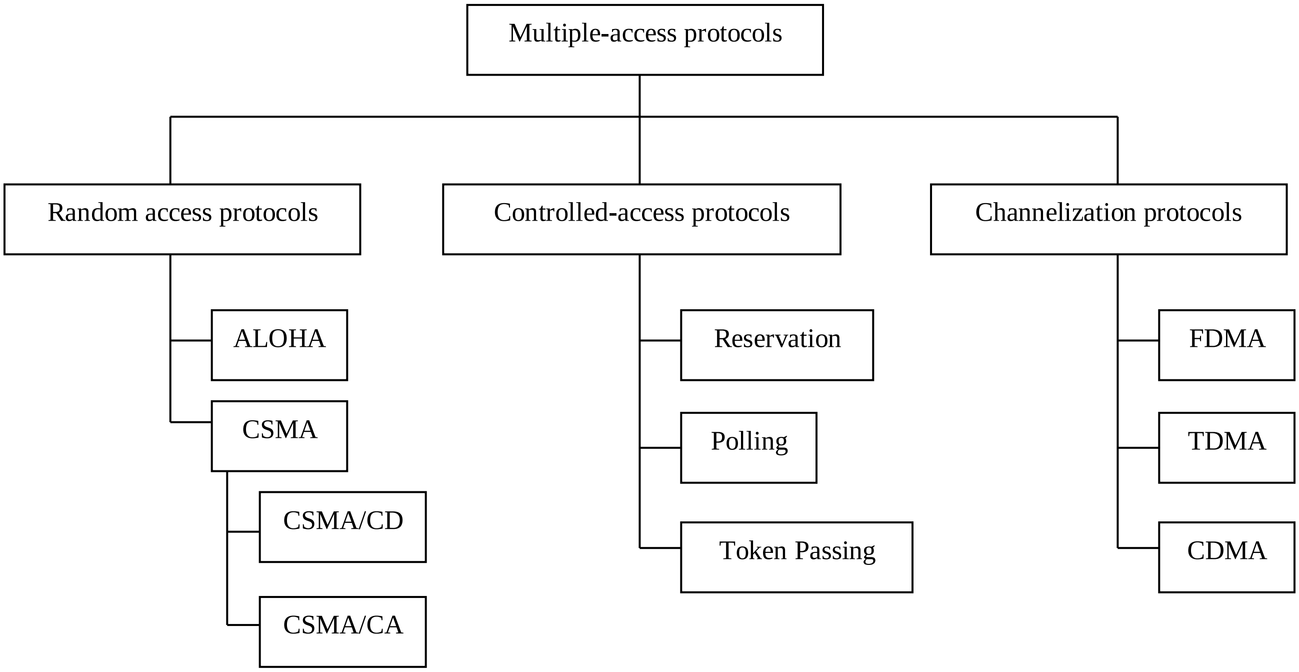
1.If it sees a 0 (i.e., the last eight bits it has looked at are 01111110), then it is the end-of- frame marker.

2.If it sees a 1 (i.e., the last eight bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.

5. Discuss Media Access Layer Protocols in detail.

- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.

TAXONOMY OF MULTIPLE ACCESS PROTOCOLS



RANDOM ACCESS

- In random access or contention methods, no station is superior to another station and none is assigned to control over another.
- No station permits, or does not permit another station to send.

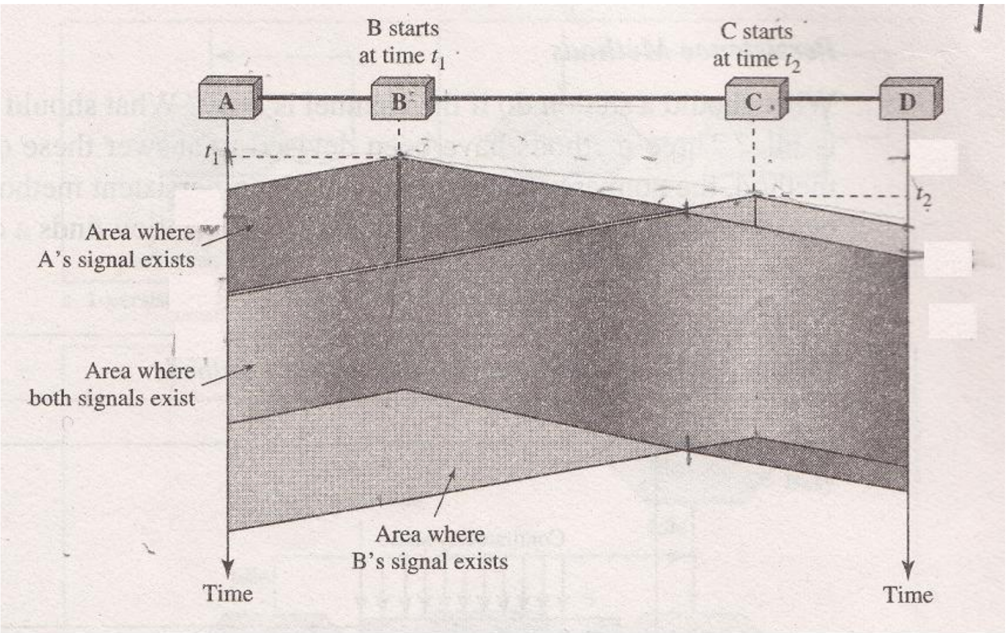
Two Features of Random Access

- There is no scheduled time for a station to transmit as the name implies. No rules specify which station should send next.
- Stations fight with one another to access the medium by a method called contention methods.

CSMA - Carrier Sense Multiple Access
CD - ***Collision Detection***
CA - ***Collision Avoidance***

CSMA

- To minimize the chance of collision and increase the performance CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

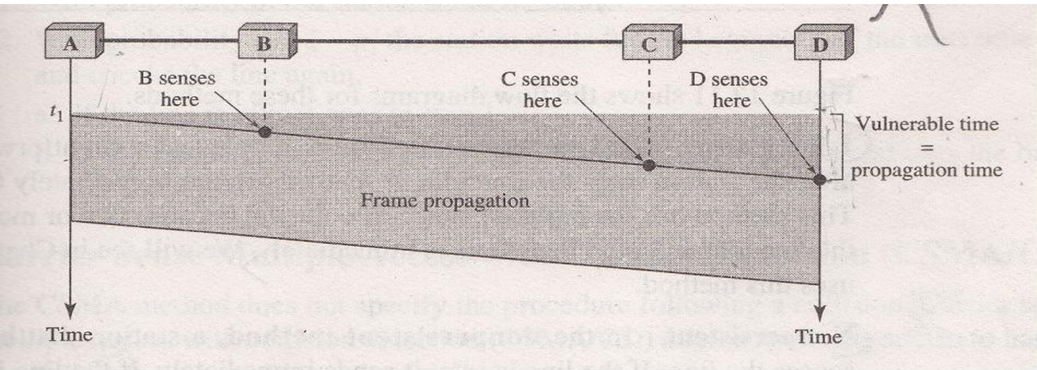


Space/time model of the collision in CSMA

- At time t1, station B senses the medium and finds it idle, so it sends a frame.
- At time t2 (t2>t1), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C.
- Station C also sends a frame.
- The two signals collide and both frames are destroyed.

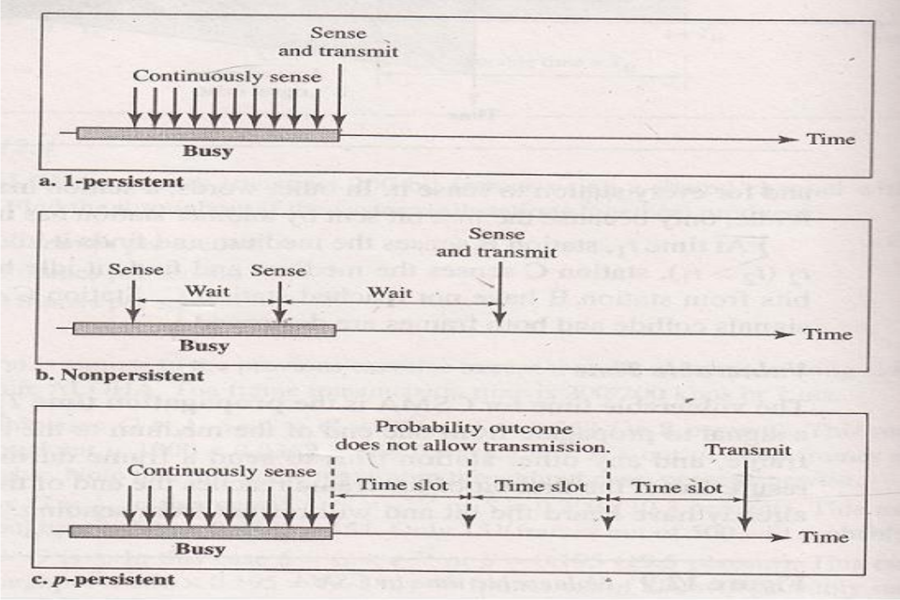
Vulnerable Time

- The vulnerable time for CSMA is the propagation time T_p.
- This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.



Vulnerable Time

Persistence Methods:



Behavior of three persistence methods

1-Persistent:

- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

Nonpersistent:

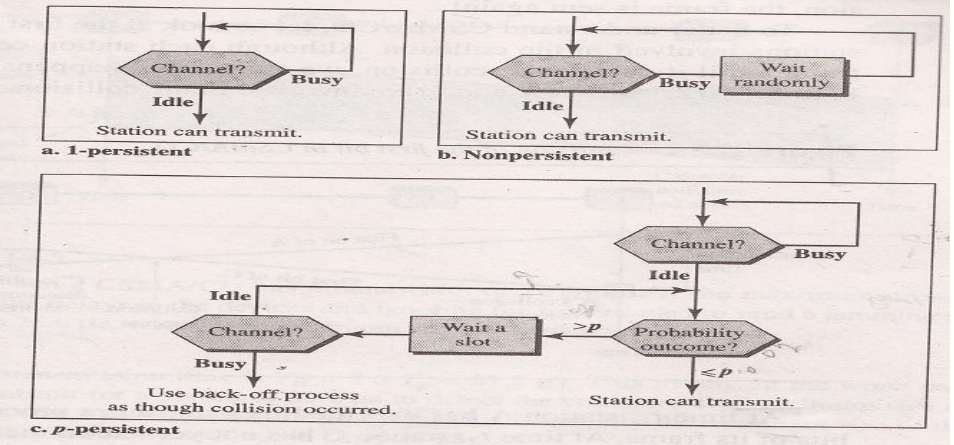
- In the nonpersistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.
- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.

P-Persistent:

- The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.

In this method, after the station finds the line idle it follows these steps:

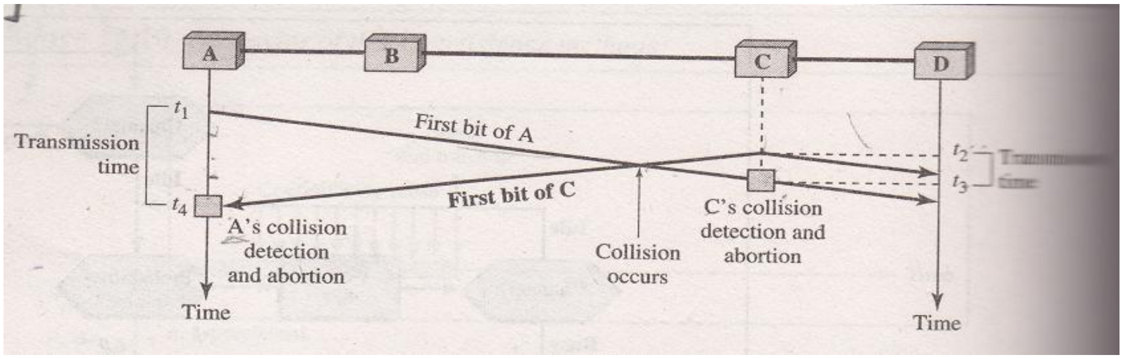
- ✓ With probability p, the station sends its frame.
- ✓ With probability q=1-p, the station waits for the beginning of the next time slot and checks the line again.
  - If the line is idle, it goes to step 1.
  - If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



CSMA/CD tells the station what to do when a collision is detected. CSMA/CA tries to avoid the collision.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- A station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished. If, however, there is a collision, the frame is sent again.



- Collision of the first bit in CSMA/CD
- At time t1, station A has executed its persistence procedure and starts sending the bits of its frame.
- At time t2, station C has not yet sensed the first bit sent by A.
- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time t2.
- Station C detects a collision at time t3 when it receives the first bit of A's frame.
- Station C immediately (or after a short time, but we assume immediately) aborts transmission.
- Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.
- Looking at the figure, we can see that A transmits for the duration t4 - t1; C transmits for the duration t3 - t2.

Minimum Frame Size:

- For CSMA/CD to work, we need a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.

- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time T_{ff} must be at least two times the maximum propagation time T_p.

Example

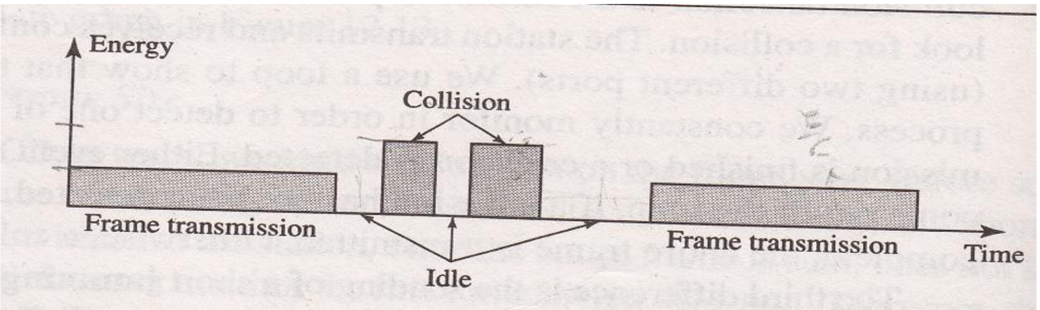
A network using CSMA/CD has a bandwidth of 10 Mbps.

If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal) is 25.6μs, what is the minimum size of the frame?

Solution: The frame transmission time is $T_{ff} = 2 X T_p = 51.2$μs. This means, in the worst case, a station needs to transmit for a period of 51.2μs to detect the collision. The minimum size of the frame is 10 Mbps X 51.2μs = 512 bits or 64 bytes.

Energy Level:

- Level of energy in a channel can have three values: Zero, normal, and abnormal.
- At the zero level, the channel is idle.
- At the normal level, a station has successfully captured the channel and is sending its frame.
- At the abnormal level, there is a collision and the level of the energy is twice the normal level.
- A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, bust or in collision mode.

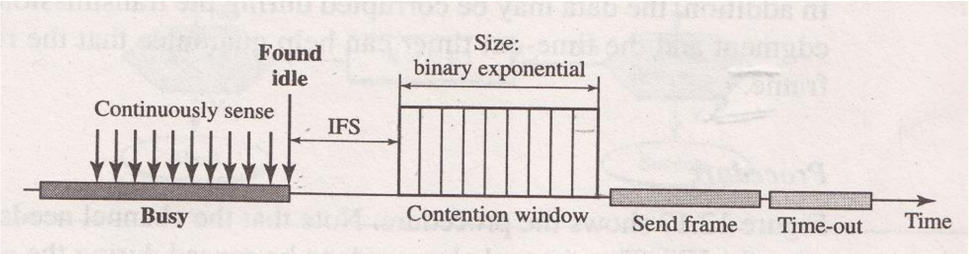


Energy level during transmission, idleness or collision

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- The basic idea behind CSMA/CA is that a station needs to be able to receive while transmitting to detect a collision.
- When there is no collision, the station receives one signal: its own signal.
- When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.

- In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver.
- This means that in a collision, the detected energy almost doubles.
- In a wireless network, much of the sent energy is lost in transmission.
- The received signal has very little energy.
- Therefore, a collision may add only 5 to 10 percent additional energy.
- This is not useful for effective collision detection.
- To avoid collisions on wireless networks because they cannot be detected carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network.
- Collisions are avoided through the use of CSMA/CA's three strategies: the inter-frame space, the contention window, and acknowledgements.



Timing in CSMA/CA

Inter-frame Space (IFS):

- First, collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found; the station does not send immediately.
- It waits for a period of time called the inter-frame space or IFS.
- Even though the channel may appear idle when it is sensed, a distance station may have already started transmitting.
- The distant station's signal has not yet reached this station.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

Contention Window:

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- The contention window is that the station needs to sense the channel after each time slot.
- In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

Acknowledgment

- With all these precautions, there still may be a collision resulting in destroyed data.
- In addition, the data may be corrupted during the transmission.
- The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

NOTE

Exponential backoff:

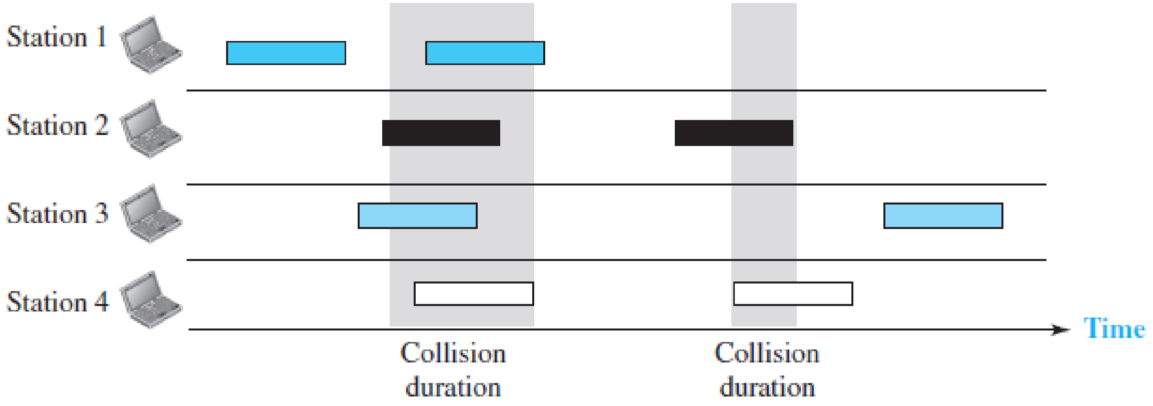
The strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential backoff**.

<u>ALOHA</u>

- ***Pure ALOHA***

The original ALOHA protocol is called ***pure ALOHA.*** This is a simple but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send (multiple access). However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure 12.2 shows an example of frame collisions in pure ALOHA.

Figure 12.2 *Frames in a pure ALOHA network*

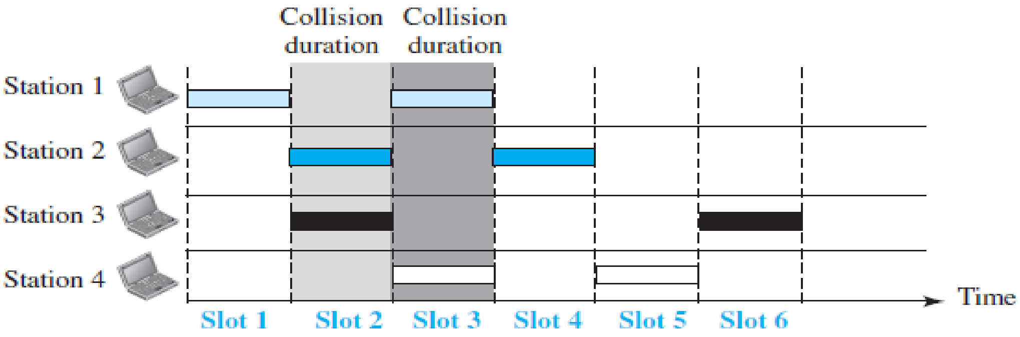


- ***Slotted ALOHA***

Pure ALOHA has a vulnerable time of 2 * *Tfr*. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or just before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In **slotted ALOHA** we divide the time into slots of *Tfr* seconds and force the station to send only at the beginning of the time slot. Figure 12.5 shows an example of frame collisions in slotted ALOHA.

Figure 12.5 *Frames in a slotted ALOHA network*



6. Explain controlled access protocol in media access control

In **controlled access,** the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three controlled-access methods

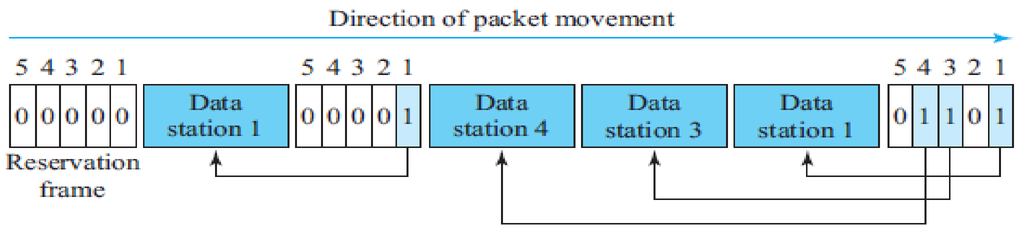
Reservation

In the **reservation** method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

If there are *N* stations in the system, there are exactly *N* reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

Figure 12.18 shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation

Figure 12.18 *Reservation access method*

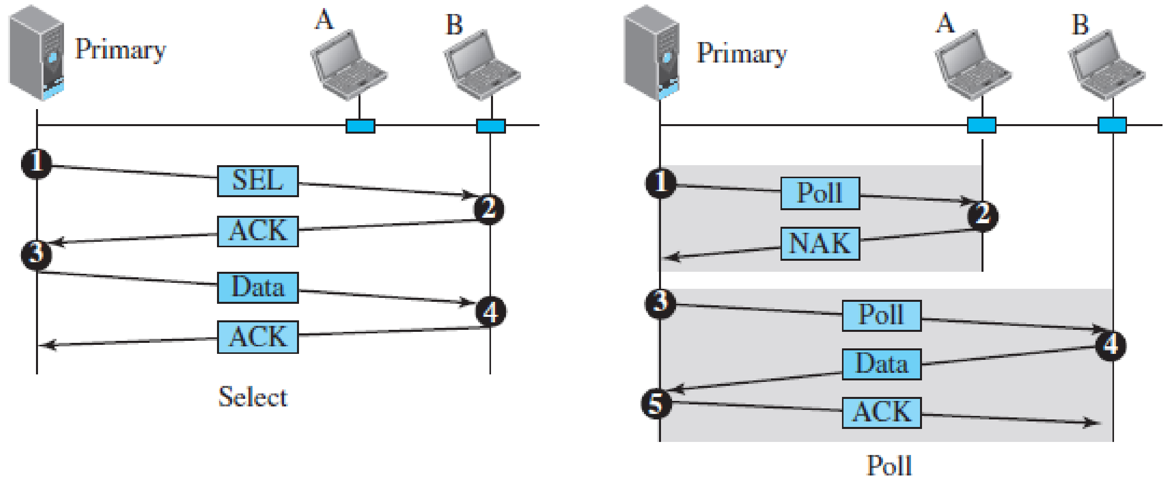


Polling

Polling works with topologies in which one device is designated as a ***primary station*** and the other devices are ***secondary stations.*** All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session (see Figure 12.19). This method uses poll and select functions to prevent collisions. However, the drawback is if the primary station fails, the system goes down.

Figure 12.19 *Select and poll functions in polling-access method*



Token Passing

In the **token-passing** method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor* and a *successor*. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

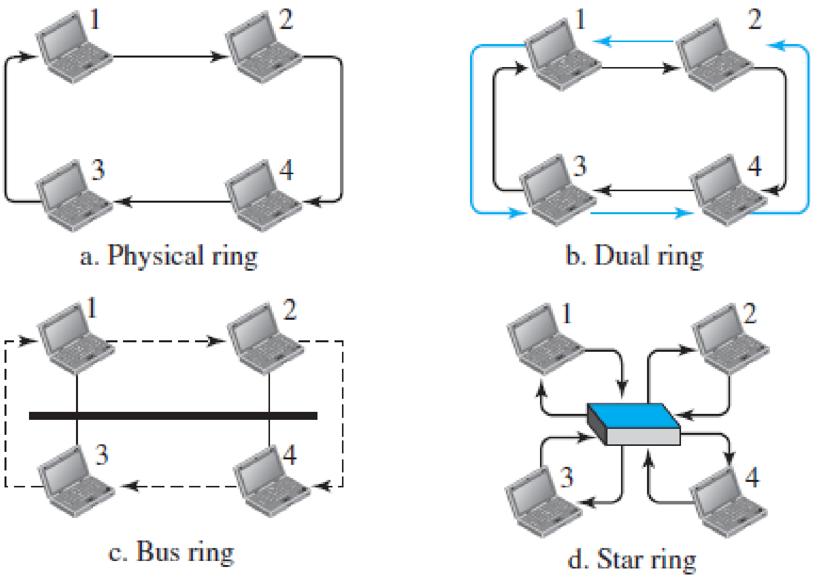
But how is the right to access the channel passed from one station to another? In this method, a special packet called a ***token*** circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station

Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to high-priority stations

Logical Ring

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one. Figure 12.20 shows four different physical topologies that can create a logical ring.

Figure 12.20 *Logical ring and physical topology in token-passing access method*



In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links—the medium between two adjacent stations—fails, the whole system fails.

The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only (such as a spare tire for a car). If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again. Note that for this topology to work, each station needs to have two transmitter ports and two receiver ports. The high-speed Token Ring networks called *FDDI (Fiber Distributed Data Interface)* and *CDDI (Copper Distributed Data Interface)* use this topology.

In the bus ring topology, also called a token bus, the stations are connected to a single cable called a *bus*. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes). When a station has finished sending its data, it releases the token and inserts the address of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media. The Token Bus LAN, standardized by IEEE, uses this topology.

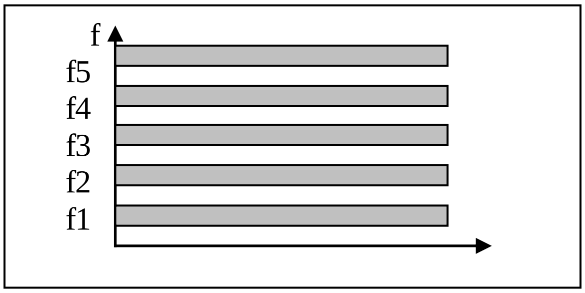
In a star ring topology, the physical topology is a star. There is a hub, however, that acts as the connector. The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections. This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate. Also adding and removing stations from the ring is easier. This topology is still used in the Token Ring LAN designed by IBM.

7. Discuss channelization protocol in media access control

Channelization (or *channel partition,* as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations. In this section, we discuss three channelization protocols: FDMA, TDMA, and CDMA.

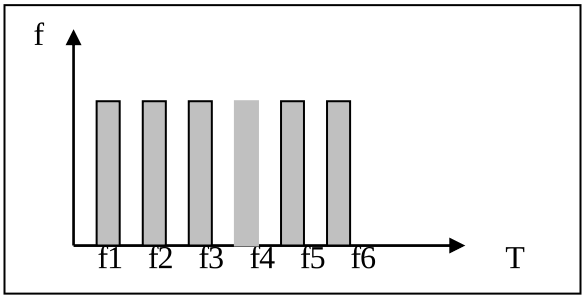
Frequency Division Multiple Access

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data.
- In this method when any one frequency level is kept idle and another is used frequently leads to inefficiency.



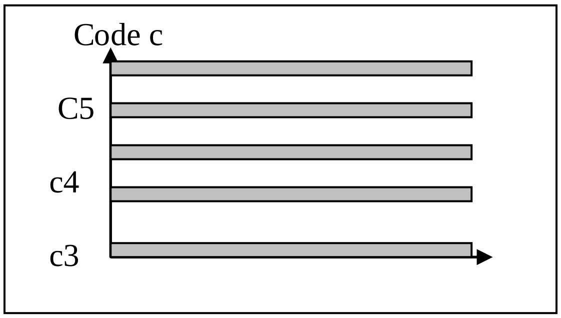
Time Division Multiple Access

- In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot.



Code Division Multiple Access

- CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.
- It differs from TDMA because all stations can send data at the same time without timesharing.
- CDMA simply means communication with different codes.
- CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips.
- Chips will be added with the original data and it can be transmitted through same medium.



8. Explain in detail about wired LAN - Ethernet (IEEE 802.3) and its frame format (OR) Explain the physical properties of Ethernet 802.3 with necessary diagram (NOV 2014)(May,Nov 2015 & 2016)

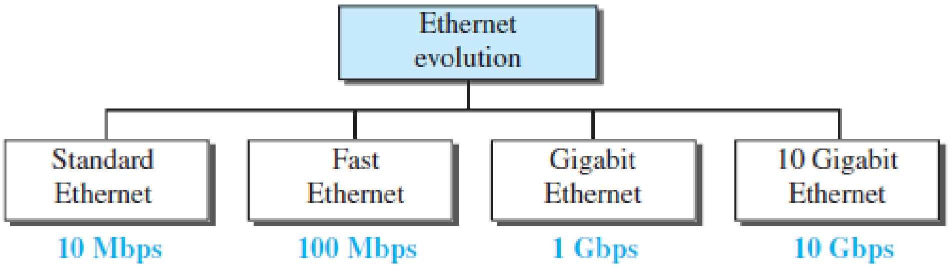
Introduction:

- The IEEE 802.3 standards committee developed a widely used LAN standard called Ethernet, which covers both the MAC layer and the physical layer.
- The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.
- The IEEE 802.3 standard uses CSMA for controlling media access and the 1-persistent algorithm explained earlier, although the lost time owing to collisions is very small.
- Also, IEEE 802.3 uses a back-off scheme known as binary exponential backoff.
- The use of random backoff minimizes subsequent collisions.
- This back-off scheme requires a random delay to be doubled after each retransmission.
- The user drops the frame after 16 retries.
- The combination of the 1-persistent scheme and binary exponential backoff results in an efficient scheme.
- The Ethernet versions have different data rates.

- Version 1000BaseSX, carrying 1 Gb/s, and 10GBase-T, carrying 10 Gb/s, hold the most promise for the future of high-speed LAN development

Ethernet Evolution

Figure 13.2 *Ethernet evolution through four generations*



Physical properties:

- An Ethernet segment is implemented on a coaxial cable of up to 500m.
- This cable is similar to the type used for cable TV, except that it typically has an impedance of 50 ohms instead of cable TV's 75 ohms.
- Hosts connect to an Ethernet segment by tapping into it; taps must be at least 2.5 m apart.
- A transceiver – a small device directly attached to the tap – detects when the line is idle and drives the signal when the host is transmitting.
- It also receives incoming signals.

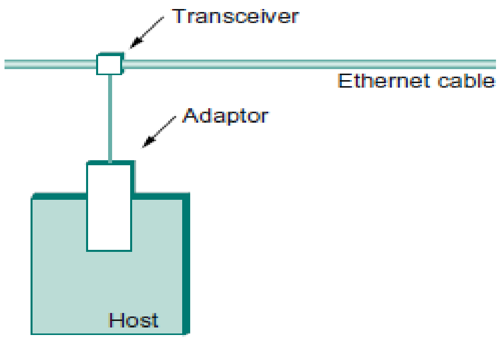


FIGURE 2.22 Ethernet transceiver and adaptor.

- The transceiver is, in turn, connected to an Ethernet adaptor, which is plugged into the host.

- Multiple Ethernet segments can be joined together by repeaters.
- A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals.
- However, no more than four repeaters may be positioned between any pair of hosts, meaning that an Ethernet has a total reach of only 2,500 m.

- Rather than using a 50-ohm coax cable, an Ethernet can be constructed from a thinner cable known as 10Base2; the original cable is called 10Base5 (the two cables are commonly called thin-net and thick-net, respectively).
- The “10” in 10Base2 means that the network operates at 10 Mbps, “Base” refers to the fact that the cable is used in a baseband system, and the “2” means that a given segment can be no longer than 200 m.
- Today, a third cable technology is predominantly used, called 10BaseT, where the “T” stands for twisted pair.
- A 10BaseT segment is usually limited to less than 100 m in length.
- Data transmitted by any one host on the Ethernet reaches all the other hosts.
- This is the good news.
- The bad news is that all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision domain.

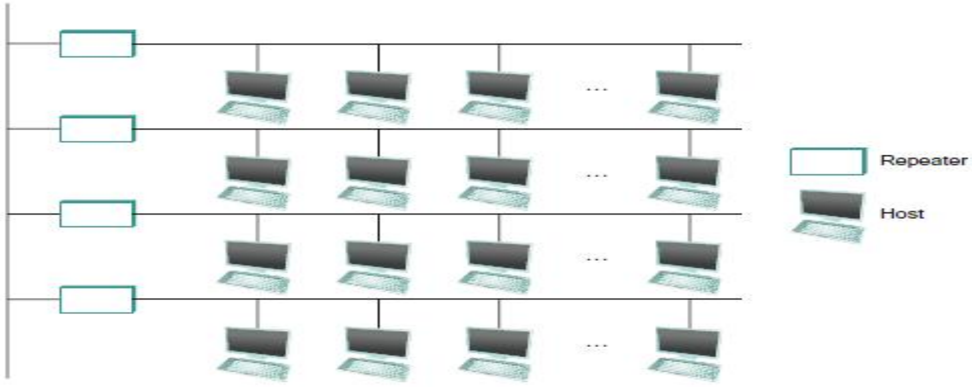


FIGURE 2.23 Ethernet repeater.

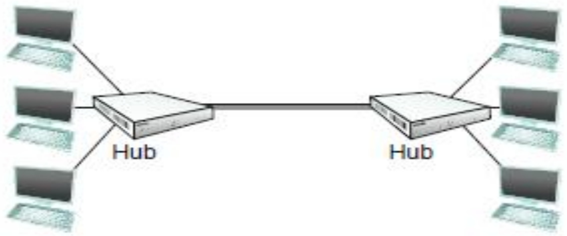


FIGURE 2.24 Ethernet hub.

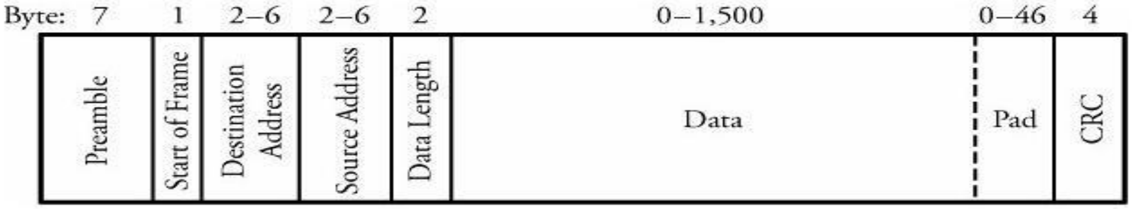
Access Protocol:

- The algorithm that controls access to the shared Ethernet link.
- This algorithm is commonly called the Ethernet’s media access control (MAC). It is typically implemented in hardware on the network adaptor.

Frame Format:

A brief description of the frame fields follows and is shown in the below figure.

- Preamble is 7 bytes and consists of a pattern of alternating 0s and 1s. This field is used to provide bit synchronization.
- Start of frame consists of a 10101011 pattern and indicates the start of the frame to the receiver.
- Destination address specifies the destination MAC address.
- Source address specifies the source MAC address.
- Length/Type specifies the frame size, in bytes. The maximum Ethernet frame
- size is 1,518 bytes.
- LLC data is data from the LLC layer.
- Pad is used to increase the frame length to the value required for collision detection to work.
- Frame check sequence is 32-bit CRC for error checking.



Ethernet IEEE 802.3 LAN frame

Address

- Each host on an Ethernet – has a unique Ethernet address.
- Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons.
- Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped.
- For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address as follows

  00001000 00000000 00101011 11100100 10110001 00000010
- Each frame transmitted on an Ethernet is received by every **adaptor** connected to that Ethernet.
- Each **adaptor** recognizes those frames addressed to its address and passes only those frames on to the host.

An Ethernet adaptor receives all frames and accepts

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode.

It passes to the host only the frames that it accepts.

Transmitter algorithm:

1-Persistent:

- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

P-Persistent:

- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.

In this method, after the station finds the line idle it follows these steps:

- With probability p, the station sends its frame.
- With probability q=1-p, the station waits for the beginning of the next time slot and checks the line again.
    - If the line is idle, it goes to step 1.
    - If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

9. Discuss the functioning (Key requirements) of wireless LAN in detail. (May 2015, Nov 2015) May 2016

Wireless technologies differ from wired links in some important ways, while at the same time sharing many common properties. Like wired links, issues of bit errors are of great concern—typically even more so due to the unpredictable noise environment of most wireless links. Framing and reliability also have to be addressed.

Unlike wired links, power is a big issue for wireless, especially because wireless links are often used by small mobile devices (like phones and sensors) that have limited access to power (e.g., a small battery). Furthermore, you can't go blasting away at arbitrarily high power with a radio transmitter—there are concerns about interference with other devices and usually regulations about how much power a device may emit at any given frequency.

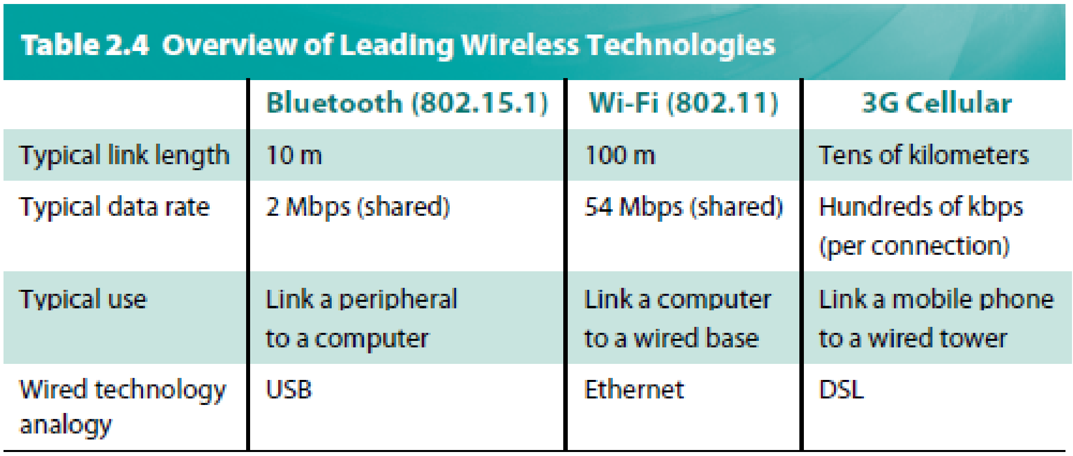


Table 2.4 Overview of Leading Wireless Technologies

	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

Introduction IEEE has defined the specification for the wireless LAN called IEEE 802.11, which covers the physical and Data Link Layers.

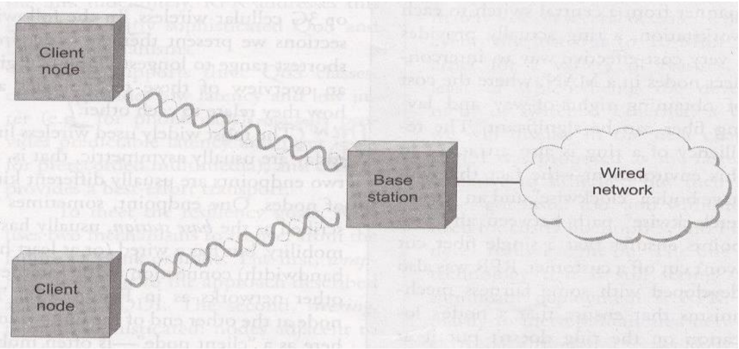
Architecture

IEEE 802.11 standard defines 2 kinds of services.

1. The basic service set (BSS)
2. The extended service set (ESS)

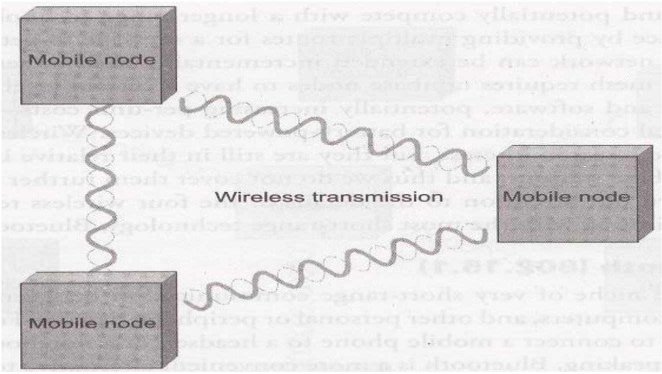
1) Basic Service Set (BSS):

A BSS is made of stationary (immobile) or mobile wireless stations and a possible central base station known as the access point AP.



Mesh or ad hoc network

The BSS without an AP is stand alone network and cannot send data to other BSS. It is called an ad hoc architecture.



2) Extended Service Set (ESS):

An ESS is made up of two or more BSS with AP. The BSS are connected through a distribution system, which is usually a wired LAN.

An ESS uses two types of stations mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of the wired LAN. When BSS are connected, the network is called an infrastructure network. In this the stations within reach of one another can communicate without the use of an AP. But communication between two stations in two different BSS usually occurs via two AP's.

Station Types

Three qualitatively different levels of mobility in a wireless LAN.

1. No transmission
2. BSS transition
3. ESS transition

1) No transmission:

The first level is no mobility, such as when a receiver must be in a fixed location to receive a directional transmission form the base station of a single BSS.

2) BSS transition:

It is defined as a station movement from one BSS to another BSS within the same ESS (Bluetooth).

3) ESS transition

It is defined as a station movement from a BSS in one ESS to a BSS with in another ESS. The third level is mobility between bases, as is the case with cell phones and Wi-Fi.

10. Discuss IEEE 802.11 (or) WI-FI in detail (or) MAC layer functions in IEEE802.11 (May 2015, 2016, 2017)(Dec 2017)

802.11 is designed for use in a limited geographical area (homes, office buildings, campuses), and its primary challenge is to mediate access to a shared communication medium—in this case, signals propagating through space.

Physical properties

IEEE 802.11 defines the specification for the conversion of bits to a signal in the physical layer. The IEEE 802.11 physical layer is of four types.

1. **Frequency-hopping spread spectrum (FHSS):** It is a method in which the sender sends one carrier frequency for a short amount of time, and then hops to another carrier frequency for the same amount of time, hops again to still another same amount of time and so on.

This technique makes use of 79 channels. FHSS operates in the 2.4 GHz ISM band and supports data rates of 1 Mb/s to 2 Mb/s.

   1. If the band width of the original signal is B, the allocated spread spectrum bandwidth is N X B.
   2. The amount of time spent at each sub band is called the dwell time.

2. **Direct-sequence spread spectrum (DSSS):** It uses seven channels, each supporting data rates of 1 Mb/s to 2 Mb/s. The operating frequency range is 2.4 GHz ISM band.

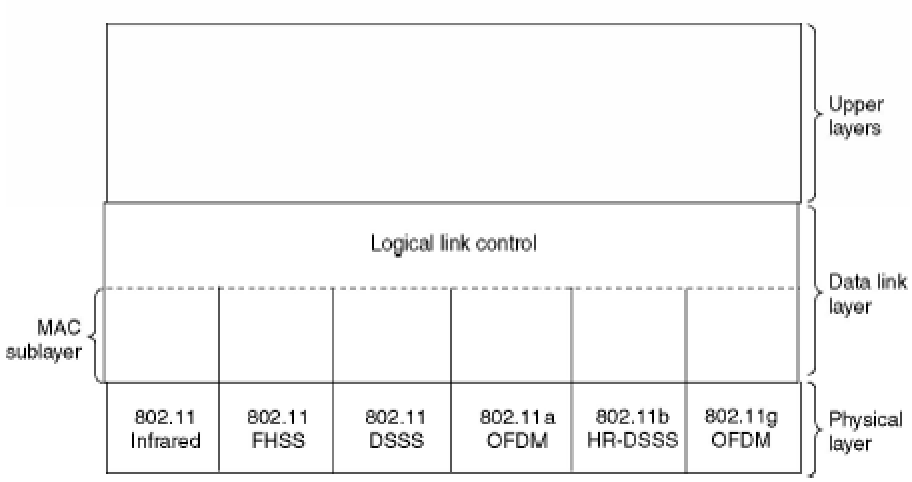
In DSSS each bit by the sender is a replaced by the sequence of bits called chip code. To avoid buffering, the time needed to send one chip code must be the same as the time needed to send one original bit.

3. **IEEE 802.11a**: Orthogonal frequency division multiplexing (OFDM): IEEE 802.11a uses OFDM, which uses 12 orthogonal channels in the 5 GHz range. All the sub bands are used by one source at a given time. The common data rates are 18 Mbps and 54 Mbps.

4. **IEEE 802.11b**: High Rate Direct-Sequence spread spectrum (HRDSSS): IEEE 802.11b operates in the 2.4 GHz band and supports data rates of 5.5 Mb/s to 11 Mb/s. It is similar to DSSS except for the encoding method which is called complementary code keying (CCK). CCK encodes four or eight bits to one CCK symbol.

5. **IEEE 802.11g**: (OFDM): IEEE 802.11g operates at 2.4 GHz and supports even higher data rates.

Protocol Stack



IEEE 802.11 MAC Layer (May 2015)

IEEE 802.11 provides several key functionalities: reliable data delivery, media access control, and security features.

The MAC layer consists of two sub layers:

1. The distributed-coordination function algorithm (DCF) and
2. The point-coordination function algorithm (PCF).

1) Point Coordination Function (PCF) Algorithm

The point-coordination function (PCF) provides a contention-free service. PCF is an optional feature in IEEE 802.11 and is built on top of the DCF layer to provide centralized media access.

2) Distributed Coordination Function (DCF) Algorithm

The DCF algorithm uses contention resolution, and its sublayer implements the CSMA scheme for media access control and contention resolution.

Begin DCF Algorithm for Wireless 802.11 MAC – **MACA (NOV/DEC 2014)**

1. The sender senses the medium for any ongoing traffic.

2. If the medium is idle, the sender waits for a time interval equal to IFS. Then the sender senses the medium again. If the medium is still idle, the sender transmits the frame immediately.
   1. After the station is found ideal, the station waits for a period of time, called the distributed inter-frame space (DIFS).

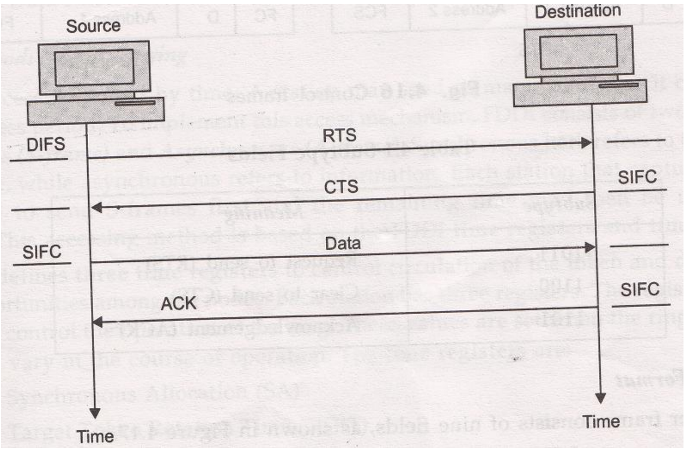
3. The station sends a control frame called the request to send (RTS).After receiving the RTS and waiting a short period called the short inter-frame space (SIFS), the destination station sends a control frame called clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

Two or more stations made try to send RTS frames at the same time, these control frames may collide. The sender assumes there has been a collision if it has not received CTS frame from the receiver and it tries again.

4. The source station sends data after waiting an amount of time equal to SIFS.

5. The destination station after waiting for an amount of time equal to SIFS sends and acknowledgement to show that the frame has been received.

6. When a station sends an RTS frame, it includes the duration of the time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a Network Allocation Vector (NAV) that all shows how much time must pass before these stations are allowed to check the channel for idleness.



MACAW (NOV/DEC 2014)

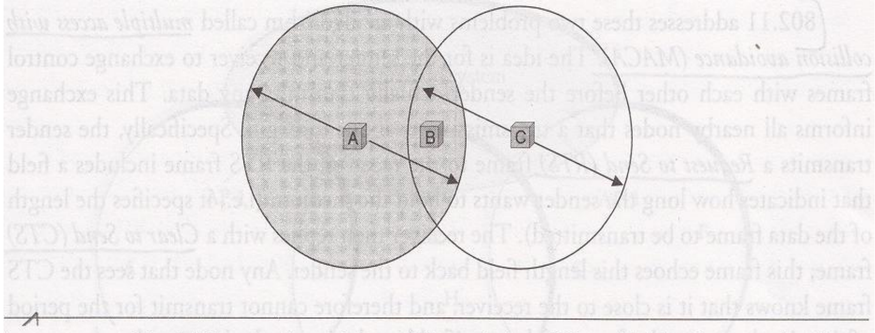
WLAN data transmission collisions can still happen, and MACA for Wireless (MACAW) is brought to extend the functionality of MACA. It demands nodes to send acknowledgments after every successful frame transmission. MACAW is commonly used in ad hoc networks. Moreover, it is the basis of various other MAC protocols found in wireless sensor networks (WSN).

Collision Avoidance:

- ✓ **Hidden node problem**
- ✓ **Exposed node problem**

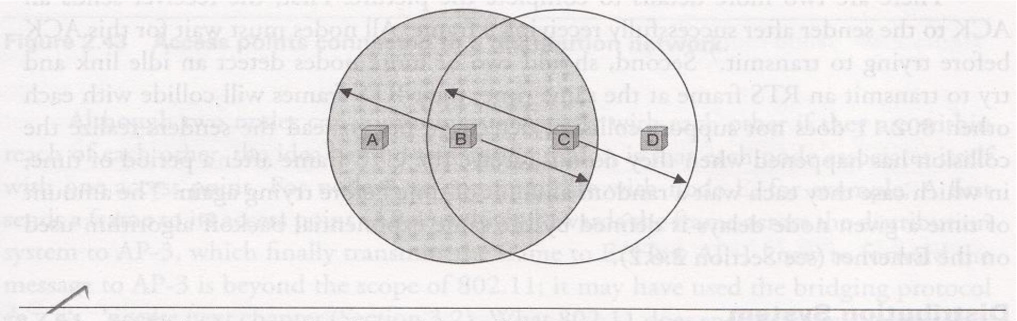
- A wireless protocol would follow the same algorithm as the Ethernet – wait until the link becomes idle before transmitting and back off should a collision occur – and to a first approximation, this is what 802.11 does.
- Consider the situation depicted in the below figure, where A and C are both within range of B but not each other.
- Suppose both A and C want to communicate with B and so they each send it a frame.
- A and C are unaware of each other since their signals do not carry that far.

- These two frames collide with each other at B, but unlike an Ethernet, neither A nor C is aware of this collision.
- A and C are said to be **hidden nodes** with respect to each other.



The hidden node problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)

- A related problem, called the **exposed node problem**, occurs under the circumstances illustrated in the below figure, where each of the four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.
- For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A.



The exposed node problem. Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A's and D's reaches are not shown.)

Distribution system

Some nodes are allowed to roam (e.g., your laptop) and some are connected to a wired network infrastructure. 802.11 calls these base stations *access points* (APs), and they are connected to each other by a so-called *distribution system*. Figure 2.32 illustrates a distribution system that connects three access points, each of which services the nodes in some region. Each access point operates on some channel in the appropriate frequency range, and each AP will typically be on a different channel than its neighbors

Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is that each node associates itself with one access point.

For node A to communicate with node E, for example, A first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E. How AP-1 knew to forward the message to AP-3 is beyond the scope of 802.11; it may have used the bridging protocol described in the next chapter (Section 3.1.4). What 802.11 does specify is how nodes select their access points and, more interestingly, how this algorithm works in light of nodes moving from one cell to another.

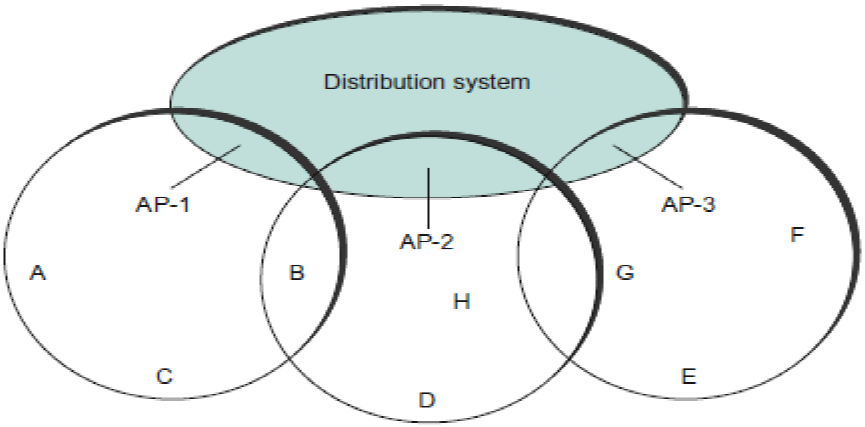


FIGURE 2.32 Access points connected to a distribution system.

The technique for selecting an AP is called *scanning* and involves the following four steps:

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

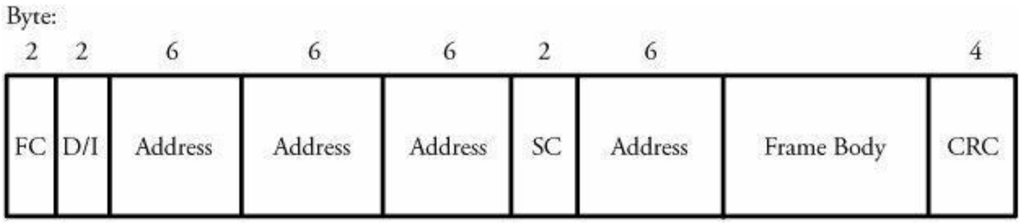
MAC Frame

The three frame types in IEEE 802.11 are control frames, data-carrying frames, and management frames.

The frame format for the 802.11 MAC is shown in the below diagram and is described as follows.

- The frame control (FC) field provides information on the type of frame: control frame, data frame, or management frame.
- Duration/connection ID (D/I) refers to the time allotted for the successful transmission of the frame.
- The addresses field denotes the 6-byte source and destination address fields.
- The sequence control (SC) field consists of 4 bits reserved for fragmentation and reassembly and 12 bits for a sequence number of frames between a particular transmitter and receiver.
- The frame body field contains a MAC service data unit or control information.
- The cyclic redundancy check (CRC) field is used for error detection.

IEEE 802.11 MAC frame



Byte: 2	2	6	6	6	2	6		4
FC	D/I	Address	Address	Address	SC	Address	Frame Body	CRC

Control frames ensure reliable data delivery. The control frames are used for accessing the channel and acknowledgement frames. It consist of

FC	D	Address 1	Address 2	FCS

RTS

FC	D	Address 1	FCS

CTS or ACK

Management frames are used to monitor and manage communication among various users in the IEEE 802.11 LAN through access points.

11. Briefly discuss Bluetooth (IEEE 802.15.1) (Dec 2017)

Introduction

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English.

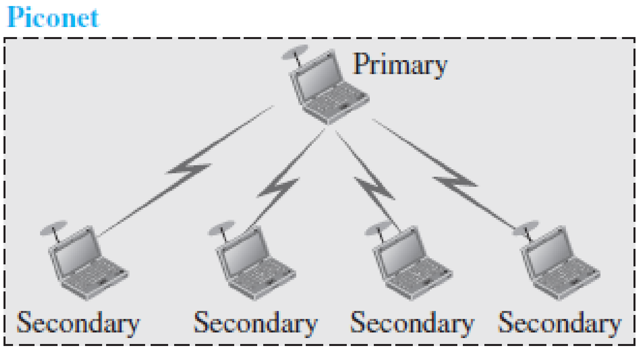
Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture

Bluetooth defines two types of networks: **piconet and scatternet.**

- ***Piconets***

Figure 15.17 *Piconet*



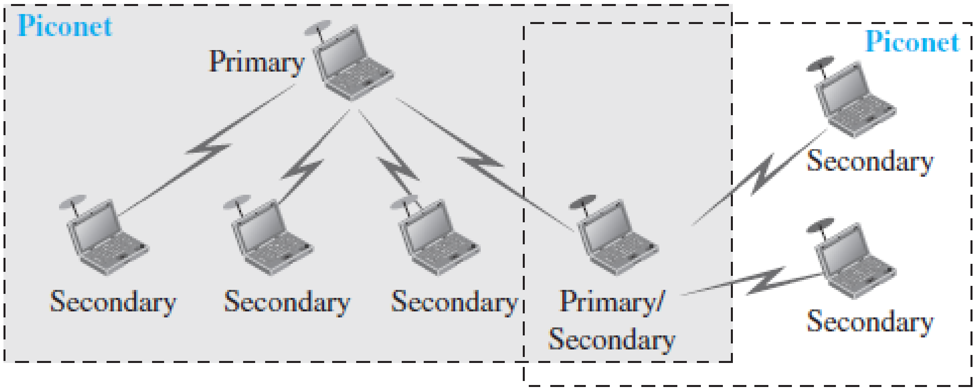
A Bluetooth network is called a ***piconet,*** or a small net. A piconet can have up to eight stations, one of which is called the *primary;* the rest are called *secondaries.* All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and secondary stations can be one-to-one or one-to-many. Figure 15.17 shows a piconet.

Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state*. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

- ***Scatternet***

Piconets can be combined to form what is called a ***scatternet.*** A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure 15.18 illustrates a scatternet.

Figure 15.18 *Scatternet*



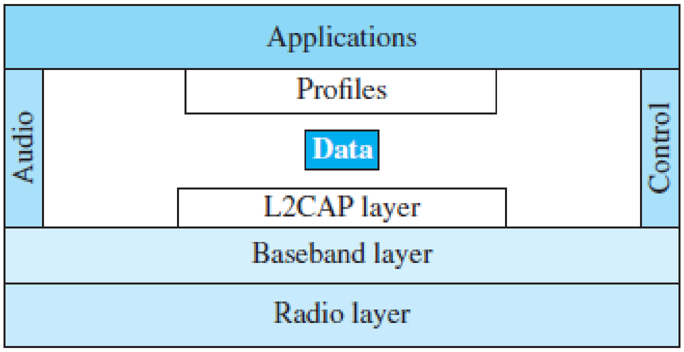
Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet model we have defined in this book. Figure 15.19 shows these layers.

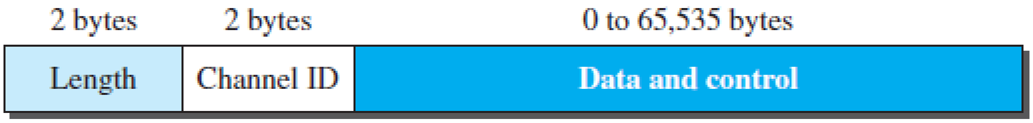
Figure 15.19 *Bluetooth layers*



L2CAP

The **Logical Link Control and Adaptation Protocol,** or **L2CAP** (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCO channels do not use L2CAP. Figure 15.20 shows the format of the data packet at this level.

Figure 15.20 *L2CAP data packet format*

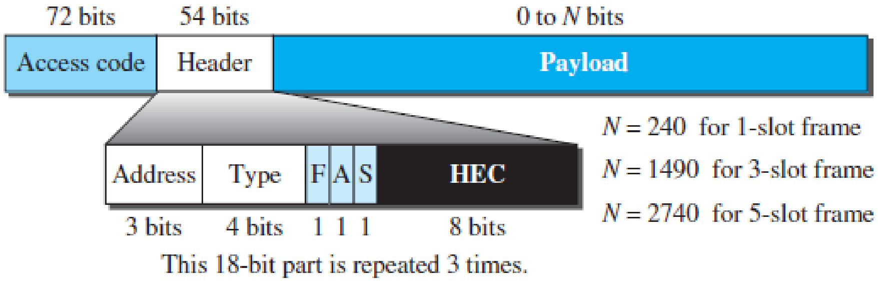


Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA

Frame Format

Figure 15.23 *Frame format types*


72 bits
54 bits
0 to N bits
Access code
Header
Payload
$N = 240$ for 1-slot frame
$N = 1490$ for 3-slot frame
$N = 2740$ for 5-slot frame
Address
Type
F
A
S
HEC
3 bits
4 bits
1 1 1
8 bits
This 18-bit part is repeated 3 times.

Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

Bluetooth uses the **frequency-hopping spread spectrum (FHSS)** method in the physical layer to avoid interference from other devices or other networks

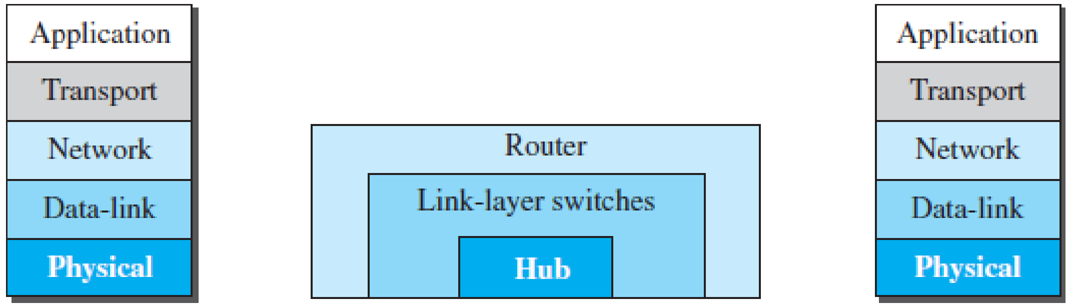
Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK

12. Explain in detail about connecting devices in network

Hosts and networks do not normally operate in isolation. We use **connecting devices** to connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model. We discuss three kinds of *connecting devices*: **hubs, link-layer switches, and routers**. Hubs today operate in the first layer of the Internet model. Link-layer switches operate in the first two layers. Routers operate in the first three layers

Figure 17.1 *Three categories of connecting devices*



Hubs

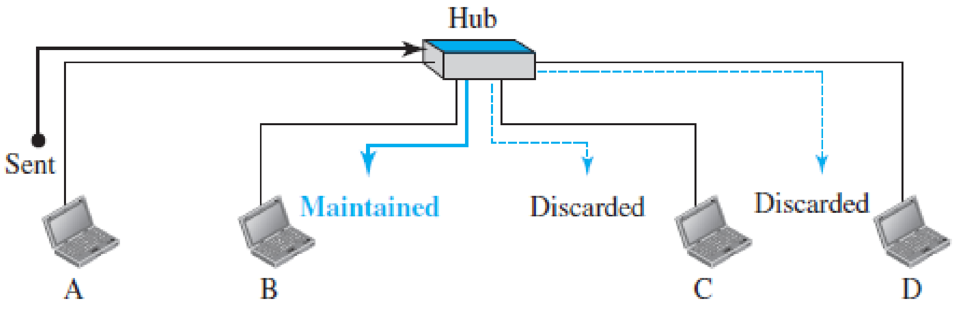
A **hub** is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A **repeater** receives a signal and, before it becomes too weak or corrupted, *regenerates* and *retimes* the original bit pattern.

The repeater then sends the refreshed signal. In the past, when Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable. Today, however, Ethernet LANs use star topology. In a star topology, a repeater is a multiport device, often called a *hub*, that can be used to serve as the connecting point and at the same time function as a repeater.

Figure 17.2 shows that when a packet from station A to station B arrives at the hub, the signal representing the frame is regenerated to remove any possible corrupting noise, but the hub forwards the packet from all outgoing ports except the one from which the signal was received. In other words, the frame is broadcast. All stations in the LAN receive the frame, but only station B keeps it. The rest of the stations discard it.

Figure 17.2 shows the role of a repeater or a hub in a switched LAN. The figure definitely shows that a hub does not have a filtering capability; it does not have the intelligence to find from which port the frame should be sent out. A hub or a repeater is a physical-layer device. They do not have a link-layer address and they do not check the link-layer address of the received frame. They just regenerate the corrupted bits and send them out from every port.

Figure 17.2 *A hub*



Link-Layer Switches

Introduction

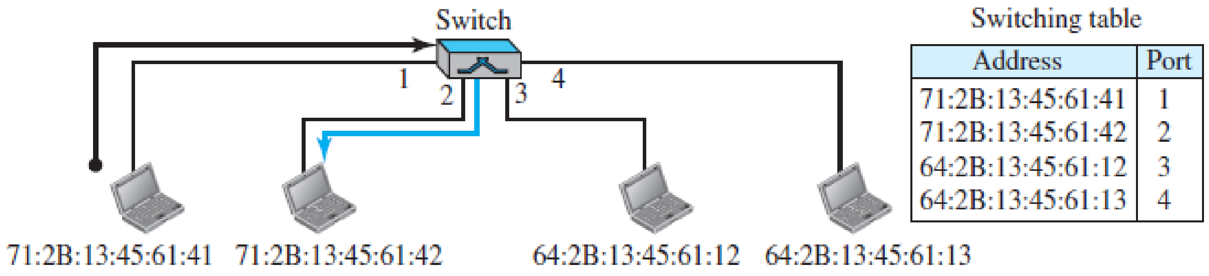
- A switch is a combination of a hub and a bridge.
- It can interconnect two or more workstations, but like a bridge, it observes traffic flow and learns.
- When a frame arrives at a switch, the switch examines the destination address and forwards the frame out the one necessary connection.
    1. Workstations that connect to a hub are on a *shared segment*.
    2. Workstations that connect to a switch are on a *switched segment*.
- The backplane of a switch is fast enough to support multiple data transfers at one time.
- A switch that employs a *cut-through architecture* is one that passes on the frame before the entire frame has arrived at the switch.
- Multiple workstations connected to a switch use dedicated segments. This is a very efficient way to isolate heavy users from the network.
- A switch can allow simultaneous access to multiple servers, or multiple simultaneous connections to a single server.

A **link-layer switch** (or ***switch***) operates in both the physical and the data-link layers. As a physical-layer device, it regenerates the signal it receives. As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

Filtering

One may ask what the difference in functionality is between a link-layer switch and hub. A link-layer switch has **filtering** capability. It can check the destination address of a frame and can decide from which outgoing port the frame should be sent.

Figure 17.3 *Link-layer switch*



Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

Transparent Switches

A **transparent switch** is a switch in which the stations are completely unaware of the switch's existence. If a switch is added or deleted from the system, reconfiguration of the stations is unnecessary. According to the IEEE 802.1d specification, a system equipped with transparent switches must meet three criteria:

❑ Frames must be forwarded from one station to another.
❑ The forwarding table is automatically made by learning frame movements in the network.
❑ Loops in the system must be prevented

Major role of Switches

- Isolating traffic patterns and providing multiple accesses.
- This design is usually done by the network manager.

Switches are easy to install and have components that are hot-swappable.

Advantages of switches

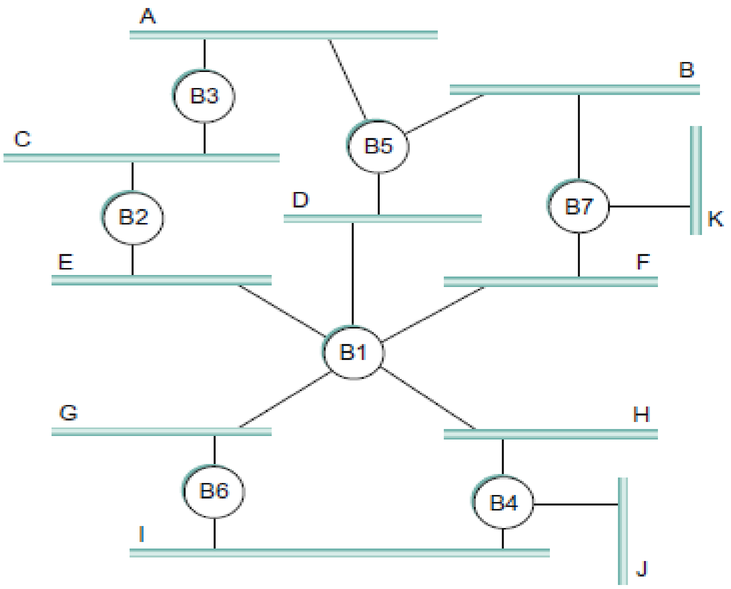
1. Switches divide a network into several isolated channels or collision domains
2. Reduce the possibility of collision
3. Each channel has its own network capacity
4. Connecting Heterogenous Devices

Limitations of switches

1. Although contains buffers to accommodate bursts of traffic, can become overwhelmed by heavy traffic
2. Device cannot detect collision when buffer full
3. Some higher level protocols do not detect error

<u>Spanning Tree Algorithm</u>

The preceding strategy works just fine until the extended LAN has a loop in it, in which case it fails in a horrible way—frames potentially loop through the extended LAN forever.



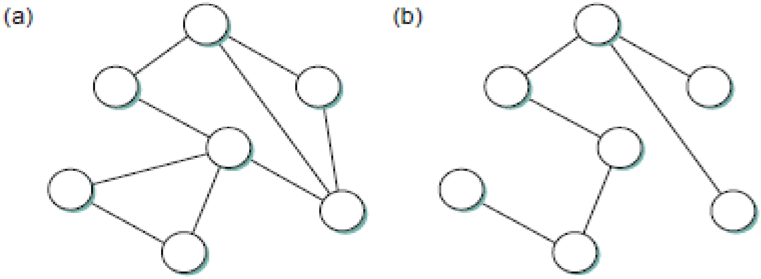
■ FIGURE 3.10 Extended LAN with loops.

This is easy to see in the example depicted in Figure 3.10, where, for example, bridges B1, B4, and B6 form a loop.
Whatever the cause, bridges must be able to correctly handle loops.

This problem is addressed by having the bridges run a distributed *spanning tree* algorithm.

If you think of the extended LAN as being represented by a graph that possibly has loops (cycles), then a spanning tree is a subgraph of this graph that covers (spans) all the vertices but contains no cycles. That is, a spanning tree keeps all of the vertices of the original graph but throws out some of the edges. For example, Figure 3.11 shows a cyclic graph on the left and one of possibly many spanning trees on the right.

The idea of a spanning tree is simple enough: It's a subset of the actual network topology that has no loops and that reaches all the LANs in the extended LAN. The hard part is how all of the bridges coordinate their decisions to arrive at a single view of the spanning tree. After all, one topology is typically able to be covered by multiple spanning trees. The answer lies in the spanning tree protocol.



■ FIGURE 3.11 Example of (a) a cyclic graph; (b) a corresponding spanning tree.

The main idea of the spanning tree is for the bridges to select the ports over which they will forward frames.

The algorithm selects ports as follows.

- Each bridge has a unique identifier; for our purposes, we use the labels B1, B2, B3, and so on.
- The algorithm first elects the bridge with the smallest ID as the root of the spanning tree;
- Next, each bridge computes the shortest path to the root and notes which of its ports is on this path.
- Finally, all the bridges connected to a given LAN elect a single *designated* bridge that will be responsible for forwarding frames toward the root bridge

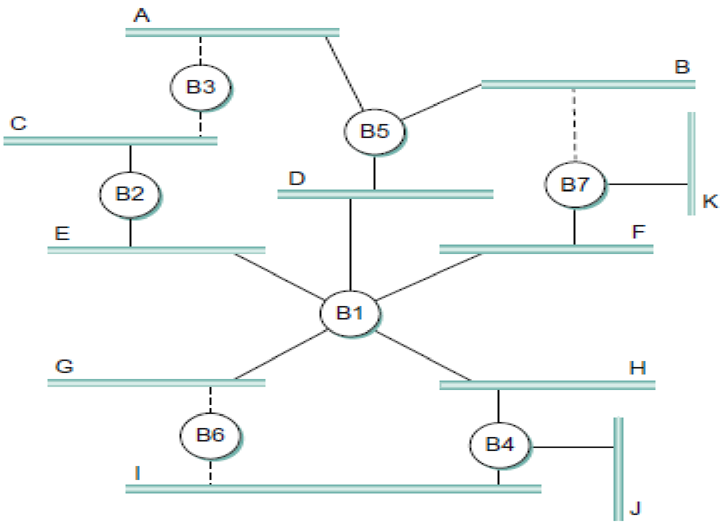


FIGURE 3.12 Spanning tree with some ports not selected.

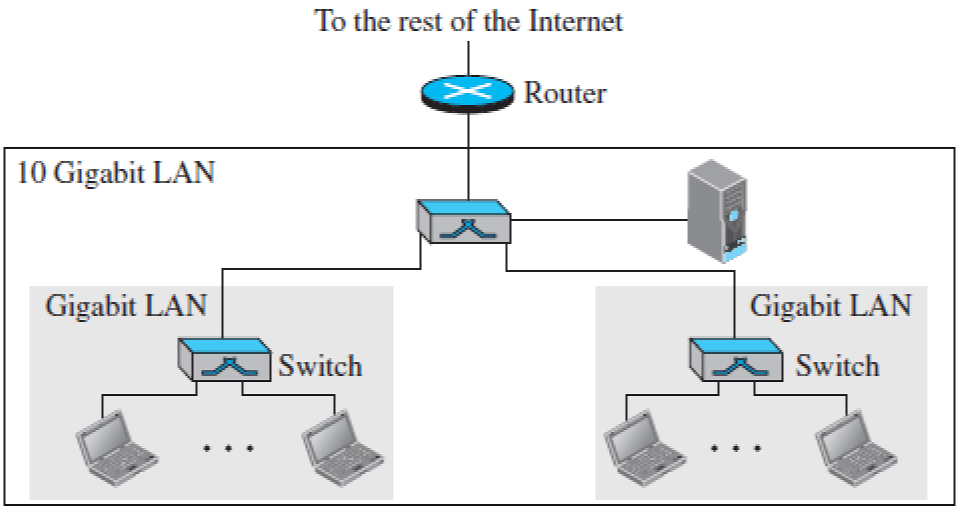
Routers

A **router** is a three-layer device; it operates in the physical, data-link, and network layers. As a physical-layer device, it regenerates the signal it receives. As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet. As a network-layer device, a router checks the network-layer addresses.

A router can connect networks. In other words, a router is an internetworking device; it connects independent networks to form an internetwork. According to this definition, two networks connected by a router become an internetwork or an internet. There are three major differences between a router and a repeater or a switch.
1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.
3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.

Let us give an example. In Figure 17.9, assume an organization has two separate buildings with a Gigabit Ethernet LAN installed in each building. The organization uses switches in each LAN. The two LANs can be connected to form a larger LAN using 10 Gigabit Ethernet technology that speeds up the connection to the Ethernet and the connection to the organization server. A router then can connect the whole system to the Internet.

Figure 17.9 *Routing example*



UNIVERSITY QUESTIONS

B.E/B.TECH NOVEMBER/DECEMBER 2014 (2008 Regulation)

2 MARKS

1. Differentiate persistent and non persistent CSMA (Q.NO. 41)
2. State the uses of valid transmission timer (Q.NO. 42)

16 MARKS

1.Explain and differentiate FDDI and Ethernet (16) (Q.NO. 2,13 & 14)

2.Write short notes on.

(i)Transparent bridges (8) (Q.NO. 6)

(ii)MACA and MACAW (8) (Q.NO. 4)

B.E/B.Tech April May 2015

2 MARKS

1. What do you understand by CSMA protocol? (Q.NO. 43)
2. List the functions of bridges (Q.NO. 44)

16 MARKS

1. Explain in detail about access method and frame format used in Ethernet and token ring (16) (Q.NO. 2 & 16)

2. (i) Discuss the MAC layer functions of IEEE802.11 (8) (Q.NO. 4)

(ii) Briefly define key requirements of wireless LAN (8) (Q.NO. 3)

B.E/B.Tech Nov-Dec 2015

2 MARKS

1. Define sub-netting. (Q.NO 28)
2. What is the need of ARP? (Q.NO 36)
3. Identify the class of the following IP address: (a) 110.34.56.45 (b) 212.208.63.23 (Q.NO 47)

16 MARKS

1. Write short notes on Ethernet & Wireless LAN (8+8) (Q.NO 2 & 3)
2. Explain in detail ARP, DHCP, ICMP (16) (Q.NO 8, 9 & 10)

B.E/B.Tech April-May 2016

2 MARKS

1. Define hidden node problem. (Q.NO 45)
2. What is Bluetooth? (Q.NO 7)
3. Expand ICMP and write the function (Q.NO 27)

16 MARKS

1. Give the comparison between different wireless technologies? Enumerate 802.11 protocol stack in detail (16) (Q.NO 3 & 4)
2. Write short notes on DHCP & ICMP (8+8) (Q.NO 9 & 10)

B.E/B.Tech Nov-Dec 2016

2 MARKS

1. What is meant by exponential backoff? (Q.NO 5)
2. What is scatternet? (Q.NO 46)
3. What is fragmentation and reassembly? (Q.NO 48)

16 MARKS

1. Explain the physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver and adapter (16) (Q.NO 2)
2. With a neat sketch explain about IP service model,packet format,Fragmentation and reassembly.(16) (Q.NO 11)

B.E/B.Tech April-May 2017

PART A

1. State the functions of bridges. (Q.NO 44)
2. When is ICMP redirect message used? (Q.NO 49)

PART B

1.i) Discuss the working of CSMA/CD protocol (6) (Q.NO 15)

ii) Explain the functions of MAC layer present in IEEE802.11 with necessary diagrams (7) (Q.NO 4)

2. Explain the working of DHCP protocol with its header format (Q.NO 9)

B.E/B.Tech Nov-Dec 2017

PART A

1. Show the Ethernet frame format (Q.NO 37)
2. Highlights the characteristics of datagram networks (Q.NO 50)

PART B

1. Explain the functions of Wi-Fi & Bluetooth in detail (13) (Q.NO 4 & 5)
2. i)Explain the datagram forwarding in IP (Q.NO 11)
   ii)Show and explain the ARP packet format for mapping IP addresses into Ethernet addresses (Q.NO 8)

UNIT III - NETWORK LAYER

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

PART A

1. List the various services provided in the Network Layer.

- Packetizing
- Routing and Forwarding
- Other Services
  - *Error Control*
  - *Flow Control*
  - *Congestion Control*
  - *Quality of Service*
  - *Security*

2. Define packetizing.

- **Packetizing:** encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

3. Define Routing and Forwarding.

Routing

- The network layer is responsible for routing the packet from its source to the destination.

Forwarding

- *Forwarding* can be defined as the action applied by each router when a packet arrives at one of its interfaces.

4. Define packet switched network and list the different approaches to route the packet.

Packet Switched Network:

- Packet switching is used at the network layer because the unit of data at this layer is a packet.
- At the network layer, a message from the upper layer is divided into manageable packets and each packet is sent through the network.
- A packet-switched network can use two different approaches to route the packets:
  - The *datagram approach* - Connectionless Service
  - The *virtual circuit approach* - Connection-Oriented Service

5. Narrate how the performance of a network or network layer can be measured ?

- The performance of a network can be measured in terms of
  - *delay,*
    - transmission delay,
    - propagation delay,
    - processing delay,
    - queuing delay.
  - *throughput,*
  - *packet loss.*
  - *Congestion Control*

6. Define Transmission delay

- A sender needs to put the bits in a packet on the line one by one.
- The transmission delay is longer for a longer packet and shorter if the sender can transmit faster.
- In other words, the transmission delay is

$$\text{Delay}_{tr} = (\text{Packet length}) / (\text{Transmission rate}).$$

7.* Define *Propagation Delay

- Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.

$$\text{Delay}_{pg} = (\text{Distance}) / (\text{Propagation speed}).$$

8.* Define *Processing Delay

- The processing delay is the time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).

$$\text{Delay}_{pr} = \text{Time required to process a packet in a router or a destination host}$$

9. Queuing Delay

- The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output queue of a router.

$$\text{Delay}_{qu} = \text{The time a packet waits in input and output queues in a router}$$

10. Define Throughput.

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.

- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.

Throughput = minimum {TR1, TR2, . . . TRn}.

11. Define Congestion Control and mention its types.

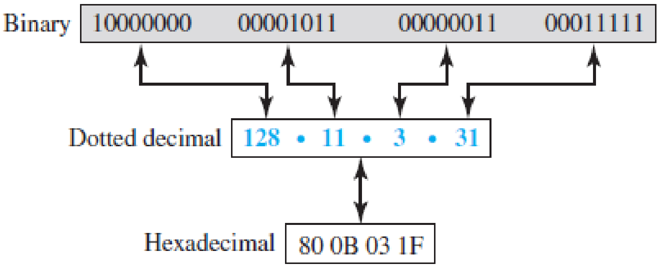
- Congestion control is a mechanism for improving performance.
- Two broad categories:
  - open-loop congestion control (prevention)
  - closed-loop congestion control (removal).

12. Define IPv4 Address and list the various types of notations.

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- IPv4 addresses are unique. If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

Notation

- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).



13. Define and Differentiate Classful and Classless Addressing.

Classful Addressing

- An IPv4 address was designed with a fixed-length prefix. The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as classful addressing.

Classless Addressing

- In addressing, the whole address space is divided into variable length classless blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- A prefix length ranges from 0 to 32.

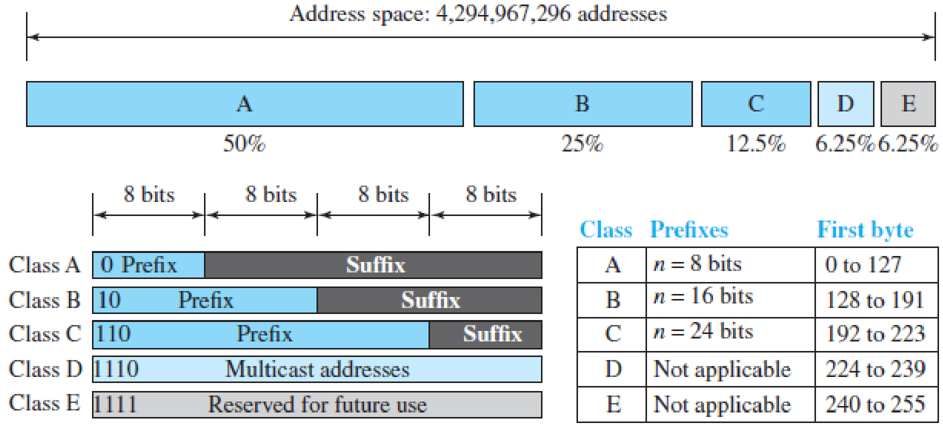
Difference between Classless Addressing and Classful Addressing

Classful Addressing	Classless Addressing
An IP Address allocation method that allocates IP addresses according to five major classes.	An IP Address allocation method that is designed to replace classful addressing to minimize the rapid exhaustion of IP addresses.
Less practical and useful.	More practical and useful.
Network ID and host ID changes depending on the classes.	There is no boundary on Network ID and host ID
Addresses have three parts: network, subnet, and host.	Addresses have two parts: subnet or prefix, and host.
IP forwarding process is restricted in how it uses the default route	IP forwarding process has no restrictions on using the default route
Routing protocol does not advertise masks nor support VLSM; RIP-1 and IGRP	Routing protocol does advertise masks and support VLSM; RIP-2, EIGRP, OSPF.

14. Define Address Masking.

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 − n) are set to 0s.
- To extract the information in a block, using the three bit-wise operations NOT, AND, and OR.
  1. The number of addresses in the block N = NOT (mask) + 1.
  2. The first address in the block = (Any address in the block) AND (mask).
  3. The last address in the block = (Any address in the block) OR [(NOT (mask)].

15. Specify the various types of Classes and its range in Classful Addressing.



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

16. A classless address is given as 167.199.170.82/27. Find the number of addresses, First address and last address of the block.

Solution:

- The **number of addresses** in the network is $2^{32} - n = 2^5$ = **32 addresses**.
- The **first address** can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

  Address:

  167.199.170.82/**27** 10100111 11000111 10101010 01010010

  First address:

  167.199.170.64/**27** 10100111 11000111 10101010 010**00000**
- The **last address** can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

  Address:

  167.199.170.82/**27** 10100111 11000111 10101010 01011111

  Last address:

  167.199.170.95/27 10100111 11000111 10101010 010**11111**

17. An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

Solution

- There are $2^{32} - {}^{24}$ = **256 addresses** in this block.
- The first address is **14.24.74.0/24**; the last address is **14.24.74.255/24**.

Subblock with 120 addresses:

- The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate **128 addresses**.
- The subnet mask for this subnet can be found as n1 = $32 - \log_2 128$ = **25**. The first address in this block is **14.24.74.0/25;** the last address is **14.24.74.127/25**.

Subblock with 60 addresses:

- The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate **64 addresses**.
- The subnet mask for this subnet can be found as n2 = $32 - \log_2 64$ = **26.**
- The first address in this block is **14.24.74.128/26**; the last address is **14.24.74.191/26**.

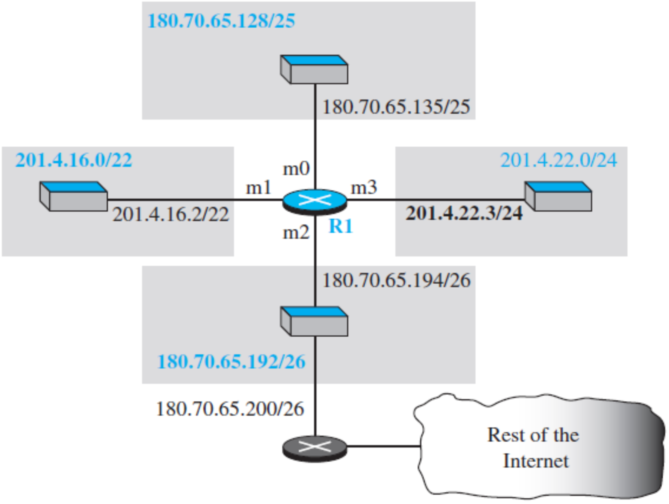
Subblock with 60 addresses:

- The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2 either. We allocate **16 addresses**.
- The subnet mask for this subnet can be found as n3 = $32 - \log_2 16$ = **28**.
- The first address in this block is **14.24.74.192/28**; the last address is

14.24.74.207/28.

- If we add all addresses in the previous subblocks, the result is **208** addresses. The first address in this range is **14.24.74.208**. The last address is **14.24.74.255**.

18. Make a forwarding table for router R1 using the configuration in Figure



Solution:

Network address/mask	*Next hop*	*Interface*
180.70.65.192/**26**	—	m2
180.70.65.128/**25**	—	m0
201.4.22.0/**24**	—	m3
201.4.16.0/**22**	—	m1
Default	180.70.65.200	m2

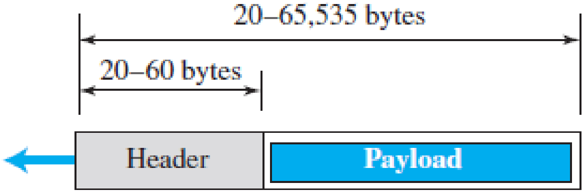
19. How the IP packets are forwarded?

FORWARDING OF IP PACKETS

- Forwarding Based on Destination Address
- Forwarding Based on Label

20. Define Datagram.

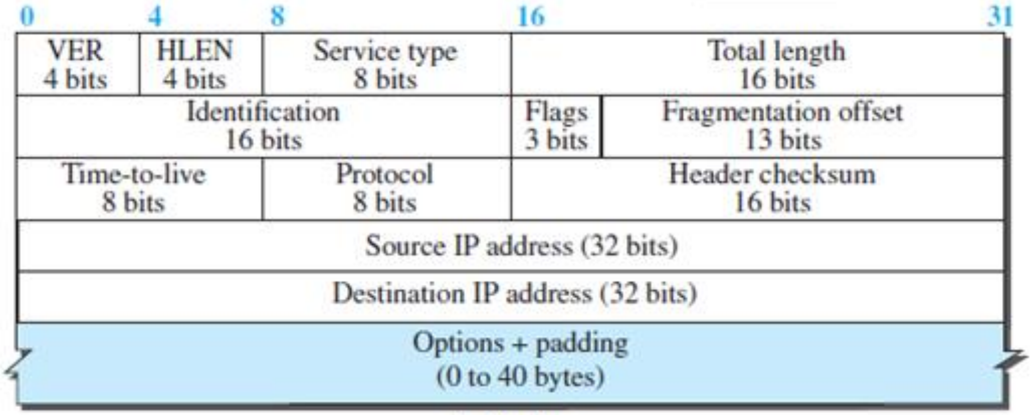
- Packets used by the IP are called *datagrams*.
- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



a. IP datagram

21. What is IPv4 and mention its IPv4 packet format.

- The Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.



b. Header

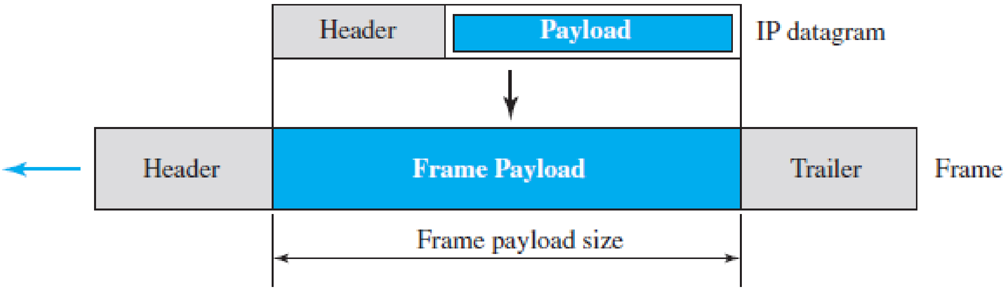
22. Define fragmentation and explain how it is performed.

➢ **Fragmentation**

- The division of a packet into smaller units to accommodate a protocol's MTU.

Maximum Transfer Unit (MTU)

- The largest size data unit a specific network can handle.



MTU: Maximum size of frame payload

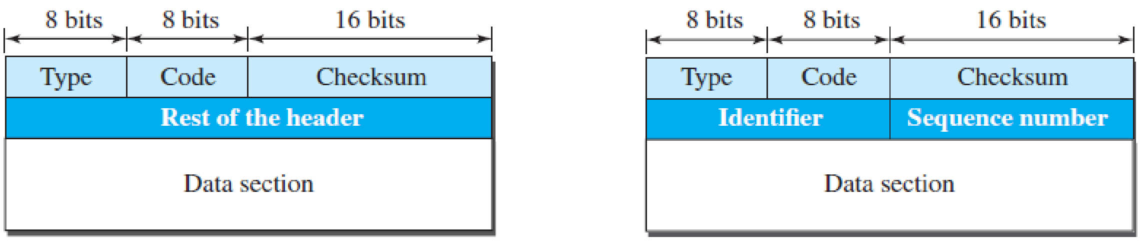
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.
- A datagram may be fragmented several times before it reaches the final destination.

23. Narrate the purpose of Internet Control Message Protocol version 4 (ICMPv4) message.

- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- ICMP is used to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them.

24. List the various ICMPv4 Error Messages.

- ICMP messages are divided into two broad categories: *error-reporting messages* and *query messages*



Error-reporting messages

Query messages

Type and code values

Error-reporting messages
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages
08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

25. List and define the two debugging tools used in ICMPv4 messages. Or Define Ping and Traceroute

- Two debugging tools: *ping* and *traceroute*.

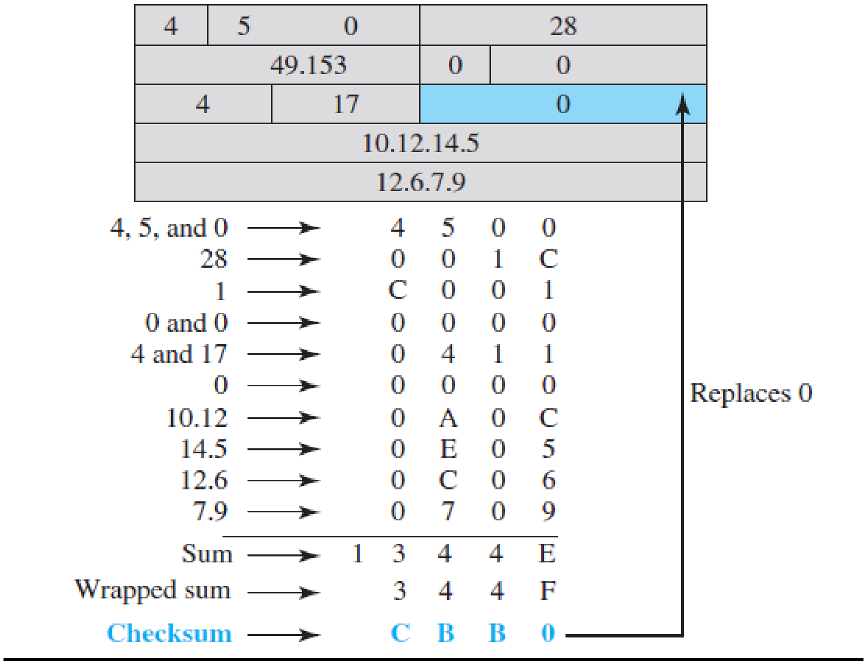
Ping

- *Ping* program is used to find if a host is alive and responding.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The ping program gets help from two query messages;

Traceroute or Tracert

- The *traceroute* program in UNIX or *tracert* in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The *traceroute* program gets help from two error-reporting messages: time-exceeded and destination-unreachable.

26. An example of a checksum calculation for an IPv4 header without options. The header is divided into 16-bit sections. All the sections are added and the sum is complemented after wrapping the leftmost digit. The result is inserted in the checksum field.



27. List the security issues practically applicable to IP Datagrams.

- There are three security issues that are particularly applicable to the IP protocol:
  - packet sniffing,
  - packet modification,
  - IP spoofing.

Packet Sniffing

- Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet.
- This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied.

Packet Modification

- The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.
- The receiver believes that the packet is coming from the original sender.
- This type of attack can be detected using a data integrity mechanism.

IP Spoofing

- An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.
- An attacker can send an IP packet to a bank pretending that it is coming from one of the customers.
- This type of attack can be prevented using an origin authentication mechanism

28. How IP packets are protected from various security issues.

IPSec

- The IP packets today can be protected from the security attacks using a protocol called IPSec (IP Security).

IPSec provides the following four services:

- *Defining Algorithms and Keys*.
- *Packet Encryption*.
- *Data Integrity*.
- *Origin Authentication*.

29. List the various routing algorithms or unicast routing algorithms in detail.

➢ **ROUTING ALGORITHMS**

- Distance-Vector Routing
- Link-State Routing
- Path-Vector Routing

30. Define *Bellman-Ford Equation*

- This equation is used to find the least cost (shortest distance) between a source node, ***x***, and a destination node, ***y***, through some intermediary nodes (**a, b, c,** . . .).
- The following shows the general case in which D***ij*** is the shortest distance and c***ij*** is the cost between nodes ***i*** and ***j***.

$$D_{xy} = \min\left\{(c_{xa} + D_{ay}), (c_{xb} + D_{by}), (c_{xc} + D_{cy}), \ldots\right\}$$

- In distance-vector routing, normally we want to update an existing least cost with a least cost through an intermediary node, such as ***z***, if the latter is shorter.

$$D_{xy} = \min\left\{D_{xy}, (c_{xz} + D_{zy})\right\}$$

31. Define Border Gateway Protocol (BGP)

- The Border Gateway Protocol version 4 (BGP4) is the only interdomain routing protocol, based on the path-vector algorithm.
- BGP allows routers to carry specific policies or constraints that they must meet.
- In BGP, two contributing (casual) routers can exchange routing information even if they are located in two different autonomous systems.

32. Write the keys for understanding the distance vector routing?

The three keys for understanding the algorithm are,

- Knowledge about the whole networks
- Routing only to neighbors
- Information sharing at regular intervals

33. Write the keys for understanding the link state routing?

The three keys for understanding the algorithm are,

- Knowledge about the neighborhood.
- Routing to all neighbors.
- Information sharing when there is a range.

34. How the packet cost referred in distance vector and link state routing?

- In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

35. What are the features in OSPF?

- Authentication of routing messages.
- Additional hierarchy.
- Load balancing.

36. Define Sub netting?

- Sub netting provides an elegantly simple way to reduce the total number of network numbers that are assigned.
- The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

37. What is DHCP? (NOV/DEC 2012)

- Dynamic Host Configuration Protocol (DHCP) is a protocol designed to provide information dynamically.
- It is a client-server program.
- DHCP is used to assign addresses to a host dynamically.
- Basically, DHCP server has two databases.
- The first database is addresses to IP addresses.

38. What are the salient features of IPV6? (NOV/DEC 2012)

- New Packet Format and Header
- Large Address Space
- State full and Stateless IPv6 address
- Multicast
- Integrated

37. What are the different routing techniques available to manage routing table entries?

1. Next hop routing.
2. Network specific routing
3. Host specific routing
4. Default routing

38. What is IPv6?

- **Internet Protocol version 6** (**IPv6**) is the latest revision of the Internet Protocol (IP), the communications that provides an identification and location system for computers on networks and routes traffic across the Internet.
- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

39. Discuss Congestion avoidance in network layer.

- Congestion occurs in a computer network when the resource demands exceed the capacity. Packets may be lost due to too much queuing in the network.
- During congestion, the network throughput may drop and the path delay may become very high.
- A congestion control scheme helps the network to recover from the congestion state.
- A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. Such schemes prevent a network from entering the congested state.
- Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism.

40. What is the need of sub netting? (NOV/DEC 2013& 2015)

- When we divide a network into several subnets, we have three levels of hierarchy
  - o The netid is the first level, defines the site.
  - o The subnetid is the 2nd level, defines the physical subnetwork.
  - o The hostid is the 3rd level defines the connection of the host to the subnetwork.

41. What is a hostid and netid?

- **Netid** – The portion of the IP address that identifies the network called the netid.
- **Hostid** – The portion of the IP address that identifies the host or router on the network is called the hostid.

42. What is the difference between boundary level masking and non-boundary level masking.

- **Boundary level Masking:**

  If the masking is at the boundary level, the mask numbers are either 255 or 0, finding the subnetwork address is very easy.
- **Non Boundary level Masking**

  If the masking is not at the boundary level, the mask numbers are not just 255 or 0, finding the subnetwork address involves using the bitwise AND operators.

43. How does a router differ from a bridge?

- Routers provide links between two separate but same type LANs and are most active at the network layer.
- Whereas bridges utilize addressing protocols and can affect the flow control of a single LAN; most active at the data link layer.

44. Identify the class and default subnet mask of the IP address 217.65.10.7.

It belongs to class C.

Default subnet mask – 255.255.255.192

45. What is the time to live field in IP header?

- Time to live field is counter used to limit packet lifetimes counts in second and default value is 255 sec.

46. What are the main disadvantages of distance vector routing?

1. Split horizon
2. Count to infinity problem

47. What are the desirable properties of a routing algorithms?

1. Correctness
2. Simplicity
3. Robustness
4. Stability
5. Fairness
6. Optimality

PART B

1. Explain in detail about Network Layer Services.

➢ **Packetizing**

- **Packetizing:** encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.
- The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and some other information that is required by the network-layer protocol and delivers the packet to the data-link layer.
- The destination host receives the network-layer packet from its data-link layer, decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.

- The routers in the path are not allowed to decapsulate the packets they received unless the packets need to be fragmented.
- The routers are not allowed to change source and destination addresses either.

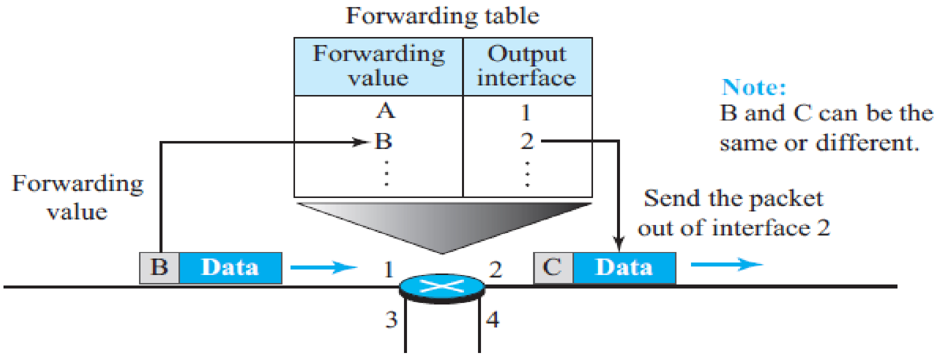
➢ **Routing and Forwarding**

Routing

- The network layer is responsible for routing the packet from its source to the destination.
- A physical network is a combination of networks (LANs and WANs) and routers that connect them.
- The network layer is responsible for finding the best one among these possible routes.

Forwarding

- *Forwarding* can be defined as the action applied by each router when a packet arrives at one of its interfaces.
- The decision-making table a router normally uses for applying this action is sometimes called the *forwarding table* and sometimes the *routing table*.
- When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network or to some attached networks.



Forwarding table

Forwarding value	Output interface
A	1
B	2
⋮	⋮

Note:
B and C can be the same or different.
Forwarding value
Send the packet out of interface 2
B
Data
C
Data
1
2
3
4

➢ **Other Services**

1. ***Error Control***

- The designers of the network layer, however, have added a checksum field to the datagram to control any corruption in the header, but not in the whole datagram.
- This checksum may prevent any changes or corruptions in the header of the datagram.
- The Internet uses an auxiliary protocol, ICMP, that provides some kind of error control if the datagram is discarded or has some unknown information in the header.

2. ***Flow Control***

- Flow control regulates the amount of data a source can send without overwhelming the receiver.
- To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data.
- The network layer in the Internet, however, does not directly provide any flow control.
-

3. ***Congestion Control***
   - Another issue in a network-layer protocol is congestion control. Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet.
   - Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.
   - If the congestion continues, sometimes a situation may reach a point where the system collapses and no datagrams are delivered.
4. ***Quality of Service***
   - As the Internet has allowed new applications such as multimedia communication, the quality of service (QoS) of the communication has become more and more important.
5. ***Security***
   - The network layer was designed with no security provision.
   - To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service. This virtual layer, called IPSec.

.

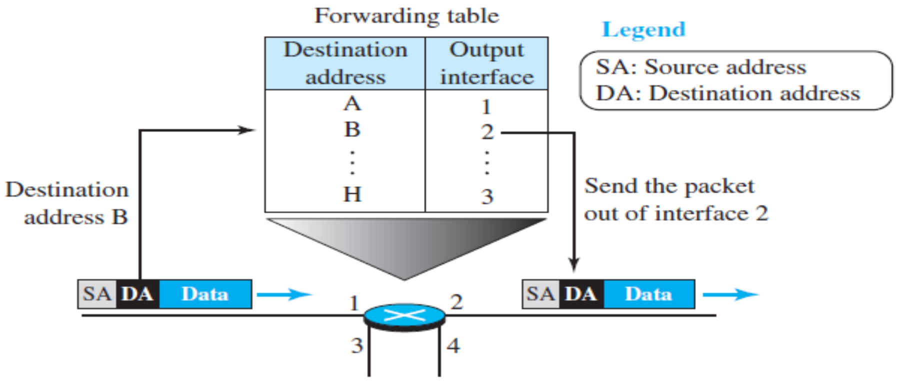
2. Explain in detail about Packet Switching in Network Layer.

➢ **PACKET SWITCHING**

- Packet switching is used at the network layer because the unit of data at this layer is a packet.
- At the network layer, a message from the upper layer is divided into manageable packets and each packet is sent through the network.
- A packet-switched network can use two different approaches to route the packets: the *datagram approach* and the *virtual circuit approach*

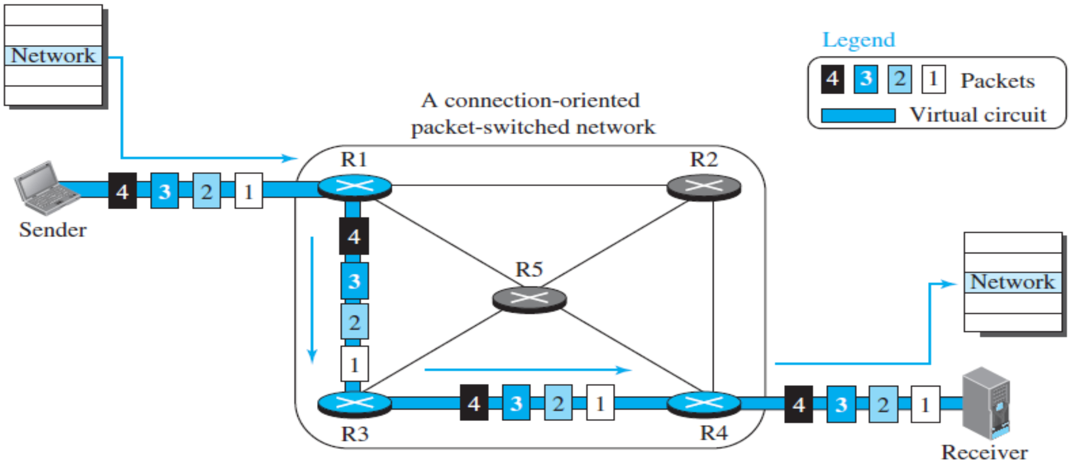
➢ **Datagram Approach: Connectionless Service**

- The network layer was designed to provide a connectionless service in which the network-layer protocol treats each packet independently.
- The network layer is only responsible for delivery of packets from the source to the destination. The switches in this type of network are called *routers*.
- Each packet is routed based on the information contained in its header: source and destination addresses.
- The destination address defines where it should go; the source address defines where it comes from.



➢ **Virtual-Circuit Approach: Connection-Oriented Service**

- In a connection-oriented service (also called *virtual-circuit approach*), there is a relationship between all packets belonging to a message.
- Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams.
- After connection setup, the datagrams can all follow the same path.
- In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.

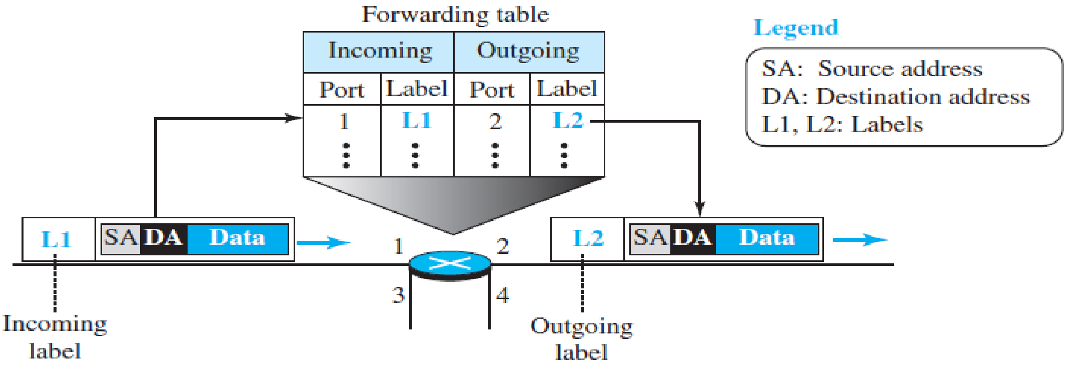


To create a connection-oriented service, a three-phase process is used:

- setup,
- data transfer
- teardown.

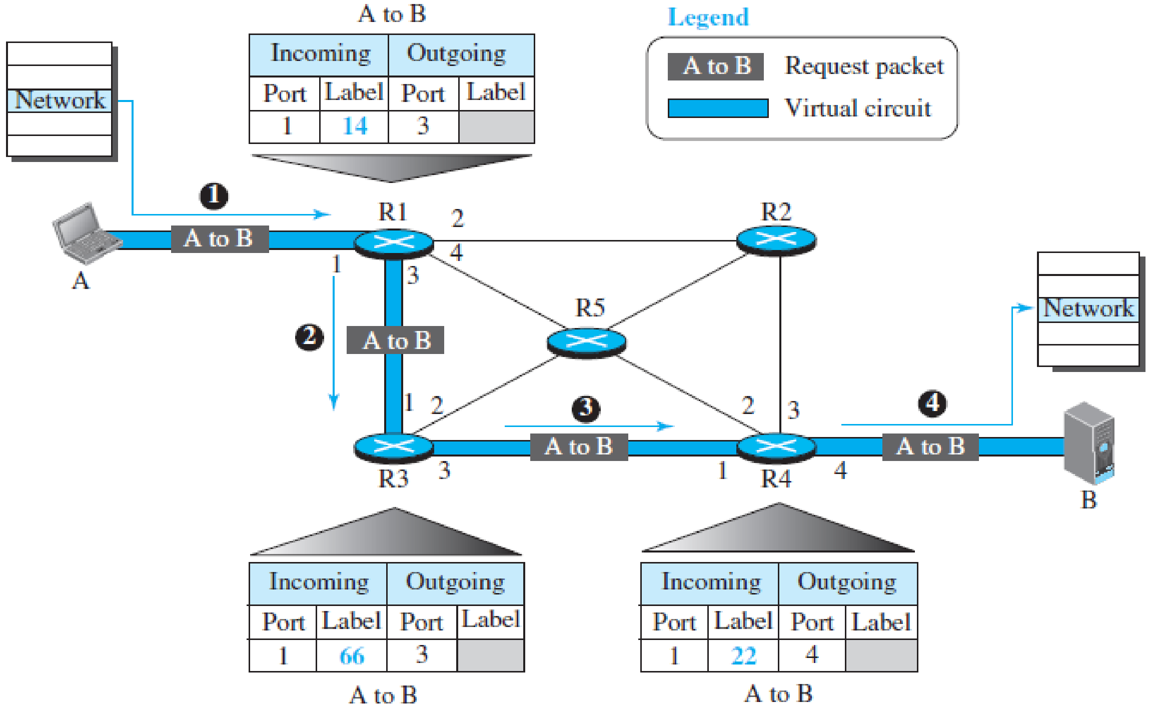
1. Setup Phase

- In the setup phase, a router creates an entry for a virtual circuit.
- For example, suppose source A needs to create a virtual circuit to destination B.
- Two auxiliary packets need to be exchanged between the sender and the receiver: the request packet and the acknowledgment packet.



Request packet

A request packet is sent from the source to the destination.

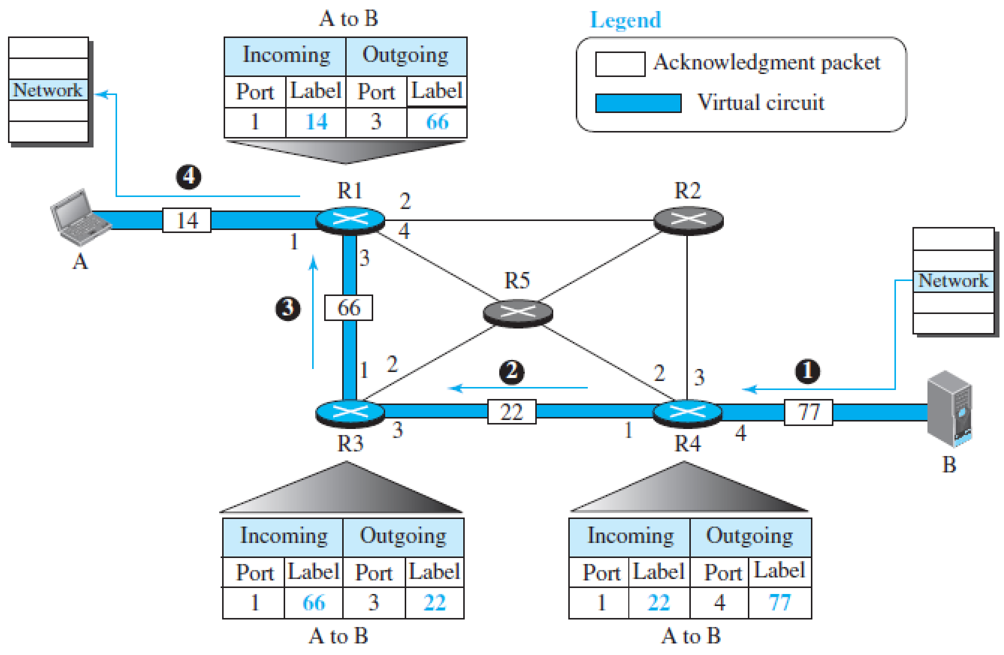


1. Source A sends a request packet to router R1.
2. Router R1 receives the request packet. It knows that a packet going from A to B goes out through port 3. The router creates an entry in its table for this virtual circuit. The router assigns the incoming port (1) and incoming label (14) and the outgoing port (3). The router then forwards the packet through port 3 to router R3.
3. Router R3 receives the setup request packet. The same events happen here as at router R1; three columns of the table are completed: in this case, incoming port (1), incoming label (66), and outgoing port (3).
4. Router R4 receives the setup request packet. Again, three columns are completed: incoming port (1), incoming label (22), and outgoing port (4).
5. Destination B receives the setup packet, and if it is ready to receive

packets from A, it assigns a label to the incoming packets that come from A, in this case 77. This label lets the destination know that the packets Come from A, and not from other sources.

Acknowledgment Packet

A special packet, called the acknowledgment packet, completes the entries in the switching tables.



A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	66

Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	22

A to B

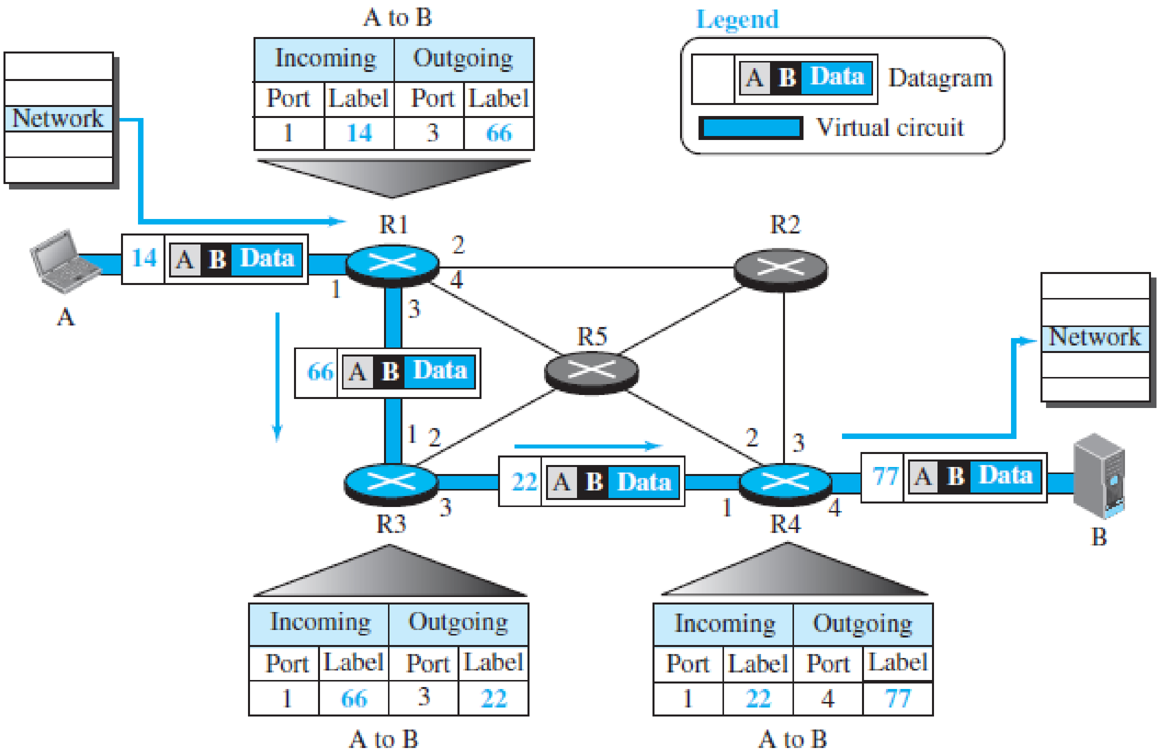
Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	77

A to B

1. The destination sends an acknowledgment to router R4. The acknowledgment carries the global source and destination addresses so the router knows which entry in the table is to be completed. The packet also carries label 77, chosen by the destination as the incoming label for packets from A. Router R4 uses this label to complete the outgoing label column for this entry. Note that 77 is the incoming label for destination B, but the outgoing label for router R4.
2. Router R4 sends an acknowledgment to router R3 that contains its incoming label in the table, chosen in the setup phase. Router R3 uses this as the outgoing label in the table.
3. Router R3 sends an acknowledgment to router R1 that contains its incoming label in the table, chosen in the setup phase. Router R1 uses this as the outgoing label in the table.
4. Finally router R1 sends an acknowledgment to source A that contains its Incoming label in the table, chosen in the setup phase.
5. The source uses this as the outgoing label for the data packets to be sent to destination B.

2. Data-Transfer Phase

- The second phase is called the data-transfer phase.
- The source computer uses the label 14, which it has received from router R1 in the setup phase. Router R1 forwards the packet to router R3, but changes the label to 66.
- Router R3 forwards the packet to router R4, but changes the label to 22.
- Finally, router R4 delivers the packet to its final destination with the label 77.
- All the packets in the message follow the same sequence of labels, and the packets arrive in order at the destination.



3. *Teardown Phase*

- In the teardown phase, source A, after sending all packets to B, sends a special packet called a teardown packet.
- Destination B responds with a confirmation packet.
- All routers delete the corresponding entries from their tables.

3. Explain the performance of network layer in detail.

- The performance of a network can be measured in terms of
  - *delay,*
  - *throughput,*
  - *packet loss.*
- *Congestion control* is an issue that can improve the performance.

1 Delay

- All of us expect instantaneous response from a network, but a packet, from its source to its destination, encounters delays.
- The delays in a network can be divided into four types:
    - transmission delay,
    - propagation delay,
    - processing delay,
    - queuing delay.

➢ ***Transmission Delay***

- A sender needs to put the bits in a packet on the line one by one.
- If the first bit of the packet is put on the line at time t1 and the last bit is put on the line at time t2, transmission delay of the packet is (t2 − t1).
- The transmission delay is longer for a longer packet and shorter if the sender can transmit faster. In other words, the transmission delay is

$$\textbf{Delay}_{\textbf{tr}} = \textbf{(Packet length) / (Transmission rate).}$$

➢ ***Propagation Delay***

- Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
- The propagation delay depends on the propagation speed of the media, which is 3 × 108 meters/second in a vacuum and normally much less in a wired medium; it also depends on the distance of the link.

$$\textbf{Delay}_{\textbf{pg}} = \textbf{(Distance) / (Propagation speed).}$$

➢ ***Processing Delay***

- The processing delay is the time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).

$$\textbf{Delay}_{\textbf{pr}} = \textbf{Time required to process a packet in a router or a destination host}$$

➢ ***Queuing Delay***

- The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output queue of a router.

$$\textbf{Delay}_{\textbf{qu}} = \textbf{The time a packet waits in input and output queues in a router}$$

➢ ***Total Delay***

- If we have *n* routers, we have (*n* + 1) links.
- Therefore, we have (*n* + 1) transmission delays related to *n* routers and the source, (*n* + 1) propagation delays related to (*n* + 1) links, (*n* + 1) processing delays related to *n* routers and the destination, and only *n* queuing delays related to *n* routers.

$$\textbf{Total delay} = (n + 1)\,(\text{Delay}_{tr} + \text{Delay}_{pg} + \text{Delay}_{pr}) + (n)\,(\text{Delay}_{qu})$$

2 Throughput

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.
- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.

Throughput = **minimum {TR1, TR2, . . . TRn}.**

3 Packet Loss

- When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
- A router, however, has an input buffer with a limited size. A time may come when the buffer is full and the next packet needs to be dropped.
- This effect is packet loss.

4 Congestion Control

- Congestion control is a mechanism for improving performance.
- Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens or remove congestion after it has happened.
- Two broad categories:
  - open-loop congestion control (prevention)
  - closed-loop congestion control (removal).

➢ ***Open-Loop Congestion Control***

- In open-loop congestion control, policies are applied to prevent congestion before it happens.
- In these mechanisms, congestion control is handled by either the source or the destination.
- The policies are Retransmission Policy, Window Policy, Acknowledgment Policy, Discarding Policy, Admission Policy.

➢ ***Closed-Loop Congestion Control***.

- Closed-loop congestion control mechanisms try to alleviate congestion after it happens.
- Several mechanisms have been used by different protocols.
  - Backpressure
  - Choke Packet
  - Implicit Signalling
  - Explicit Signalling

4. Explain in detail IPv4 Addresses.

IPV4 ADDRESSES

1. Address Space
2. Classful Addressing
3. Classless Addressing

IPV4 ADDRESSES

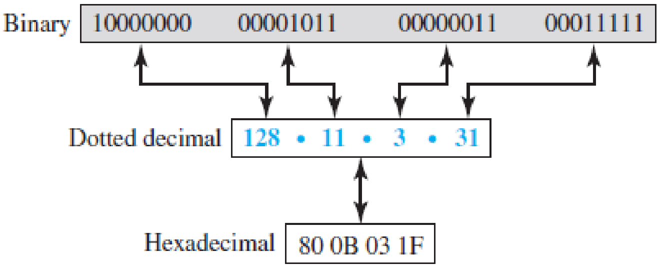
- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- IPv4 addresses are unique. If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

1. Address Space

- A protocol like IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion

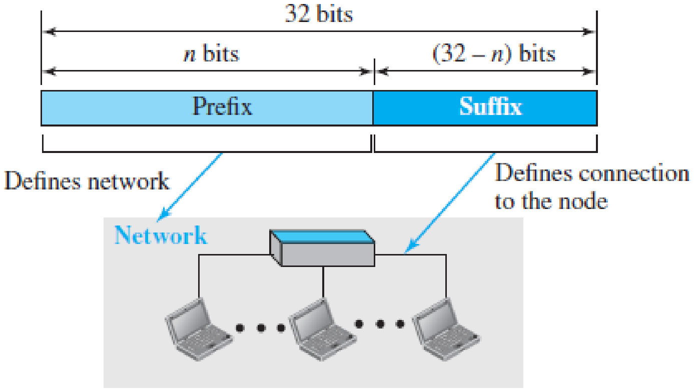
Notation

- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).
- In binary notation, an IPv4 address is displayed as 32 bits.
- Dotted-decimal notation is decimal point (dot) separating the bytes.
- IPv4 address in hexadecimal notation. Each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits.



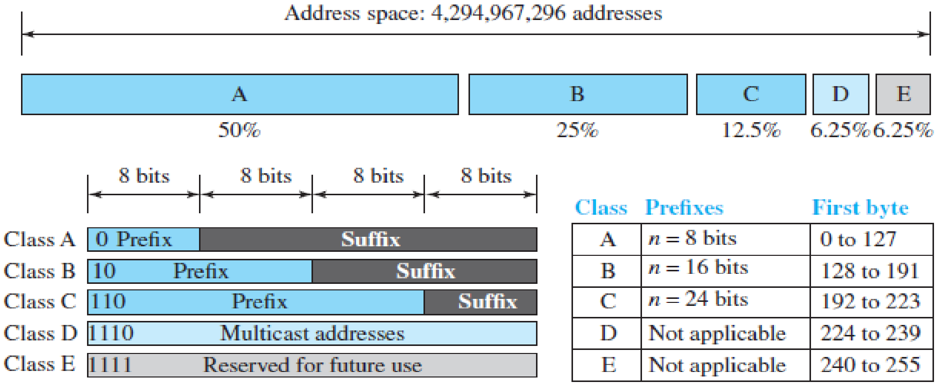
Hierarchy in Addressing

- A 32-bit IPv4 address is also hierarchical, but divided only into two parts. The first part of the address, called the prefix, defines the network; the second part of the address, called the suffix, defines the node (connection of a device to the Internet).
- The prefix length is n bits and the suffix length is (32 − n) bits. A prefix can be fixed length or variable length.

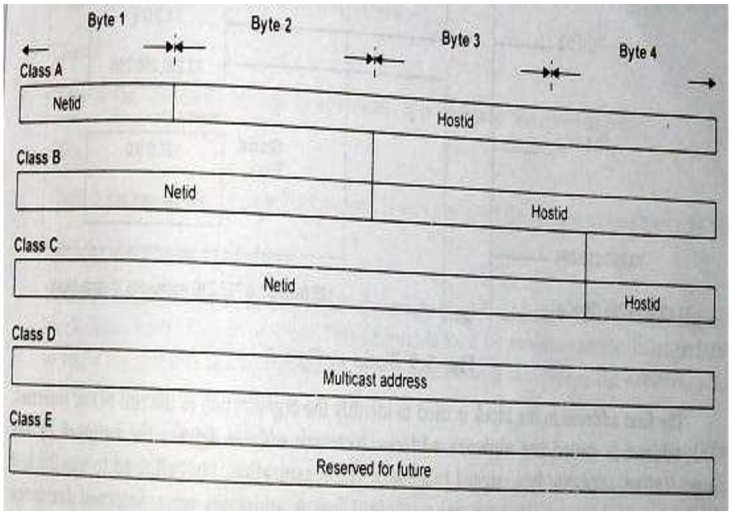


2 Classful Addressing

An IPv4 address was designed with a fixed-length prefix. The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as classful addressing.



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255



- Addresses in classes A, B and C are for unicast communication, from one source to one destination.

- Addresses in class D are for multicast communication, from one source to a group of destination. A multicast address is used only in destination addresses.
- Addresses in class E are reserved. The original idea was to use them for special purpose.

Subnetting and Supernetting

- To alleviate address depletion, two strategies were proposed and implemented: subnetting and supernetting.
- In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network.
- Subnetting allows the addresses to be divided among several organizations.
- Supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block.

Advantage of Classful Addressing

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately.

Examples:

1. Find the class for the following IP addresses. (i) 205.55.43.11 and (ii) 100.23.28.65

<u>**Solution:**</u>

i) Class C (First byte 205 between 192 to 223)

ii) Class A (First byte 100 between 0 to 127)

2. Find the class for the following IP address:

i) 11110111 11110010 10000011 10101010 - Class E (First byte starts with 1111)

ii) 01111111 11110000 01010111 00001100 - Class A (First byte starts with 0)

3. Find the netid and hostid for the following:

i) 19.34.1.5 - netid = 19 hostid = 34.1.5

ii) 190.3.70.10 - netid = 190.3 hostid = 70.10

iii) 246.3.4.10 - No netid and no hostid because 246.3.4.10 is the class E address.

i) 201.2.4.2 - netid = 201.2.4 hostid = 2

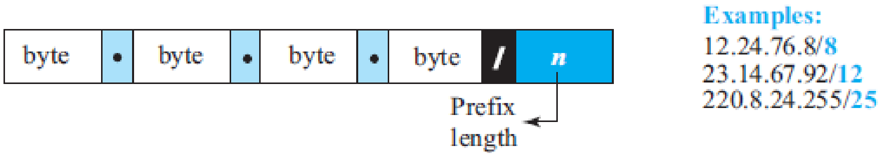
3 Classless Addressing

- In addressing, the whole address space is divided into variable length classless blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- A prefix length ranges from 0 to 32. The size of the network is inversely

- proportional to the length of the prefix. A small prefix means a larger network; a large prefix means a smaller network.

Prefix Length: Slash Notation

- The prefix length, n, is added to the address, separated by a slash.
- The notation is informally referred to as slash notation and formally as classless interdomain routing or CIDR strategy.
- An address in classless addressing can then be represented as shown in



Address Mask

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 − n) are set to 0s.
- To extract the information in a block, using the three bit-wise operations NOT, AND, and OR.

  1. The number of addresses in the block N = NOT (mask) + 1.
  2. The first address in the block = (Any address in the block) AND (mask).
  3. The last address in the block = (Any address in the block) OR [(NOT (mask)].

Network Address

- The network address is actually the identifier of the network; because it is used in routing a packet to its destination network.

5. Explain the forwarding of IP packets in detail.

FORWARDING OF IP PACKETS

- Forwarding Based on Destination Address
- Forwarding Based on Label
- Routers as Packet Switches

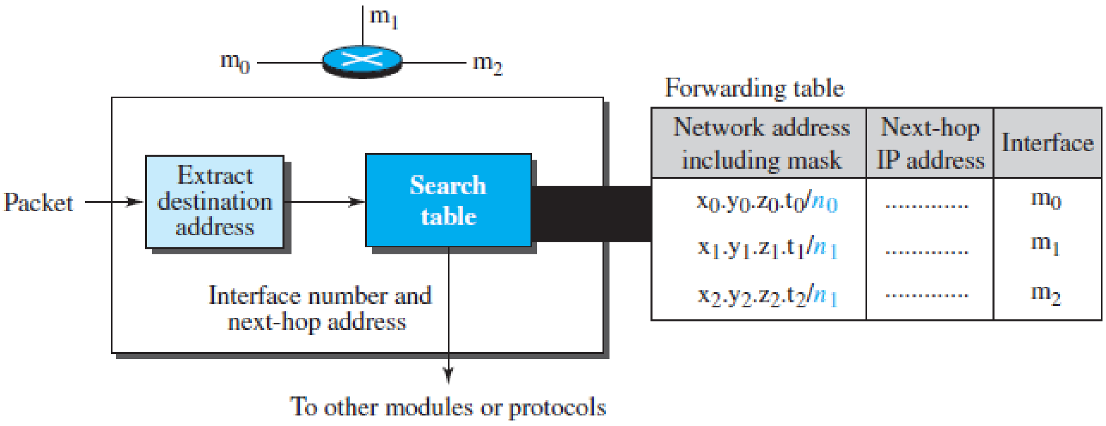
➢ **FORWARDING OF IP PACKETS**

- Forwarding means to place the packet in its route to its destination.
- When IP is used as a connectionless protocol, forwarding is based on the destination address of the IP datagram; when the IP is used as a connection-oriented protocol, forwarding is based on the label attached to an IP datagram.

➢ **Forwarding Based on Destination Address**

- Forwarding requires a host or a router to have a forwarding table.
- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.

- The table needs to be searched based on the network address.
- Unfortunately, the destination address in the packet gives no clue about the network address.
- To solve the problem, we need to include the mask (/*n*) in the table.
- A classless forwarding table needs to include four pieces of information: the mask, the network address, the interface number, and the IP address of the next router.
- For example, if *n* is 26 and the network address is 180.70.65.192, then one can combine the two as one piece of information: 180.70.65.192/**26**.


m1
m0
m2
Packet
Extract destination address
Search table
Interface number and next-hop address
To other modules or protocols
Forwarding table

Network address including mask	Next-hop IP address	Interface
$x_0.y_0.z_0.t_0/n_0$	....	m_0
$x_1.y_1.z_1.t_1/n_1$	....	m_1
$x_2.y_2.z_2.t_2/n_1$	....	m_2

➢ Forwarding Based on Label

- In a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to the packet.
- When the forwarding algorithm gets the destination address of the packet, it needs to apply the mask to find the destination network address.
- It then needs to check the network addresses in the table until it finds the match.
- The router then extracts the next-hop address and the interface number to be delivered to the data-link layer.

➢ Routers as Packet Switches

- The packet switches that are used in the network layer are called routers.
- Routers can be configured to act as either a datagram switch or a virtual-circuit switch.

6. Explain about INTERNET PROTOCOL (IP) in detail. [May/June 2014]

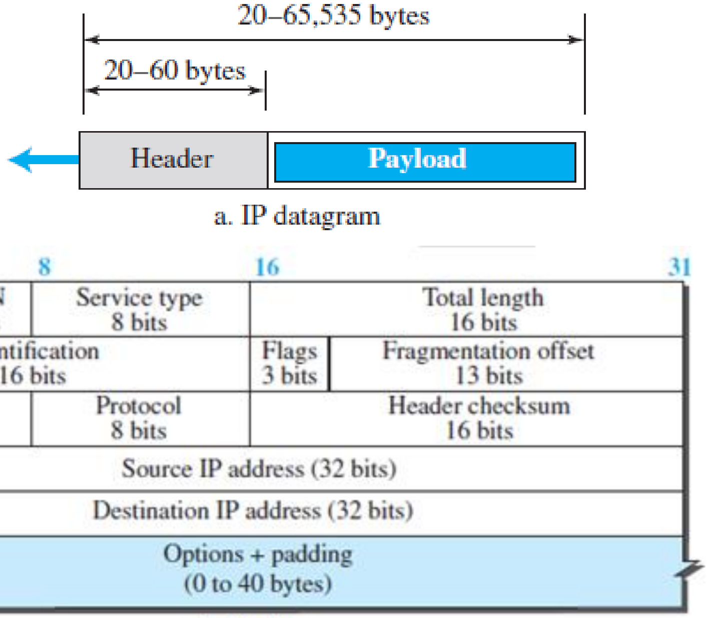
➢ INTERNET PROTOCOL (IP)

- The Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.

Datagram Format

- Packets used by the IP are called *datagrams*.
- A datagram is a variable-length packet consisting of two parts: header and payload (data).

- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



a. IP datagram

b. Header

- ***Version Number.***
  - The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.
- ***Header Length.***
  - The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.
- ***Service Type.***
  - **T**ype of service (TOS), defines how the datagram should be handled.
- ***Total Length.***
  - This 16-bit field defines the total length (header plus data) of the IP datagram in bytes
- ***Identification, Flags, and Fragmentation Offset.***
  - These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.
- ***Time-to-live.***
  - The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field.
  - Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.
- ***Protocol.***
  - In TCP/IP, the data section of a packet, called the *payload*, carries the whole packet from another protocol.

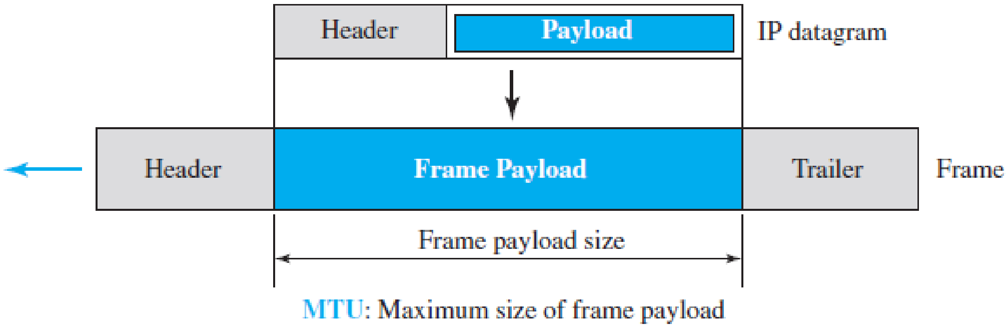
  - A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.
- ***Header checksum.***
  - IP adds a header checksum field to check the header for error control, but not the payload.
  - Since the value of some fields, such as TTL, which are related to fragmentation and options, may change from router to router, the checksum needs to be recalculated at each router.
- ***Source and Destination Addresses.***
  - These 32-bit source and destination address fields define the IP address of the source and destination respectively.
  - The source host should know its IP address.
  - The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS.
- ***Options.***
  - A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.
- ***Payload.***
  - Payload is the packet coming from other protocols that use the service of IP.

➢ **Fragmentation**

- The division of a packet into smaller units to accommodate a protocol's MTU.

Maximum Transfer Unit (MTU)

- The largest size data unit a specific network can handle.



MTU: Maximum size of frame payload

- The value of the MTU differs from one physical network protocol to another.
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.
- A datagram may be fragmented several times before it reaches the final destination.
- The host or router that fragments a datagram must change the values of three fields: flags, fragmentation offset, and total length.

Three fields in an IP datagram are related to fragmentation:

identification, flags, and *fragmentation offset.*

- The 16-bit *identification field* identifies a datagram originating from the source host.
- The 3-bit *flags field* defines three flags.
  - The leftmost bit is reserved (not used).
  - The second bit (D bit) is called the *do not fragment* bit.
    - If its value is 1, the machine must not fragment the datagram.
    - If its value is 0, the datagram can be fragmented if necessary.
  - The third bit (M bit) is called the *more fragment bit*.
    - If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
    - If its value is 0, it means this is the last or only fragment.
- The 13-bit *fragmentation offset field* shows the relative position of this fragment with respect to the whole datagram.

7. Explain about Internet Control Message Protocol version 4 (ICMPv4) in detail.

ICMPv4
- MESSAGES
- Debugging Tools
- ICMP Checksum

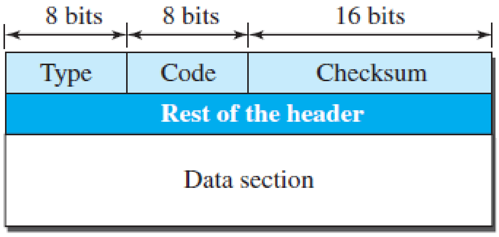
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- ICMP is used to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them.

➢ MESSAGES

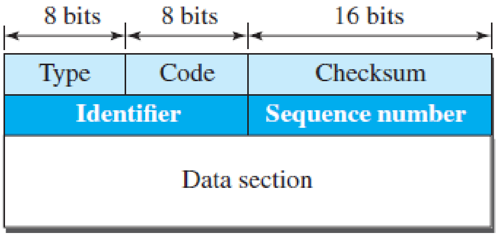
- ICMP messages are divided into two broad categories:

  error-reporting messages **and** ***query messages***

- An ICMP message has an 8-byte header and a variable-size data section.
- The first field, ICMP type, defines the type of the message.
- The code field specifies the reason for the particular message type.
- The last common field is the checksum field.
- The rest of the header is specific for each message type.
- The data section in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of query.



Error-reporting messages



Query messages

Type and code values

Error-reporting messages
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages
08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Error Reporting Messages

- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- To make the error-reporting process simple, ICMP follows some rules in
- reporting messages.
  - First, no error message will be generated for a datagram having a multicast address or special address (such as *this host* or *loopback*).
  - Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.
  - Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.

1. Destination Unreachable

- The most widely used error message is the destination unreachable (type 3).
- This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.

2. Source Quench

- It informs the sender that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.

3. Redirection Message

- The *redirection message* (type 5) is used when the source uses a wrong router to send out its message.
- The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future.

4. Time Exceeded

- When the TTL value becomes 0, the datagram is dropped by the visiting router and a *time exceeded* message (type 11) with code 0 is sent to the source to inform it about the situation.

- The time-exceeded message (with code 1) can also be sent when not all fragments of a datagram arrive within a predefined period of time.

5. Parameter Problem

- A *parameter problem message* (type 12) can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

Query Messages

- Query messages are used to probe or test the liveliness of hosts or routers in the Internet.
- The query messages come in pairs: request and reply.
- The *echo request* (type 8) and the *echo reply* (type 0) pair of messages are used by a host or a router to test the liveliness of another host or router. A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

➢ **Debugging Tools**

- Two debugging tools: *ping* and *traceroute*.

Ping

- *Ping* program is used to find if a host is alive and responding.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The ping program gets help from two query messages;

Traceroute or Tracert

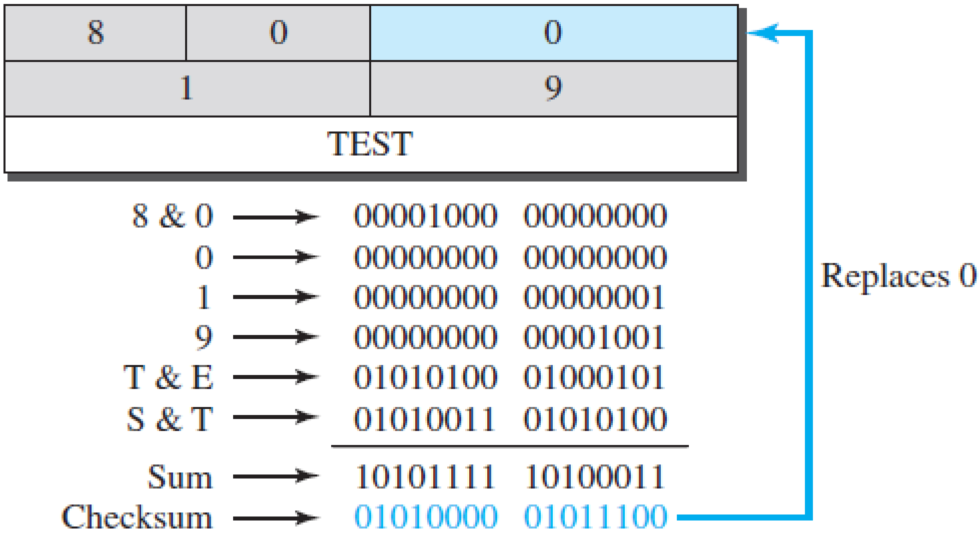
- The *traceroute* program in UNIX or *tracert* in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- the *traceroute* program gets help from two error-reporting messages: time-exceeded and destination-unreachable.

➢ **ICMP Checksum**

- In ICMP the checksum is calculated over the entire message (header and data).

Example

An example of checksum calculation for a simple echo-request message. We
randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added and the sum is complemented. Now the sender can put this value in the checksum field.



8. Elaborate the various routing algorithms or unicast routing algorithms in detail.

➢ **ROUTING ALGORITHMS**

- Distance-Vector Routing
- Link-State Routing
- Path-Vector Routing

➢ **Distance-Vector (DV) Routing**

- In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbours.
- The incomplete trees are exchanged between immediate neighbours to make the trees more and more complete and to represent the whole internet.

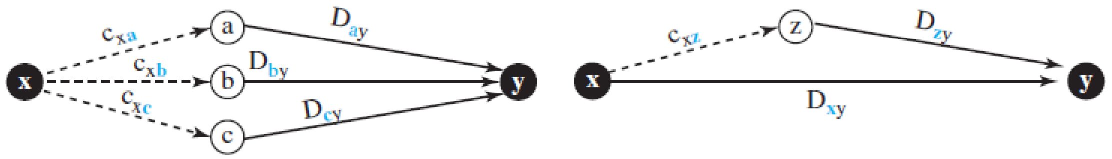
Bellman-Ford Equation

- This equation is used to find the least cost (shortest distance) between a source node, ***x***, and a destination node, ***y***, through some intermediary nodes (**a, b, c,** . . .).
- The following shows the general case in which D***ij*** is the shortest distance and c***ij*** is the cost between nodes ***i*** and ***j***.

$$D_{xy} = \min\{(c_{xa} + D_{ay}), (c_{xb} + D_{by}), (c_{xc} + D_{cy}), \ldots\}$$

- In distance-vector routing, normally we want to update an existing least cost with a least cost through an intermediary node, such as ***z***, if the latter is shorter.

$$D_{xy} = \min\{D_{xy}, (c_{xz} + D_{zy})\}$$



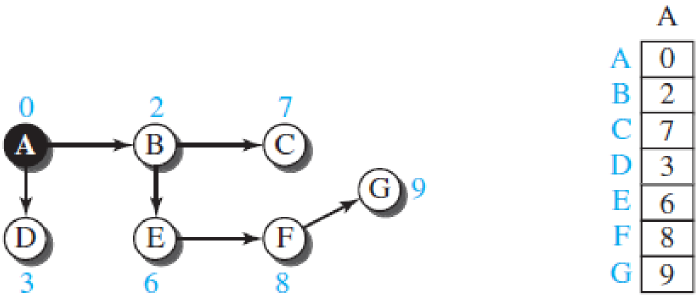
a. General case with three intermediate nodes

b. Updating a path with a new route

(a→y), (b→y), and (c→y) as previously established least-cost paths and (x→y) as the new least-cost path.

Distance Vectors

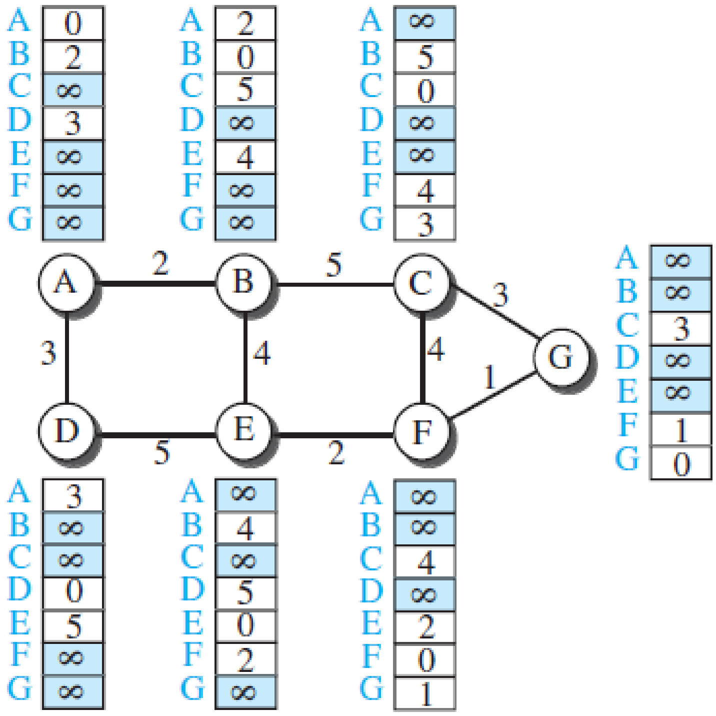
- A least-cost tree is a combination of least-cost paths from the root of the tree to all destinations.
- These paths are graphically glued together to form the tree.



	A
A	0
B	2
C	7
D	3
E	6
F	8
G	9

a. Tree for node A

b. Distance vector for node A



Distance-Vector Routing Algorithm

```
1       Distance_Vector_Routing ( )
2       {
3         // Initialize (create initial vectors for the node)
4               D[myself ] = 0
5               for (y = 1 to N)
6               {
7                     if (y is a neighbour)
8                           D[y] = c[myself ][y]
9                     else
10                          D[y] = ∞
11              }
12              send vector {D[1], D[2], …, D[N]} to all neighbours

13      // Update (improve the vector with the vector received from a
        neighbour)
14              repeat (forever)
15              {
16                    wait (for a vector Dw from a neighbour w or any change
                   in the link)
17                    for (y = 1 to N)
18                    {
19                          D[y] = min [D[y], (c[myself ][w] + Dw[y ])]
                                                      // Bellman-Ford equation
20                    }
21                    if (any change in the vector)
22                          send vector {D[1], D[2], …, D[N]} to all neighbours
23              }
24        } // End of Distance Vector
```

- Lines 4 to 11 initialize the vector for the node.
- Lines 14 to 23 show how the vector can be updated after receiving a vector from the immediate neighbour.
- The *for* loop in lines 17 to 20 allows all entries (cells) in the vector to be updated after receiving a new vector.
- Note that the node sends its vector in line 12, after being initialized, and in line 22, after it is updated.

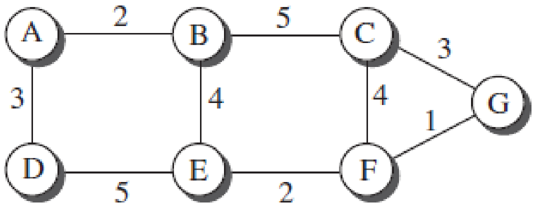
➢ **Link-State Routing**

- This method uses the term *link-state* to define the characteristic of a link (an edge) that represents a network in the internet.

- Links with lower costs are preferred to links with higher costs; if the cost of a link is infinity, it means that the link does not exist or has been broken.

Link-State Database (LSDB)

- The LSDB can be represented as a two-dimensional array(matrix) in which the value of each cell defines the cost of the corresponding link.



a. The weighted graph

	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. Link state database

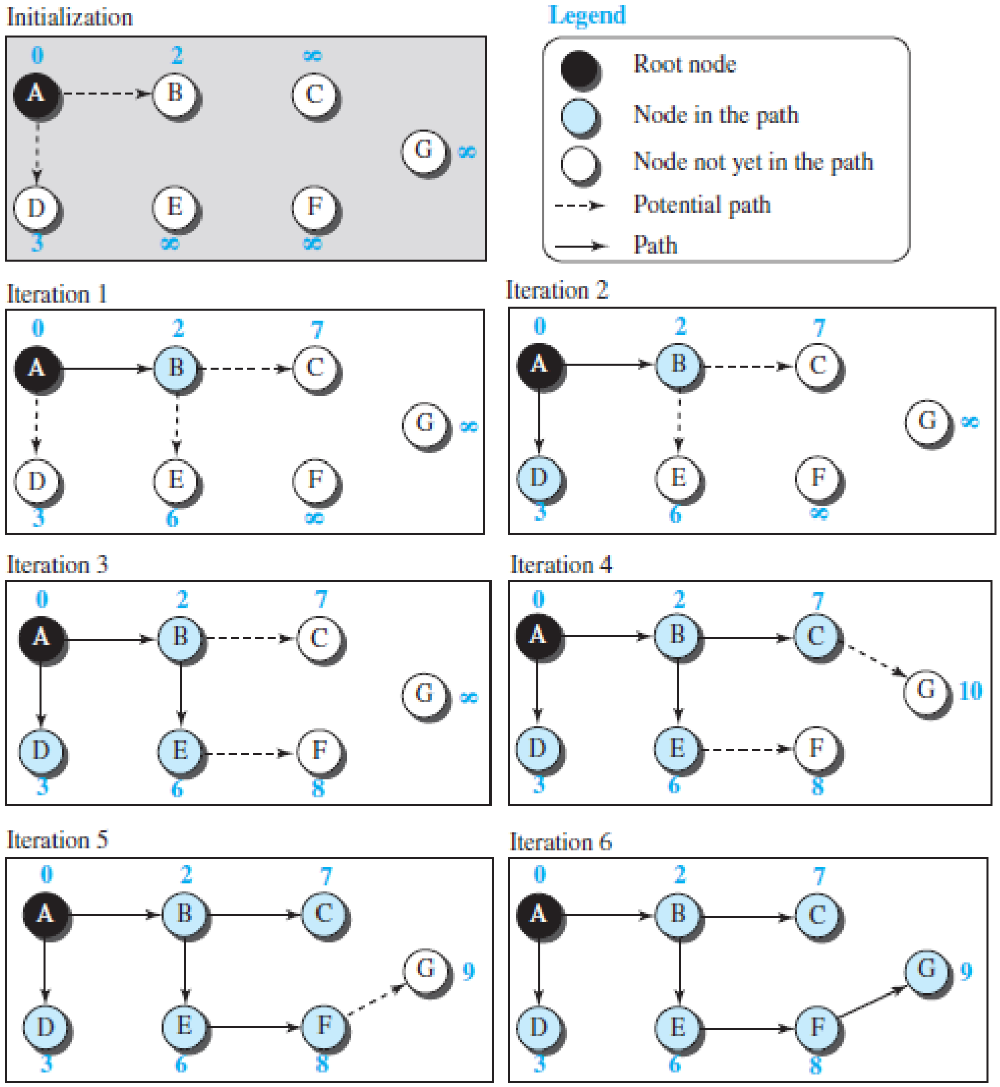
Formation of Least-Cost Trees

- To create a least-cost tree for itself, using the shared LSDB, each node needs to run the famous Dijkstra Algorithm.
- This iterative algorithm uses the following steps:
  1. The node chooses itself as the root of the tree, creating a tree with a single node, and sets the total cost of each node based on the information in the LSDB.
  2. The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree. After this node is added to the tree, the cost of all other nodes not in the tree needs to be updated because the paths may have been changed.
  3. The node repeats step 2 until all nodes are added to the tree.

Dijkstra’s Algorithm

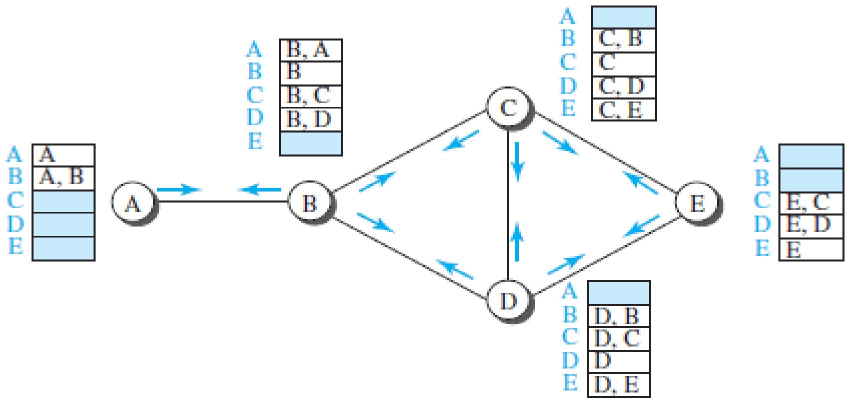
```
Dijkstra’s Algorithm ( )
{
    // Initialization
    Tree = {root} // Tree is made only of the root
    for (y = 1 to N) // N is the number of nodes
    {
        if (y is the root)
            D[y] = 0
        // D[y] is shortest distance from root to node y
        else if (y is a neighbour)
            D[y] = c[root][y]
        // c[x][y] is cost between nodes x and y in LSDB
        else
            D[y] = ∞
        }
        // Calculation
    repeat
    {
        find a node w, with D[w] minimum among all nodes not
        in the Tree
        Tree = Tree ∪ {w} // Add w to tree
        // Update distances for all neighbours of w
    for (every node x, which is a neighbour of w and not in the Tree)
        {
            D[x] = min{D[x], (D[w] + c[w][x])}
        }
    } until (all nodes included in the Tree)
} // End of Dijkstra
```

Example:



- **Path-Vector Routing**
    - In path-vector routing, the path from a source to all destinations is also determined by the best spanning tree.
    - The best spanning tree, however, is not the least-cost tree; it is the tree determined by the source when it imposes its own policy.
    - Path-vector routing, is an asynchronous and distributed routing algorithm.

$$\text{Path}(x, y) = \text{best}\ \{\text{Path}(x, y), [(x + \text{Path}(v, y)]\} \qquad \text{for all } v\text{'s in the internet.}$$



A	A
B	A, B
C	
D	
E	

A	B, A
B	B
C	B, C
D	B, D
E	

A	
B	C, B
C	C
D	C, D
E	C, E

A	
B	
C	E, C
D	E, D
E	E

A	
B	D, B
C	D, C
D	D
E	D, E

Path-vector algorithm for a node

```
Path_Vector_Routing ( )
{
// Initialization
    for (y = 1 to N)
    {
        if (y is myself)
            Path[y] = myself
        else if (y is a neighbour)
            Path[y] = myself + neighbour node
        else
            Path[y] = empty
    }
    Send vector {Path[1], Path[2], …, Path[y]} to all neighbours
 // Update
    repeat (forever)
    {
        wait (for a vector Path from a neighbour w)
        for (y = 1 to N)
        {
        if (path includes myself)
            discard the path // Avoid any loop
        else
            Path[y] = best {Path[y], (myself + Path w[y])}
        }
        If (there is a change in the vector)
            Send vector {Path[1], Path[2], …, Path[y]} to all
            neighbours
    }
  } // End of Path Vector
```

9. Discuss in detail about Routing algorithms. [May/June 2014]-Nov-15

ROUTING ALGORITHMS PROTOCOL

- Routing Information Protocol (RIP), based on the distance-vector algorithm,
- Open Shortest Path First (OSPF), based on the link-state algorithm,
- Border Gateway Protocol (BGP), based on the path-vector algorithm.

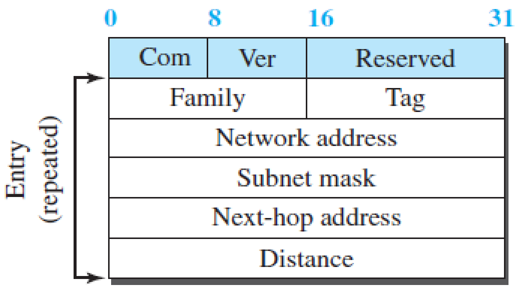
➢ Routing Information Protocol (RIP)

- The **Routing Information Protocol** (**RIP**) is one of the most widely used intradomain routing protocols based on the distance-vector routing algorithm.

RIP Implementation

- RIP is implemented as a process that uses the service of UDP on the well-known port number 520. RIP messages are encapsulated inside UDP user datagrams, which in turn are encapsulated inside IP datagrams.

RIP Messages



Fields

Com: Command, request (1), response (2)
Ver: Version, current version is 2
Family: Family of protocol, for TCP/IP value is 2
Tag: Information about autonomous system
Network address: Destination address
Subnet mask: Prefix length
Next-hop address: Address length
Distance: Number of hops to the destination

- RIP has two types of messages: request and response.
- A request message is sent by a router that can ask about specific entries or all entries.
- A response (or update) message can be either solicited or unsolicited. A solicited response message is sent only in answer to a request message. It contains information about the destination specified in the corresponding request message.
- An unsolicited response message, on the other hand, is sent periodically, every 30 seconds or when there is a change in the forwarding table.

RIP Packet Format

- Each packet consists of several address distances.
- The header format contains the following specifications for the first address distance.

Byte:

1	1	2	2	2	4	4	4	4
Command	Version Number	0	Address Family Identifier	0	IP Address	0	0	Metric

- **Command** indicates a request with value 1 or a reply with value 2.
- **Version number** specifies the version: RIP-1 or RIP-2.
- **Address family identifier** shows the type of address, such as an IP address.

- **IP address** provides the IP address in a particular network.
- **Metric** identifies the distance from a router to a specified network.

Timers in RIP

- RIP uses three timers to support its operation.
  - The *periodic timer* controls the advertising of regular update messages.
  - The *expiration timer* governs the validity of a route.
  - The *garbage collection timer* is used to purge a route from the forwarding table.

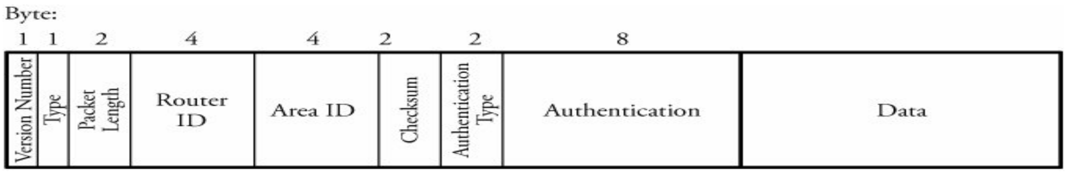
Performance

- ***Update Messages.*** The update messages in RIP have a very simple format and are sent only to neighbours; they are local.
- ***Convergence of Forwarding Tables*.** RIP uses the distance-vector algorithm, which can converge slowly if the domain is large, but, since RIP allows only 15 hops in a domain, there is normally no problem in convergence.
- ***Robustness*.** If there is a failure or corruption in one router, the problem will be propagated to all routers and the forwarding in each router will be affected.

Open Shortest Path First (OSPF)

Open Shortest Path First (**OSPF**) is also an intradomain routing protocol. OSPF is an *open* protocol, which means that the specification is a public document.

OSPF Packet Format



All OSPF packets use a 24-byte header as follows:

- Version number indicates the version of OSPF.
- Type is one of the five types of packets for OSPF to choose from: hello, database description, link-state request, link-state update, and link-state acknowledgment.
- Packet length specifies the length of the OSPF packet.
- Router ID specifies the packet's source router ID.
- Area ID refers to the area that the source router belongs to.
- Checksum specifies the standard IP checksum of the packet contents.
- Authentication type identifies which authentication method to choose.
- Authentication specifies the authentication method.

OSPF Messages

- OSPF is a very complex protocol; it uses five different types of messages.
- The ***hello*** message (type 1) is used by a router to introduce itself to the neighbours and announce all neighbours that it already knows.
- The ***database description*** message (type 2) is normally sent in response to the hello message to allow a newly joined router to acquire the full LSDB.
- The ***link-state request*** message (type 3) is sent by a router that needs information about a specific LS.
- The ***link-state update*** message (type 4) is the main OSPF message used for building the LSDB.
- The ***link-state acknowledgment*** message (type 5) is used to create reliability in OSPF; each router that receives a link-state update message needs to acknowledge it.

OSPF Algorithm

- OSPF implements the link-state routing.

***Performance* of OSPF**:

- Update Messages.
- Convergence of Forwarding Tables.
- Robustness.

➢ ***Border Gateway Protocol (BGP)***

- The Border Gateway Protocol version 4 (BGP4) is the only interdomain routing protocol, based on the path-vector algorithm.
- BGP allows routers to carry specific policies or constraints that they must meet.
- In BGP, two contributing (casual) routers can exchange routing information even if they are located in two different autonomous systems.

Details of BGP

- BGP has three functional components:
    - Neighbor relationship
    - Neighbor maintenance
    - Network maintenance
- The neighbor relationship refers to an agreement between two routers in two different autonomous systems to exchange routing information on a regular basis.
- A router may reject its participation in establishing a neighbor relationship for several reasons, such as the rule of the domain, overload, or a temporary malfunctioning of external links.
- Neighbor maintenance is a process of maintaining the neighbor relationship already established.
- For this reason, two routers send keep-alive messages to each other. The last BGP process is network maintenance.

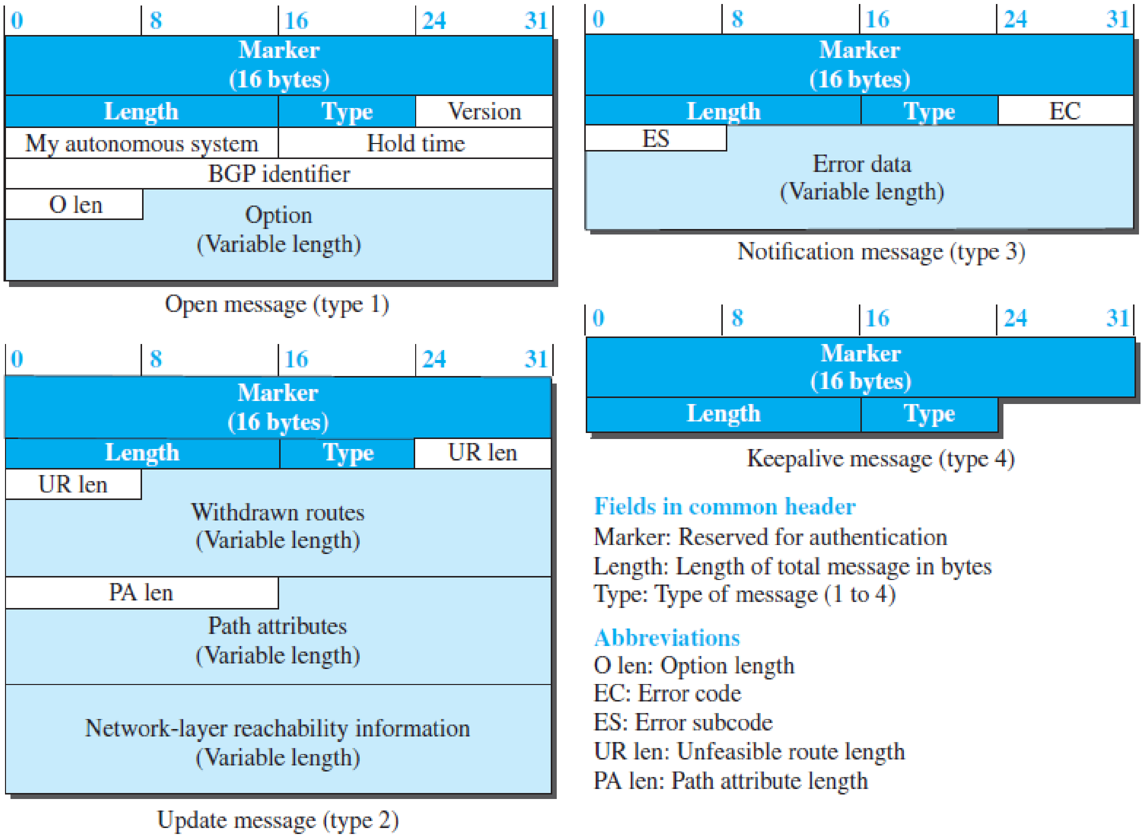
- Each router keeps the database of the subnetworks that it can reach and tries to get the best route for that subnetwork.

BGP Packets / Messages

- **Open packet.** This packet requests establishment of a relationship between two routers.
- **Update packet**. This packet conveys update information about routes.
- **Keep-alive packet**. Once a relationship between two routers is established, this packet confirms its neighbor relationship frequently.
- **Notification packet.** This packet is used when an error occurs.

Performance

- BGP speakers exchange a lot of messages to create forwarding tables, but BGP is free from loops and count-to-infinity.



Open message (type 1)

Notification message (type 3)

Keepalive message (type 4)

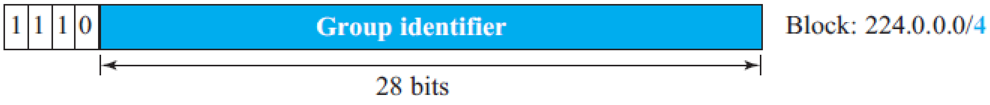
Update message (type 2)

10. Explain in detail about multicasting basics.

- **MULTICASTING BASICS**
  - Multicast Addresses
  - Delivery at Data-Link Layer
  - Collecting Information about Groups
  - Multicast Forwarding
  - Two Approaches to Multicasting

Multicast Addresses

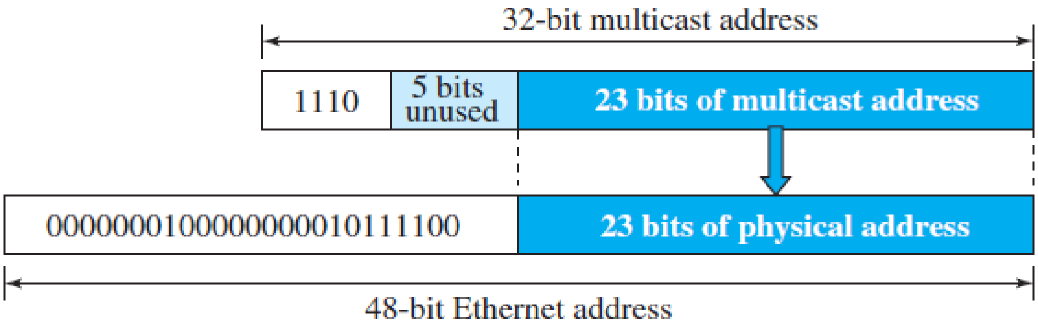
- In multicast communication, the sender is only one, but the receiver is many.
- A multicast address defines a group of recipients, not a single one.
- In other words, a multicast address is an identifier for a group.
- A host, which is a member of *n* groups, actually has (*n* + 1) addresses: one unicast address that is used for source or destination address in unicast communication and *n* multicast addresses that are used only for destination addresses to receive messages sent to a group.
- In classful addressing, all of class D was composed of these addresses; classless addressing used the same block, but it was
- referred to as the block 224.0.0.0/**4** (from 224.0.0.0 to 239.255.255.255).



Delivery at Data-Link Layer

- Data-link layer multicast addresses are also needed to deliver a multicast packet encapsulated in a frame.

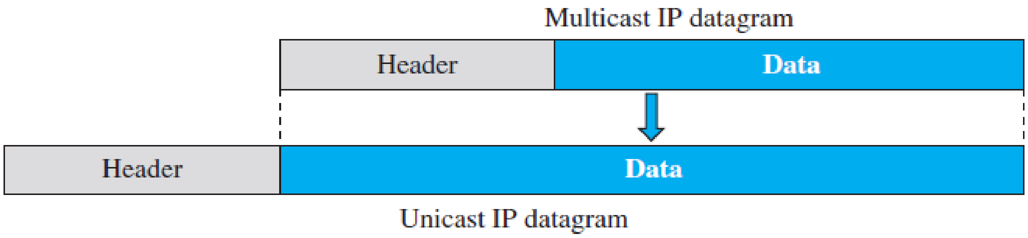
Mapping class D to Ethernet physical address



- Most LANs support physical multicast addressing. Ethernet is one of them.
- An Ethernet physical address (MAC address) is six octets (48 bits) long.
- If the first 25 bits in an Ethernet address are 00000001 00000000 01011110 0, this identifies a physical multicast address for the TCP/IP protocol.
- The remaining 23 bits can be used to define a group.
- To convert an IP multicast address into an Ethernet address, the multicast router extracts the least significant 23 bits of a multicast IP address and inserts them into a multicast Ethernet physical address

Network with No Multicast Support

- To send a multicast packet through WANs, a process called *tunnelling* is used. In **tunnelling,** the multicast packet is encapsulated in a unicast packet and sent through the network, where it emerges from the other side as a multicast packet



- **Collecting Information about Groups**

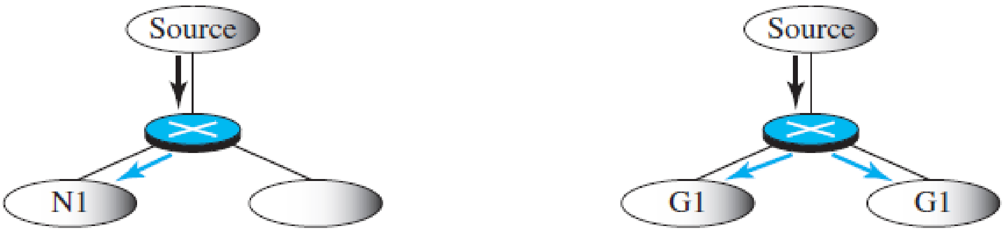
Creation of forwarding tables in both unicast and multicast routing involves two steps:

1. A router needs to know to which destinations it is connected.
2. Each router needs to propagate information obtained in the first step to all Other routers so that each router knows to which destination each other router is connected.

- **Multicast Forwarding**

1. In unicast communication, the destination address of the packet defines one single destination.

In multicast communication, the destination of the packet defines one group, but that group may have more than one member in the internet.

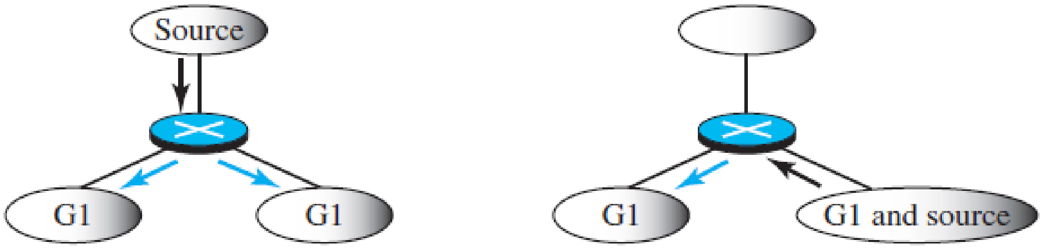


a. Destination in unicasting is one

b. Destination in mulicasting is more than one

2. Forwarding decisions in unicast communication depend only on the Destination address of the packet.

Forwarding decisions in multicast communication depend on both the destination and the source address of the packet



a. Packet sent out of two interfaces

b. Packet sent out of one interface

- **Two Approaches to Multicasting**

1. Source-Based Tree Approach

- In the source-based tree approach to multicasting, each router needs to create a separate tree for each source-group combination.

- If there are m groups and n sources in the internet, a router needs to create (m × n) routing trees.
- In each tree, the corresponding source is the root, the members of the group are the leaves, and the router itself is somewhere on the tree.

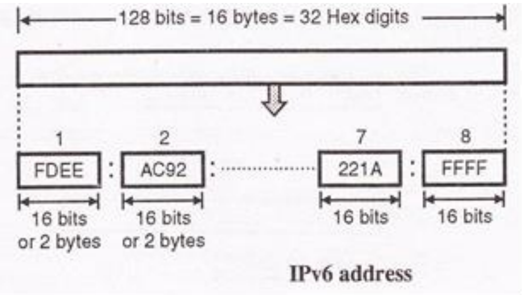
2. ***Group-Shared Tree Approach***

- In the **group-shared tree** approach, the designated router, which is called the *core* router or the *rendezvous point* router, acts as the representative for the group.
- Any source that has a packet to send to a member of that group sends it to the core center (unicast communication) and the core center is responsible for multicasting.
- The core center creates one single routing tree with itself as the root and any routers with active members in the group as the leaves.
- In this approach, there are *m* core routers (one for each group) and each core router has a routing tree, for the total of *m* trees.
- This means that the number of routing trees is reduced from (*m* × *n*) in the source-based tree approach to *m* in this approach.

11. Explain in detail about IPv6 ADDRESSING.

➢ **IPv6 ADDRESSING**

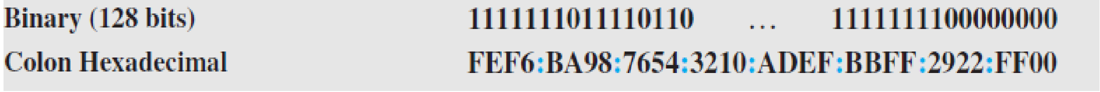
- The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4.
- An IPv6 address is 128 bits or 16 bytes (octets) long, four times the address length in IPv4.



IPv6 address

➢ **Representation / Notations**

- Binary notation is used when the addresses are stored in a computer.
- The **colon hexadecimal notation** divides the address into eight sections, each made of four hexadecimal digits separated by colons.

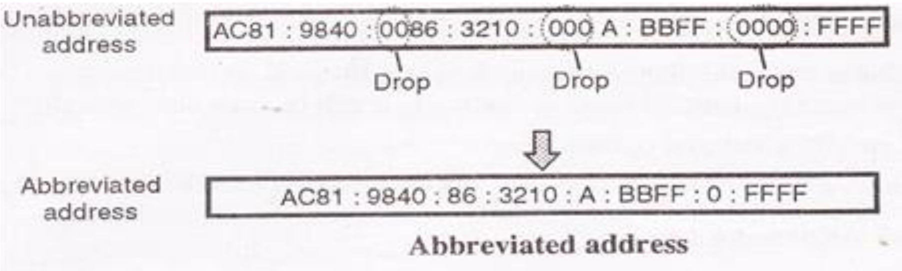


Binary (128 bits)	1111111011110110 … 1111111100000000
Colon Hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

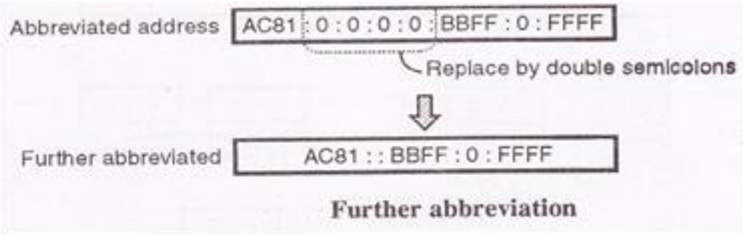
Abbreviation :

Zero Compression

- The IPv6 address, even in hexadecimal format is very long. But in this address there are many of the zero digits in it. In such a case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted.
- Note that only the leading zeros can be dropped but the trailing zeros cannot drop.


Unabbreviated address
AC81 : 9840 : 0086 : 3210 : 000 A : BBFF : 0000 : FFFF
Drop
Drop
Drop
Abbreviated address
AC81 : 9840 : 86 : 3210 : A : BBFF : 0 : FFFF

Abbreviated address


Abbreviated address
AC81 : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF
Replace by double semicolons
Further abbreviated
AC81 : : BBFF : 0 : FFFF

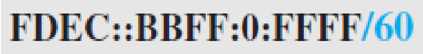
Further abbreviation

Mixed Notation

- Mixed representation of an IPv6 address: colon hex and dotted decimal notation.
- This is appropriate during the transition period in which an IPv4 address is embedded in an IPv6 address (as the rightmost 32 bits).
- For example, the address (::130.24.24.18) is a legitimate address in IPv6.

CIDR Notation

- IPv6 uses hierarchical addressing. For this, IPv6 allows slash or CIDR notation.
- For example, the following shows how we can define a prefix of 60 bits using CIDR.



FDEC::BBFF:0:FFFF/60

- **Address Space**
  - The address space of IPv6 contains 2128 addresses. This address space is 296 times the IPv4 address.

Three Address Types

- In IPv6, a destination address can belong to one of three categories:
  - unicast,
  - anycast,
  - multicast.

1. *Unicast Address*

- A unicast address defines a single interface (computer or router).
- The packet sent to a unicast address will be routed to the intended recipient.

2. *Anycast Address*

- An **anycast address** defines a group of computers that all share a single address.

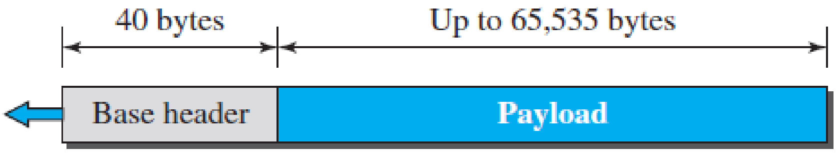
- A packet with an anycast address is delivered to only one member of the group, the most reachable one.

3. Multicast Address

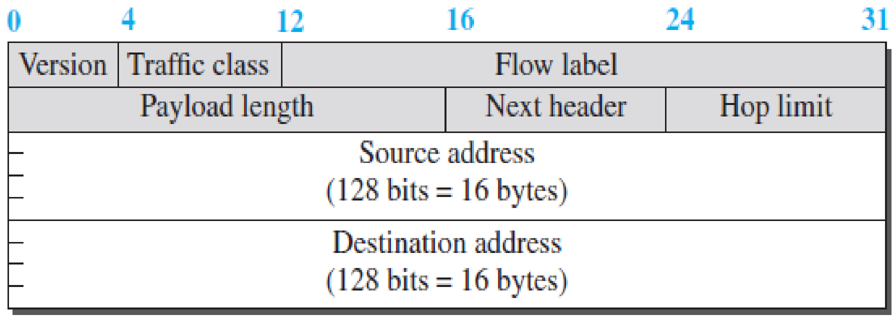
- A multicast address also defines a group of computers.
- In multicasting each member of the group receives a copy.

IPv6 Packet Format:

- Each packet is composed of a base header followed by the payload.
- The base header occupies 40 bytes, whereas payload can be up to 65,535 bytes of information.



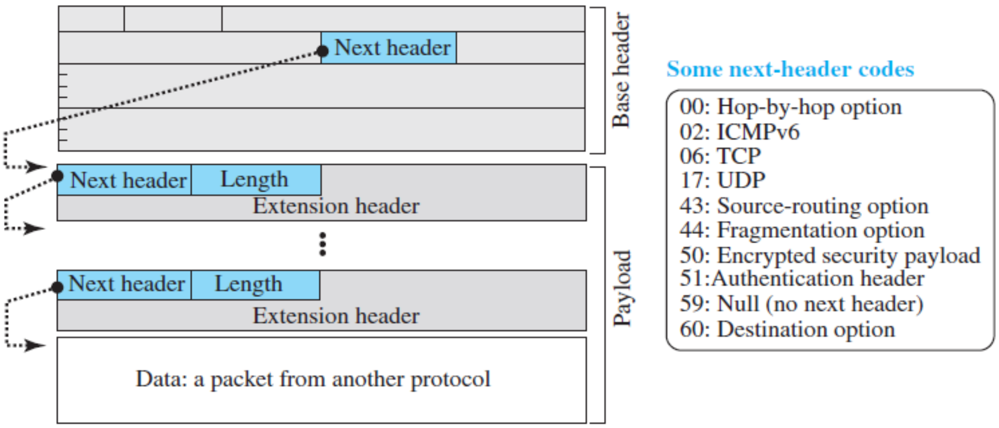
a. IPv6 packet



b. Base header

- **Version.** The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.
- **Traffic class.** The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service field in IPv4.
- **Flow label.** The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data. We will discuss this field later.
- **Payload length.** The 2-byte payload length field defines the length of the IP datagram excluding the header.
- **Hop limit.** The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source and destination addresses.** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram. The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.
- **Payload.** Compared to IPv4, the payload field in IPv6 has a different format and meaning.

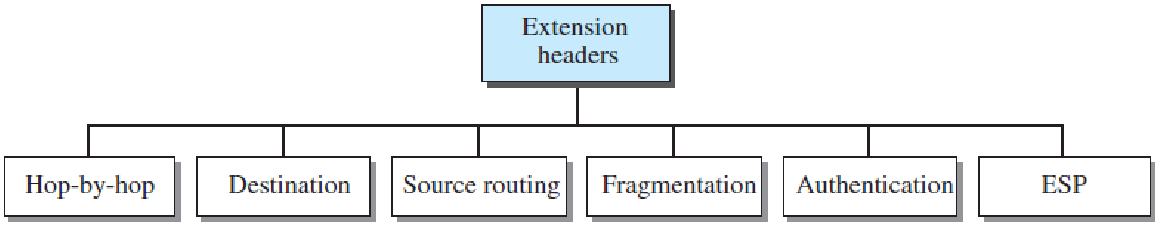
Figure 22.7 *Payload in an IPv6 datagram*



- The payload in IPv6 means a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).
- Each extension header has two mandatory fields, next header and the length, followed by information related to the particular option.

➢ Extension Header

- An IPv6 packet is made of a base header and some extension headers.
- The length of the base header is fixed at 40 bytes.
- Extension headers are hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.



Hop-by-Hop Option

- The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.
- Only three hop-by-hop options have been defined:
  - Pad1, PadN, and jumbo payload.
- Pad1. This option is 1 byte long and is designed for alignment purposes.
- PadN. PadN is used when 2 or more bytes are needed for alignment.
- Jumbo payload. Length of the payload in the IP datagram can be a maximum of 65,535 bytes.

Destination Option

- The destination option is used when the source needs to pass information to the destination only.

- The format of the destination option is the same as the hop-by-hop option.

Source Routing

- The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.

Fragmentation

- The concept of fragmentation in IPv6 is the same as that in IPv4.
- In IPv6, only the original source can fragment.

Authentication

- The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.

Encrypted Security Payload

- The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

➢ **Advantages of IPv6:**

- ***Larger address space***
  - IPv6 has 128-bit address space, which is 4 times wider in bits in compared to IPv4's 32-bit address space.
- ***Better header format***
  - IPv6 uses a better header format. In its header format the options are separated from the base header.
- ***New option***
  - New options have been added in IPv6 to increase the functionality.
- ***Possibility of extension***
  - IPv6 has been designed in such a way that there is a possibility of extension of protocol if required.
- ***More security***
  - IPv6 includes security in the basic specification.
  - It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH: Authentication Header).
- ***Support to resource allocation***
  - To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification.
  - With flow label mechanism, routers can recognize to which end-to-end flow the packets belong.
- ***Plug and play***
  - IPv6 includes plug and play in the standard specification.
  - It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.
- ***Clearer specification and optimization***

- IPv6 follows good practices of IPv4, and rejects minor flaws/obsolete items of IPv4.

- **Comparison of Options between IPv4 and IPv6**
  - The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
  - The record route option is not implemented in IPv6 because it was not used.
  - The timestamp option is not implemented because it was not used.
  - The source route option is called the source route extension header in IPv6.
  - The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
  - The authentication extension header is new in IPv6.
  - The encrypted security payload extension header is new in IPv6.

12. For the following networks, develop the datagram forwarding table for all the nodes. The links are labeled with relative costs. The tables should forward each packet via the least cost path to destination.

Solution: Initial distance stored at each node.

Information stored at node	Distance				
	A	B	C	D	E
A	0	∞	10	∞	2
B	∞	0	4	2	3
C	10	4	0	1	∞
D	∞	2	1	0	∞
E	2	3	∞	∞	0

Step: 1 To find Initial Routing table at node A.

Destination	Cost	NextHop
B	∞	-
C	10	C
D	∞	-
E	2	E

To find Final Routing table at node A.

Destination	Cost	NextHop
B	5	E
C	10	D
D	7	B
E	2	E

Step: 2 To find Initial Routing table at node B.

Destination	Cost	NextHop
A	∞	-
C	4	C
D	2	D
E	3	E

To find Final Routing table at node B.

Destination	Cost	NextHop
A	5	E
C	4	C
D	2	D
E	3	E

Step: 3 To find Final Routing table at node C.

Destination	Cost	NextHop
A	8	D
B	4	B
D	1	D
E	6	B

Step: 4 To find Final Routing table at node D.

Destination	Cost	NextHop
A	7	B
B	2	B
C	1	C
E	5	B

Step: 5 To find Final Routing table at node E.

Destination	Cost	NextHop
A	2	A
B	3	B
C	6	D
D	5	B

Final distance stored at each node.

CS8591 - COMPUTER NETWORKS

UNIT I - INTRODUCTION AND PHYSICAL LAYER

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching

PART A

1. List the requirements to building a network.

- ✓ Scalable Connectivity
- ✓ Cost-Effective Resource Sharing
- ✓ Support for Common Services
- ✓ Manageability

2. Write the parameters used to measure network performance (May 2016)

- ➢ Bandwidth and Latency
- ➢ Delay×Bandwidth Product
- ➢ High-Speed Networks
- ➢ Application Performance Needs

3. What are the three criteria necessary for an effective and efficient network?

The most important criteria are

- ✓ Performance
- ✓ Reliability
- ✓ Security

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. *Reliability* is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. *Security* issues include protecting data from unauthorized access and viruses.

4. Group the OSI layers by function?

The seven layers of the OSI model belonging to three subgroups. Physical, data link and network layers are the *network support layers*; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the *user support layers*; they allow interoperability among unrelated software systems. The transport layer ensures *end-to-end reliable data transmission*.

5. What are the features provided by layering? (May 2013)

Two features:

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

6. Why are protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

7. What are the two interfaces provided by protocols?

- Service interface

- Peer interface

Service interface- defines the operations that local objects can perform on the protocol.
Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

8. Mention the different physical media?

- Twisted pair (the wire that your phone connects to)
- Coaxial cable (the wire that your TV connects to)
- Optical fiber (the medium most commonly used for high-bandwidth, long-distance links)
- Space (the stuff that radio waves, microwaves and infra red beams propagate through)

9. Explain the two types of duplex?

- *Full duplex*-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
- *Half duplex*-it supports data flowing in only one direction at a time.

10. What is spread spectrum and explain the two types of spread spectrum?

Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.

- Frequency Hopping
- Direct sequence

11. What are the different encoding techniques?

- NRZ
- NRZI
- Manchester
- 4B/5B

12. What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following.
a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

13. Define flow control? (NOV 2011)(May 2015) (May 2016)

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

14. Mention the categories of flow control?

There are 2 methods have been developed to control flow of data across communication links.
a) Stop and wait **-** send one from at a time.
b) Sliding window **-** send several frames at a time.

15. What is a buffer?

Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

16. What is the difference between a passive and an active hub?

An active hub contains a repeater that regenerates the received bit patterns before sending them out. A passive hub provides a simple physical connection between the attached devices.

17. For n devices in a network, what is the number of cable links required for a mesh and ring topology?

- Mesh topology – n (n-1)/2
- Ring topology – n

18. What are the two types of line configuration? (NOV 2010)

- Point-to-point & Multipoint

19. What do you meant by error control? (NOV 2010)(May 2015)

Error control is used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

20. Define Error detection (NOV 2011)

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected

Types of error:

- ✓ Single bit error
- ✓ Burst error

The three error detecting techniques are:

- Parity check
- Check sum algorithm
- Cyclic Redundancy Check

21. What is the use of Two dimensional parity in error detection? (NOV 2012)

- It is based on simple parity.
- It performs calculation for each bit position across each byte in the frame.
- This adds extra parity byte for entire frame, in addition to a parity bit for each byte.

22. What are the issues (Services) in data link layer? (NOV 2012) (May 2016) (Nov 2016)

a) Services Provided to the Network Layer
b) Framing
c) Error Control
d) Flow Control

23. Define network and computer network

A **network** is any collection of independent computers that communicate with one another over a shared network medium. A **computer network** is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

24. List the components of data communication

- ✓ Message
- ✓ Sender
- ✓ Receiver
- ✓ Medium
- ✓ Protocol

25. Define bit stuffing. Give example (MAY 2011) (May 2017)

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

e.g, Sending side - 011111**0**10

26. What are the major duties of network layer? (MAY 2012)

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

27. What are the functions of application layer? (MAY 2011)

- **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

28. Define a layer. (Nov/Dec 2013)

The OSI (Open System Interconnection) Model breaks the various aspects of a computer network into seven distinct layers. Each successive layer envelops the layer beneath it, hiding its details from the levels above.

29. What do you mean by framing? (Nov/Dec 2013) (Nov/Dec 2014)

Frames are the small data units created by data link layer and the process of creating frames by the data link layer is known as framing

30. What is protocol? What are its key elements? (NOV/DEC 2007) (May 2016)

Set of rules that govern the data communication is protocol. The key elements are

i) Syntax ii) Semantics iii) Timing

31. Define (or) mechanism of stop and wait protocol (Nov 2016)

The idea of stop-and-wait is straightforward: After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.

32. Define sliding window algorithm

The sender can transmit several frames before needing an acknowledgement. Frames can be sent one right after another meaning that the link can carry several frames at once and its capacity can be used efficiently. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames

33. Define character stuffing

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by “escaping” the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing.

34. List the 7 OSI layers

- Physical Layer
- Data link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

35. Define hamming distance (Nov/Dec 2014)

Hamming distance = the number of bit positions in which two code-words differ.

Eg. How to calculate ?

(Exclusive OR=XOR):

```
        10001001
        10110001
        ------------
        00111000
```

=> The number of 1's give the number of different bits

36. Write down any two differences between circuit switching and packet switching (Nov/Dec 2014) (May 2017)

Circuit switching

- In circuit switching network dedicated channel has to be established before the call is made between users
- The channel is reserved between the users till the connection is active

Packet switching

- In packet switching network unlike CS network, it is not required to establish the connection initially
- The connection/channel is available to use by many users.

37. Define the terms: Bandwidth & Latency (Dec 2017)

Network performance was measured in two fundamental ways: *bandwidth* (also called *throughput*) and *latency* (also called *delay*).

- The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time
- The second performance metric, latency, corresponds to how long it takes a message to travel from one end of a network to the other.

38. Compare Byte oriented versus Bit-oriented protocol (Dec 2017)

- **Bit oriented** protocol defined as it is a communication protocol it uses individual bits for control codes that bits information should be in byte.
- **Byte oriented** protocol used for framing and communication purpose, in which bytes are used for control codes

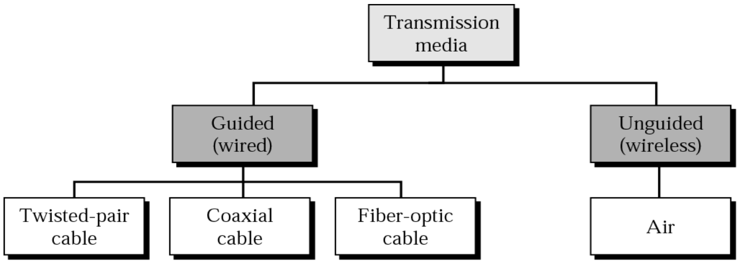
39. Define protocol layering

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**

40. List the types of transmission media

Communication can be made by 2 ways

1. Guided (Wired)
2. Unguided (Wireless



41. Define switching & list its types

SWITCHING

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

Type of switching

- Circuit Switching
- Packet Switching
- Message Switching

42. Define VCI

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the ***virtual-circuit identifier*** **(VCI)** or the ***label.*** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches

43. What is the use of routing table?

The destination addresses and the corresponding forwarding output ports are recorded in the tables. The routing tables are dynamic and are updated periodically.

PART B

1. Discuss the applications, advantages and disadvantages of networks

Applications of Computer Network:-

1.Business Applications
  a.Database resource
  b.Communication Medium
  c.Electronic commerce
2.Home Applications
  a.Internet Access
  b.Personal Communication
  c.Entertainment
  d.Electronic Commerce
3.Mobile Computers
  a.Wireless networks

Advantages of Network

- **Speed**. Sharing and transferring files within Networks are very rapid. Thus saving time, while maintaining the integrity of the file.
- **Cost**. Individually licensed copies of many popular software programs can be costly. Networkable versions are available at considerable savings. Shared programs, on a network allows for easier upgrading of the program on one single file server, instead of upgrading individual workstations.
- **Security**. Sensitive files and programs on a network are passwords protected or designated as "copy inhibit," so that you do not have to worry about illegal copying of programs.
- **Centralized Software Management**. Software can be loaded on one computer (the file server) eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout the building.
- **Resource Sharing**. Resources such as, printers, fax machines and modems can be shared.
- **Electronic Mail**. E-mail aids in personal and professional communication.
- **Flexible Access**. Access their files from computers throughout the firm.
- **Workgroup Computing**. Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently.

Disadvantages of Network

- Server faults stop applications being available
- Network faults can cause loss of data.
- Network fault could lead to loss of resources
- User work dependent upon network
- Could become inefficient
- Could degrade in performance
- Resources could be located too far from users

2. Explain in detail about Networks & Discuss the types and connections of networks

Network :

A **network** is any collection of independent computers that communicate with one another over a shared network medium. A **computer network** is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

Network Criteria:

The most important criteria are
- ✓ Performance
- ✓ Reliability
- ✓ Security

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. ***Reliability*** is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. ***Security*** issues include protecting data from unauthorized access and viruses

TYPE OF CONNECTION:

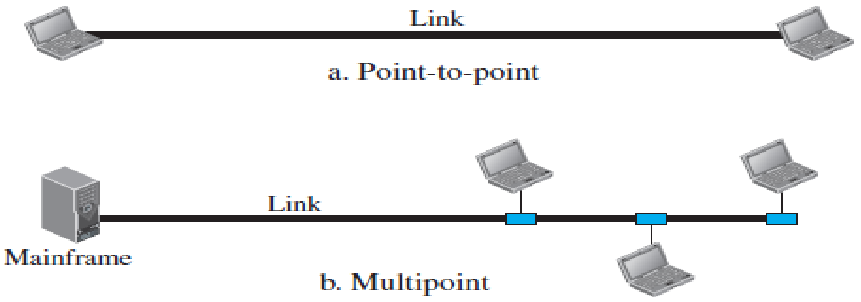
There are two types are,
1. Point to point
2. Multi point

1. Point To Point:

It provides a dedicated link between two devices of the channel. The entire capacity of the channel is reserved for transmission between those two devices.

2. Multipoint:

More than two devices can share a link by using this type of connection. It also called as multidrop. The capacity channel is shared either temporary or spatially. It simultaneously use, it is spatially shared. If it takes turns, it is time shared line configuration



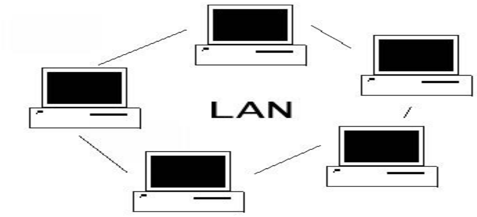
Types of Network

Computer network design is dividing into three basic types such as
- ➢ LAN (local area network),
- ➢ MAN (Metropolitan area network)

- WAN (wide area network)

LAN (Local area networks)

Generally called **LANs**, are privately-owned **networks within a single building or campus of up to a few kilometers in size.** They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.

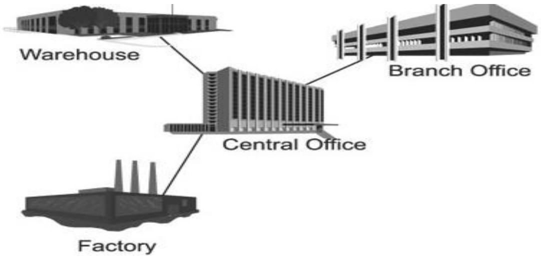


LAN configuration consists of:

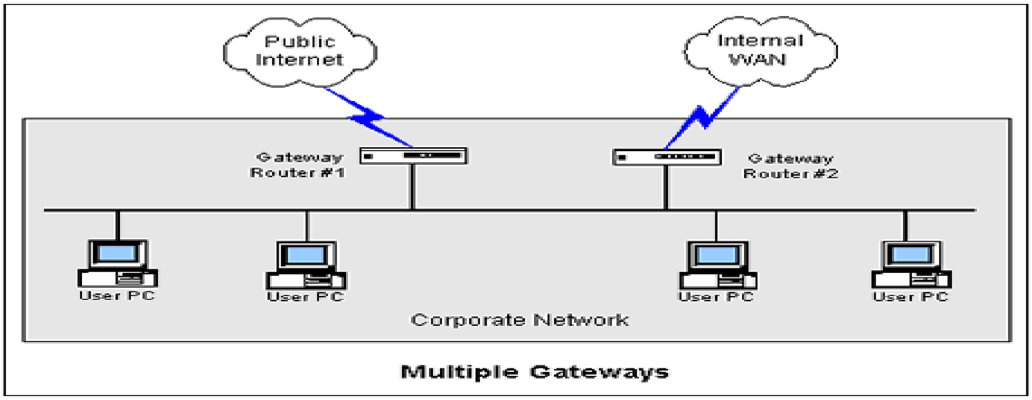
- A file server
- A workstation
- Cables

MAN (Metropolitan area network)

A metropolitan area network (MAN) is a large **computer network that usually spans a city or a large campus.** A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks and the Internet



WAN (Wide Area Network) A **WAN** spans a **large geographic area, such as a state, province or country.** WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs). The world's most popular WAN is the Internet.

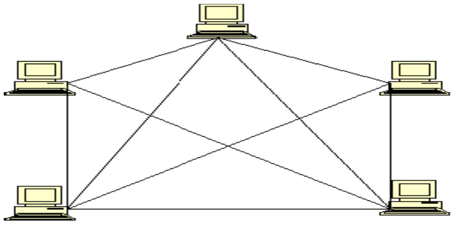


3. Discuss about topology and its types

Network Topologies

Topology refers to the way a network is laid out either physically or logically. Two or more devices connect to a link; two or more links form a topology. It is the geographical representation of the relationship of all the links and linking devices to each other.
1. Mesh
2. Star
3. Tree
4. Bus
5. Ring
6. Hybrid

1. Mesh Topology:
Here every device has a dedicated point to point link to every other device. A fully connected mesh can have n(n-1)/2 physical channels to link n devices. It must have n-1 IO ports.



Advantages:
1. They use dedicated links so each link can only carry its own data load. So traffic problem can be avoided.
2. It is robust. If any one link get damaged it cannot affect others
3. It gives privacy and security
4. Fault identification and fault isolation are easy.

Disadvantages:
1. The amount of cabling and the number IO ports required are very large. Since every device is connected to each other devices through dedicated links.
2. The sheer bulk of wiring is larger then the available space
3. Hardware required to connect each device is highly expensive.

Example:
A mesh network has 8 devices. Calculate total number of cable links and IO ports needed.
Solution:
Number of devices = 8
Number of links = n (n-1)/2
= 8(8-1)/2
= 28
Number of port/device = n-1
= 8-1 = 7

2. STAR TOPOLOGY:
Here each device has a dedicated link to the central 'hub'. There is no direct traffic between devices. The transmission are occurred only through the central controller namely hub.

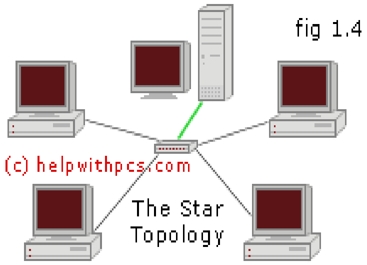


fig 1.4

Advantages:

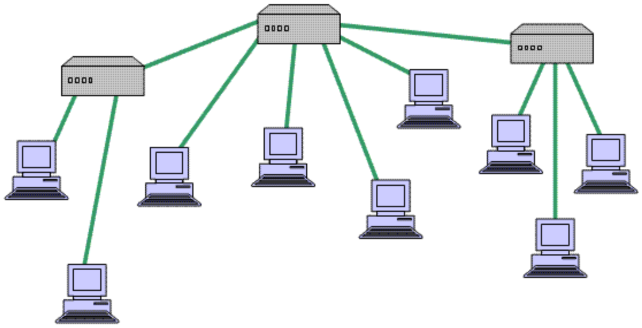
1. Less expensive then mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is need then mesh.
4. Robustness.
5. Easy to fault identification & isolation.

Disadvantages:

1. Even it requires less cabling then mesh when compared with other topologies it still large.

3. TREE TOPOLOGY:

It is a variation of star. Instead of all devices connected to a central hub here most of the devices are connected to a secondary hub that in turn connected with central hub. The central hub is an active hub. An active hub contains a repeater, which regenerate the received bit pattern before sending.



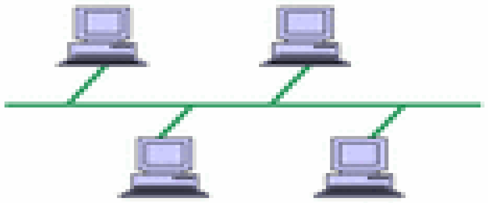
The secondary hub may be active or passive. A passive hub means it just precedes a physical connection only.

Advantages:

1. Can connect more than star.
2. The distance can be increased.
3. Can isolate and prioritize communication between different computers.

4. BUS TOPOLOGY:

A bus topology is multipoint. Here one long cable is act as a backbone to link all the devices are connected to the backbone by drop lines and taps. A drop line is the connection between the devices and the cable. A tap is the splice into the main cable or puncture the sheathing.



Advantages:

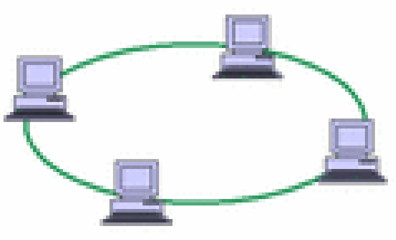
1. Ease of installation.
2. Less cabling.

Disadvantages:

1. Difficult reconfiguration and fault isolation.
2. Difficult to add new devices.
3. Signal reflection at top can degradation in quality
4. If any fault in backbone can stops all transmission

5. Ring topology

Each node is connected to exactly two other nodes, forming a ring. Can be visualized as a circular configuration. Requires at least three nodes



Advantages:

1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

Disadvantages:

1. Unidirectional traffic.
2. Break in a single ring can break entire network.

6. Hybrid topology

A combination of any two or more network topologies.

4. Explain the list of requirements (challenges faced) to building a computer network (May 2017) (Nov 2017)

- ✓ Scalable Connectivity
- ✓ Cost-Effective Resource Sharing
- ✓ Support for Common Services
- ✓ Manageability

1. Scalable Connectivity

Networks (of which the Internet is the prime example) are designed to grow in a way that allows them the potential to connect all the computers in the world. A system that is designed to support growth to an arbitrarily large size is said to *scale*.

Links, Nodes, and Clouds

A network can consist of two or more computers directly connected by some physical medium, such as a coaxial cable or an optical fiber. We call such a physical medium **a *link***, and we often refer to the computers it connects as ***nodes***.

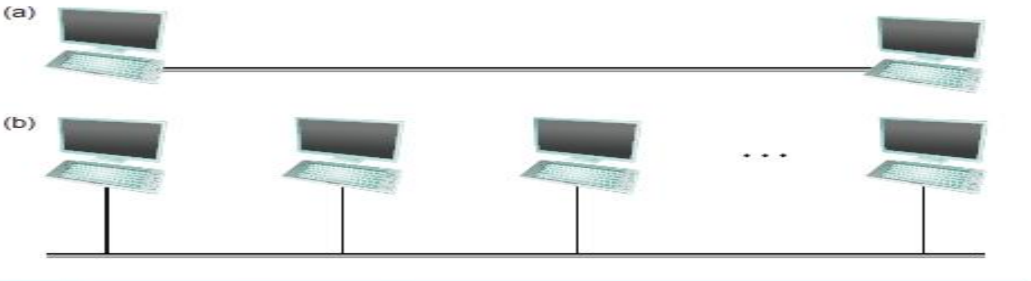


FIGURE 1.2 Direct links: (a) point-to-point; (b) multiple-access.

The cloud distinguishes between the nodes on the inside that *implement* the network (they are commonly called *switches*, and their primary function is to store and forward packets) and the nodes on the outside of the cloud that *use* the network (they are commonly called *hosts*, and they support users and run application programs).

2. Cost-Effective Resource Sharing

Given a collection of nodes indirectly connected by a nesting of networks, it is possible for any pair of hosts to send messages to each other across a sequence of links and nodes. Of course, we want to do more than support just one pair of communicating hosts—we want to provide all pairs of hosts with the ability to exchange messages.

Multiplexing can be explained by analogy to a timesharing computer system, where a single physical processor is shared (multiplexed) among multiple jobs, each of which believes it has its own private processor. Similarly, data being sent by multiple users can be multiplexed over the physical links that make up a network. There are several different methods for multiplexing multiple flows onto one physical link. One common method is *synchronous time- division multiplexing* (STDM).

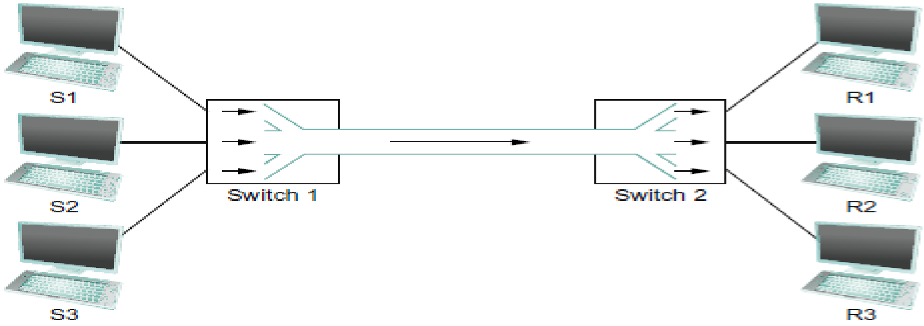


FIGURE 1.5 Multiplexing multiple logical flows over a single physical link.

3. Support for Common Services

The next requirement of a computer network is that the application programs running on the hosts connected to the network must be able to communicate in a meaningful way. From the application developer's perspective, the network needs to make his or her life easier we use a cloud to abstractly represent connectivity among a set of computers, we now think of a channel as connecting one process to another.

Diagram shows a pair of application-level processes communicating over a logical channel that is, in turn, implemented on top of a cloud that connects a set of hosts. We can think of the channel as being like a pipe connecting two applications, so that a sending application can put data in one end and expect that data to be delivered by the network to the application at the other end of the pipe

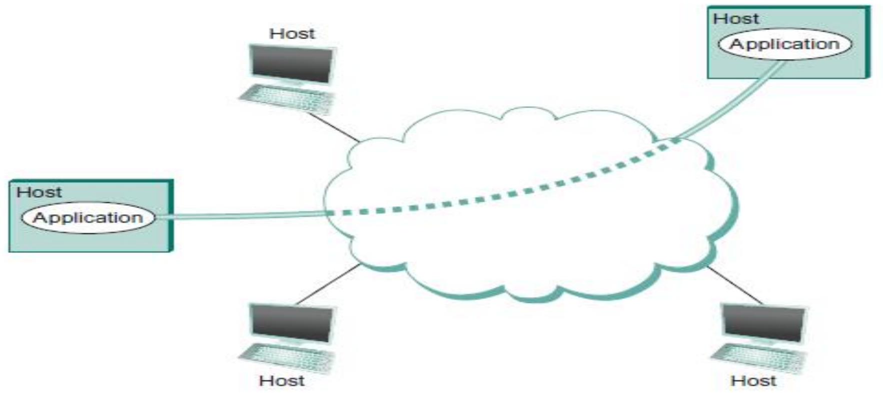


FIGURE 1.7 Processes communicating over an abstract channel.

4. Manageability

Managing a network includes making changes as the network grows to carry more traffic or reach more users, and troubleshooting the network when things go wrong or performance isn't as desired. This requirement is partly related to the issue of scalability discussed above—as the Internet has scaled up to support billions of users and at least hundreds of millions of hosts, the challenges of keeping the whole thing running correctly and correctly configuring new devices as they are added have become increasingly problematic.

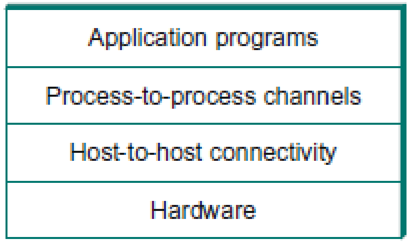
5. Discuss protocol layering in detail

Layering and Protocols

When the system gets complex, the system designer introduces another level of abstraction. It defines unifying model with important aspects of the system, encapsulated this model in interface objects and hide it from users

In network, abstraction leads to layering. Layering provides two nice features.

- It decomposes the problem of building a network into more manageable components. Rather than implementing a monolithic piece of software that does everything implement several layers, each of which solves one part of the problem.
- It provides more modular design. To add some new service, it is enough to modify the functionality at one layer, reusing the functions provided at all the other layers.



Application programs

Process-to-process channels

Host-to-host connectivity

Hardware

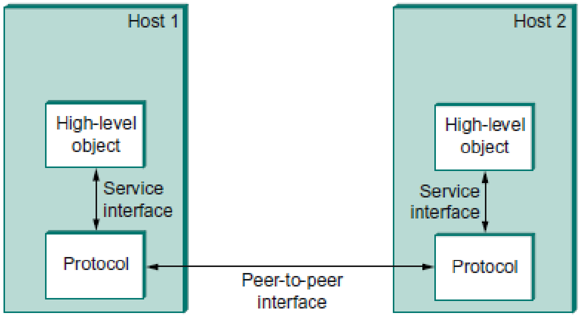
Example of a layered network system.

Protocols

A protocol is a set of rules that governs data communication. It defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Each protocol defines two different interfaces.

- ➢ **Service interface** - to the other objects on the same computer that want to use its communication services. This service interface defines the operations that local objects can perform on the protocol.
- ➢ **Peer interface** - to its counterpart (peer) on another machine. It also defines the form and meaning of messages exchanged between protocol peers to implement the communication service.



■ FIGURE 1.10 Service interfaces and peer interfaces.

Encapsulation

Control information must be added with the data to instruct the peer how to handle with the received message. It will be added into the header or trailer.

Header - Small data structure from few bytes to few kilobytes attached to the front of message.
Trailer – Information will be added at the end of the message
Payload or message body – Data send by the program
In this case data is encapsulated with new message created by protocol at each level.

Multiplexing and De-Multiplexing

The fundamental idea of packet switching is to multiplex multiple flows of data over a single physical link. This can be achieved by adding identifier to the header message. It is known as **demultiplexing or demux key.** It gives the address to which it has to communicate.
The messages are demultiplexed at the destination side. In some cases same demux key is used on both sides and in some cases different keys are used.

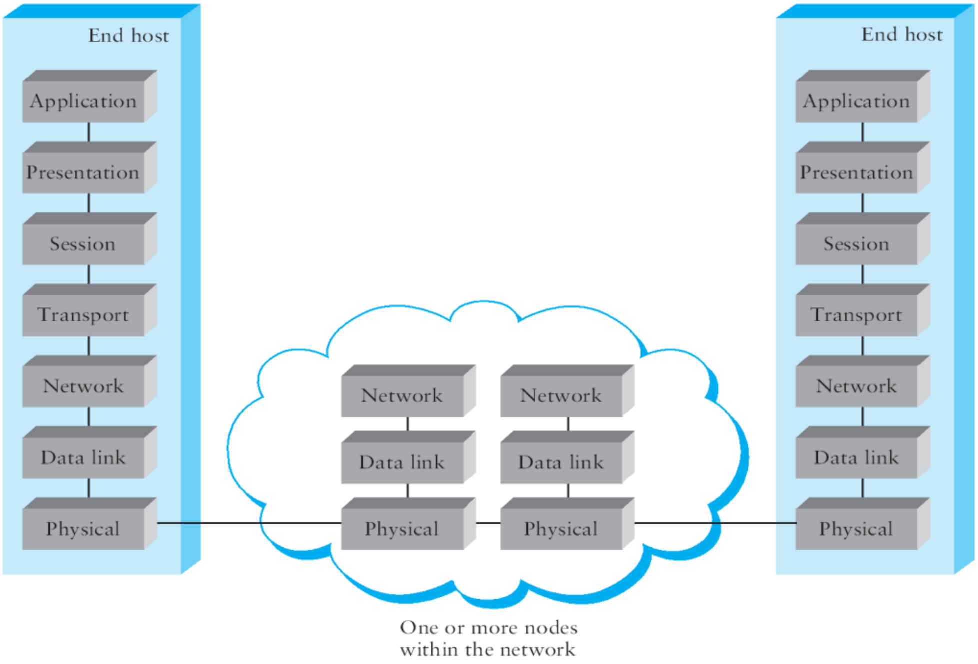
6. Explain OSI model in detail (or) Discuss ISO-OSI architecture in detail

OSI Architecture (NOV 2012) (MAY 2012)

ISO defines a common way to connect computer by the architecture called Open System Interconnection (OSI) architecture.

Network functionality is divided into seven layers.

- **Physical Layer**
- **Data link Layer**
- **Network Layer**
- **Transport Layer**
- **Session Layer**
- **Presentation Layer**
- **Application Layer**



Organization of the layers

The 7 layers can be grouped into 3 subgroups

1. **Network Support Layers**

Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.

2. **Transport Layer**

Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

3. **User Support Layers**

Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

Functions of the Layers

1. **Physical Layer**

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

The physical layer is concerned with the following:

➢ **Physical characteristics of interfaces and media -** The physical layer defines the characteristics of the interface between the devices and the transmission medium.

➢ **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.

➢ **Data Rate or Transmission rate -** The number of bits sent each second – is also defined by the physical layer.

➢ **Synchronization of bits -** The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.

➢ **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

➢ **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. Data Link Layer

It is responsible for transmitting frames from one node to next node.

The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control-** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control-** Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.

It is mainly required, when it is necessary to send information from one network to another.

The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

4. TRANSPORT LAYER

- It is responsible for **Process to Process** delivery.
- It also ensures whether the message arrives in order or not.

The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection-oriented.** The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

5. SESSION LAYER

This layer establishes, manages and terminates connections between applications.

The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization**-This allows to add checkpoints into a stream of data.

6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information exchanged between two systems.

The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

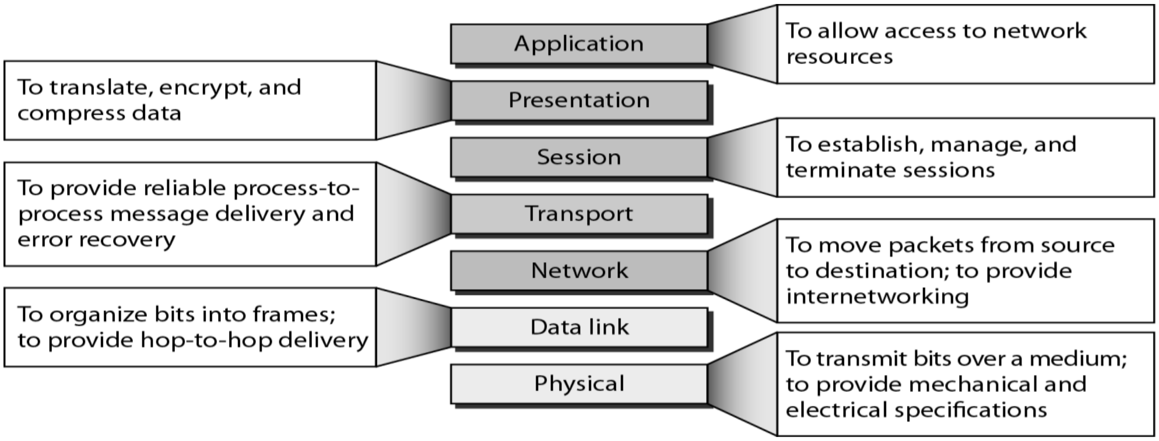
7. APPLICATION LAYER

This layer enables the user to access the n/w. This allows the user to log on to remote user.

The other responsibilities of this layer are

- **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

Summary of layers

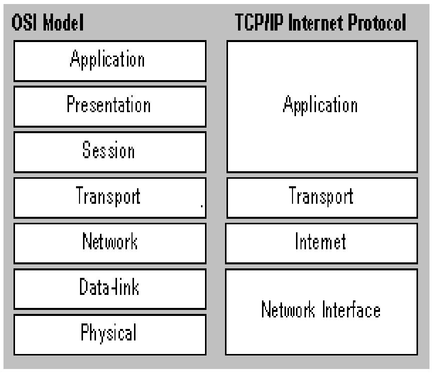

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

7. Explain TCP/IP protocol suite (Internet architecture) in detail (May 2015) (May 2017)

TCP/IP ARCHITECTURE

TCP/IP model is an implementation of OSI reference model. It has four layers. They are

- Network Interface Layer
- Internet Layer
- Transport (also known as Host-to-Host or Transmission) Layer
- Application Layer (known earlier as the Process Layer)



OSI Model	TCP/IP Internet Protocol
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data-link	Network Interface
Physical	

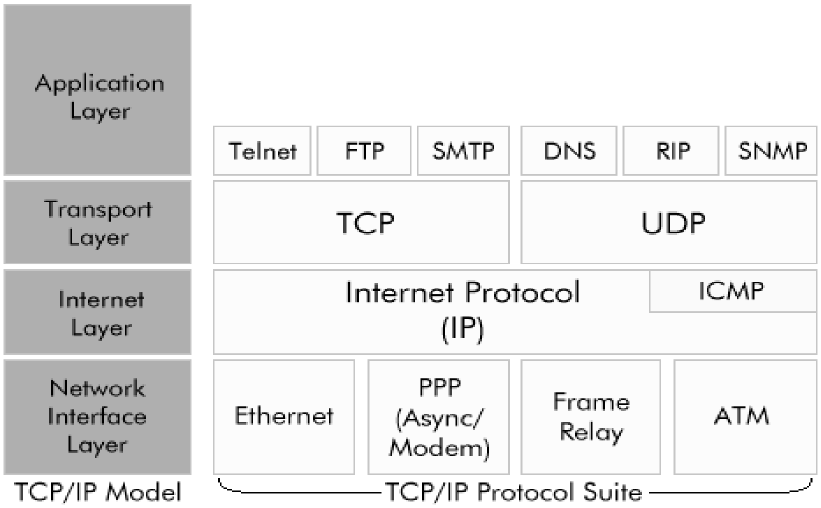


Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*

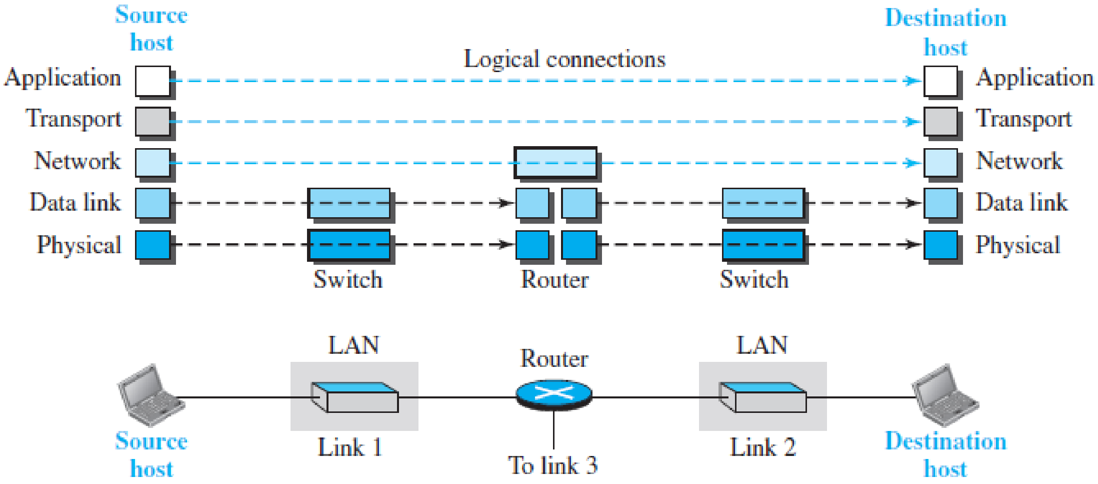
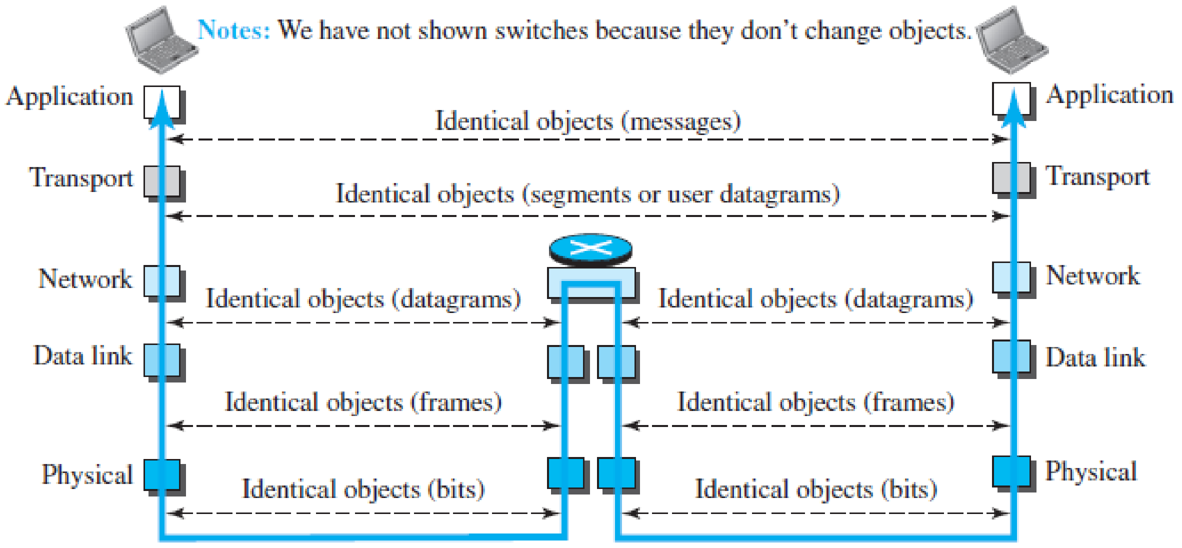


Figure 2.7 *Identical objects in the TCP/IP protocol suite*



Notes: We have not shown switches because they don't change objects.

Application
Transport
Network
Data link
Physical
Identical objects (messages)
Identical objects (segments or user datagrams)
Identical objects (datagrams)
Identical objects (datagrams)
Identical objects (frames)
Identical objects (frames)
Identical objects (bits)
Identical objects (bits)
Application
Transport
Network
Data link
Physical

1) Network interface layer (or) The Host to Network Layer:

Below the internet layer is great void. The TCP/IP reference model does not really say such about what happen here, except to point out that the host has connect to the network using some protocol so it can transmit IP packets over it. This protocol is not specified and varies from host to host and network to network.

2) Internet layer:

Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. They may appear in a different order than they were sent in each case it is job of higher layers to rearrange them in order to deliver them to proper destination.

The internet layer specifies an official packet format and protocol known as internet protocol. The job of internet layer is to transport IP packets to appropriate destination. Packet routing is very essential task in order to avoid congestion. For these reason it is say that TCP/IP internet layer perform same function as that of OSI network layer.

3) Transport layer:

In the TCP/IP model, the layer above the internet layer is known as transport layer. It is developed to permit entities on the source and destination hosts to carry on a conversation. It specifies 2 end-to-end protocols

i) TCP (Transmission Control Protocol)

ii) UDP (User Datagram Protocol)

TCP

It is a reliable connection-oriented protocol that permits a byte stream originating on one machine to be transported without error on any machine in the internet. It divides the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination, the receiving TCP process collects the received message into the output stream. TCP deals with flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

UDP

It is an unreliable, connectionless protocol for applications that do not want TCP’s sequencing on flow control and wish to offer their own. It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

4) Application Layer:

In TCP/IP model, session or presentation layer are not present. Application layer is present on the top of the Transport layer. It includes all the higher-level protocols which are virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP).

The virtual terminal protocol permits a user on one machine to log into a distant machine and work there. The file transfer protocol offers a way to move data efficiently from one machine to another. Electronic mail was used for file transfer purpose but later a specialized protocol was developed for it.

The Application Layer defines following protocols

i) File Transfer Protocol (FTP)

It was designed to permit reliable transfer of files over different platforms. At the transport layer to ensure reliability, FTP uses TCP.

FTP offers simple commands and makes the differences in storage methods across networks transparent to the user. The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client.

FTP does not offer a user interface, but it does offer an application program interface for file transfer. The client part of the protocol is called as FTP and the server part of the protocol is known as FTPd. The suffix "d" means Daemon this is a legacy from Unix computing where a daemon is a piece of software running on a server that offers a service.

ii) Hyper Text Transfer Protocol

HTTP permits applications such as browsers to upload and download web pages. It makes use of TCP at the transport layer again to check reliability.

HTTP is a connectionless protocol that sends a request, receives a response and then disconnects the connection.

HTTP delivers HTML documents plus all of the other components supported within HTML such as JavaScript, Visual script and applets.

iii) Simple Mail Transfer Protocol

By using TCP, SMTP sends email to other computers that support the TCP/IP protocol suite. SMTP provides extension to the local mail services that existed in the early years of LANs. It supervises the email sending from the local mail host to a remote mail host. It is not reliable for accepting mail from local users or distributing received mail to recipients this is the responsibility of the local mail system.

SMTP makes use of TCP to establish a connection to the remote mail host, the mail is sent, any waiting mail is requested and then the connection is disconnected. It can also return a forwarding address if the intended recipient no longer receives email at that destination. To enable mail to be delivered across differing systems, a mail gateway is used.

iv) Simple Network Management Protocol

For the transport of network management information, SNMP is used as standardized protocol. Managed network devices can be cross examined by a computer running to return details about their status and level of activity. Observing software can also trigger alarms if certain performance criteria drop below acceptable restrictions. At the transport layer SNMP protocol uses UDP.

The use of UDP results in decreasing network traffic overheads.

8. Discuss in detail about the network performance measures (Nov 2016)

Like any computer system, however, computer networks are also expected to perform well. This is because the effectiveness of computations distributed over the network often depends directly on the efficiency with which the network delivers the computation's data.

While the old programming adage "first get it right and then make it fast" is valid in many settings, in networking it is usually necessary to "design for performance." It is therefore important to understand the various factors that impact network performance.

- ✓ **Bandwidth**
- ✓ **Throughput**
- ✓ **Latency (Delay)**
- ✓ **Jitter**

Bandwidth

The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

- ***Bandwidth in Hertz***

We have discussed this concept. Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

- ***Bandwidth in Bits per Seconds***

The term *bandwidth* can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Throughput

The **throughput** is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps through this link with *T* always less than *B*. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

Latency or delay

The **latency** or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

- ***Propagation Time***

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance / (Propagation Speed)

- ***Transmission Time***

In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The **transmission time** of a message depends on the size of the message and the bandwidth of the channel.

Transmission time = (Message size) / Bandwidth

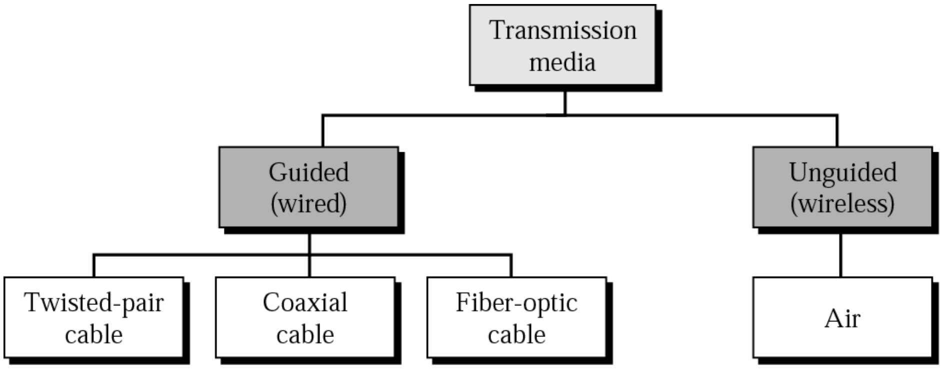
Jitter

Another performance issue that is related to delay is **jitter.** We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

9. Discuss physical links (or) transmission media (or) how communication made by network?

Communication can be made by 2 ways

3. Guided (Wired)
4. Unguided (Wireless)



Guided Media

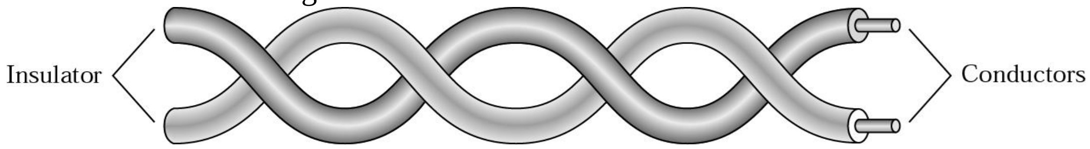
Guided media conduct signals from one device to another include Twisted-pair cable, Coaxial Cable and Fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a glass cable that accepts and transports signals in the form of light.

Twisted Pair Cable

A twisted pair consists of two conductors (normally copper) each with its own plastic insulation, twisted together.

- One of the wires is used to carry signals to the receiver
- Other is used as ground reference



Interference and cross talk may affect both the wires and create unwanted signals, if the two wires are parallel.

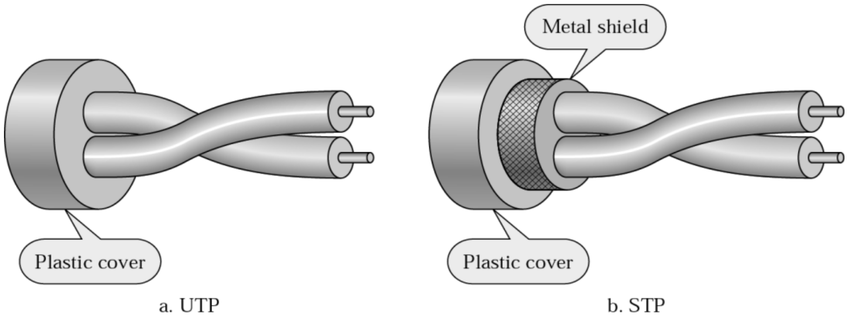
By twisting the pair, a balance is maintained. Suppose in one twist one wire is closer to noise and the other is farther in the next twist the reverse is true. Twisting makes it probable that both wires are equally affected by external influences.

Twisted Pair Cable comes into two forms:

- **Unshielded**
- **Shielded**

Unshielded versus shielded Twisted-Pair Cable

- Shielded Twisted-Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.
- Metal casing improves that quality of cable by preventing the penetration of noise or cross talk.
- It is more expensive. The following figure shows the difference between UTP and STP



Applications

- Twisted Pair cables are used in telephone lines to provide voice and data channels.
- Local area networks also use twisted pair cables.

Connectors

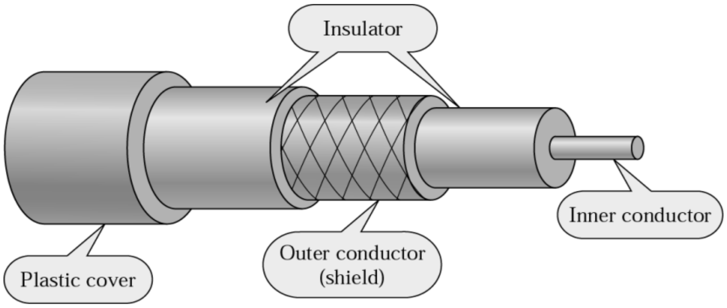
The most common UTP connector is RJ45.

Coaxial Cable

Coaxial cable (coax) carries signals of higher frequency ranges than twisted pair cable.

Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, and with outer conductor of metal foil.

The outer metallic wrapping serves both as a shield against noise and as the second conductor and the whole cable is protected by a plastic cover.



]

Categories of coaxial cables

Category	Impedance	Use
RG-59	75	Cable TV
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

Applications

- ➢ It is used in analog and digital telephone networks
- ➢ It is also used in Cable TV networks
- ➢ It is used in Ethernet LAN

Connectors

- ➢ BNC connector – to connect the end of the cable to a device
- ➢ BNC T - to branch out network connection to computer
- ➢ BNC terminator - at the end of the cable to prevent the reflection of the signal.

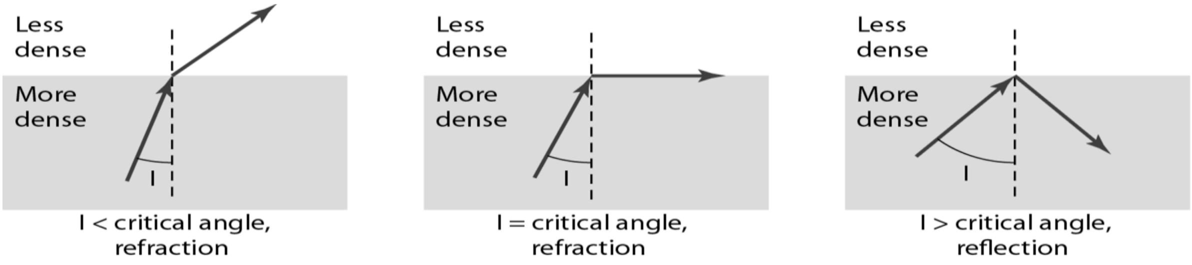
<u>Fiber Optic Cable</u>

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Properties of light

- ➢ Light travels in a straight line as long as it moves through a single uniform substance. If traveling through one substance suddenly enters another, ray changes its direction.

Bending of light ray

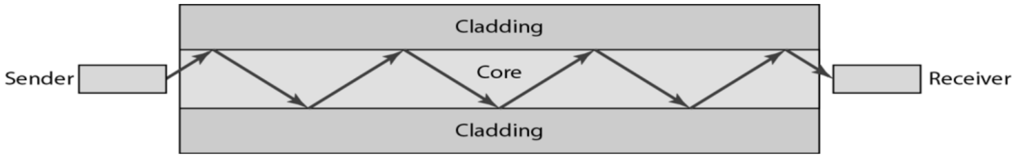

Less dense
More dense
I
I < critical angle, refraction
Less dense
More dense
I
I = critical angle, refraction
Less dense
More dense
I
I > critical angle, reflection

If the angle of incidence(the angle the ray makes with the line perpendicular to the interface between the two medium) is less than the critical angle the ray refracts and move closer to the surface.

If the angle of incidence is equal to the critical angle, the light bends along the interface.

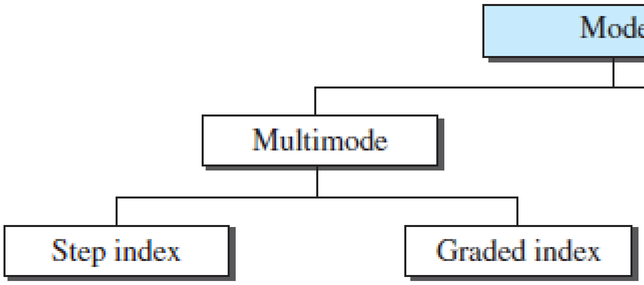
If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance. Critical angle differs from one medium to another medium.

Optical fiber use reflection to guide light through a channel.



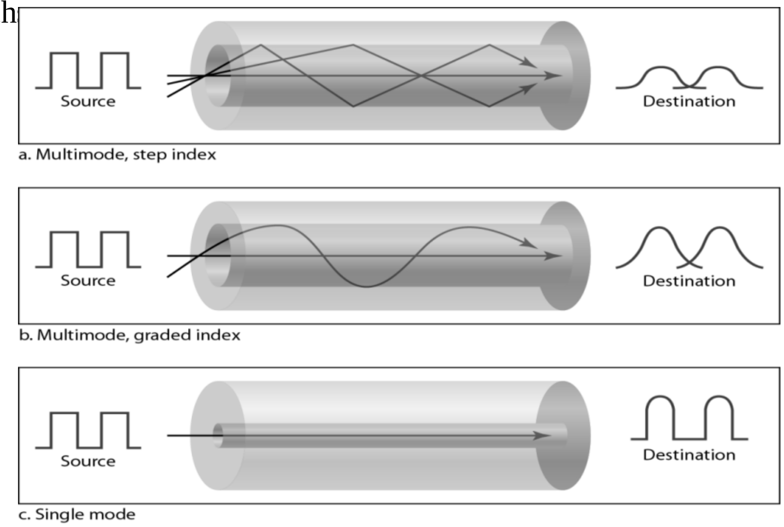
A Glass or plastic core is surrounded by a cladding of less dense glass or plastic.

Propagation Modes



<u>Multimode</u>

In the multiple mode, multiple light beams from a source move through the core in different path



a. Multimode, step index

b. Multimode, graded index

c. Single mode

- **Multimode-Step-Index fiber:** The density of core remains constant from the centre to the edge.

  A ray of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface there is an abrupt change to a lower density that changes the angle of the beam's motion.
- **Multimode- Graded -Index fiber:** The density is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

<u>Single Mode</u>

Single mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

The single mode fiber itself is manufactured with a much smaller diameter than that of multimedia fiber.

Connectors

- **Subscriber channel** (SC) **connector** is used for cable TV.
- **Straight-tip** (ST) **connector** is used for connecting cable to networking devices.

Advantages of Optical Fiber

- Noise resistance

- Less signal attenuation
- Light weight

Disadvantages

- Cost
- Installation and maintenance
- Unidirectional
- Fragility (easily broken)

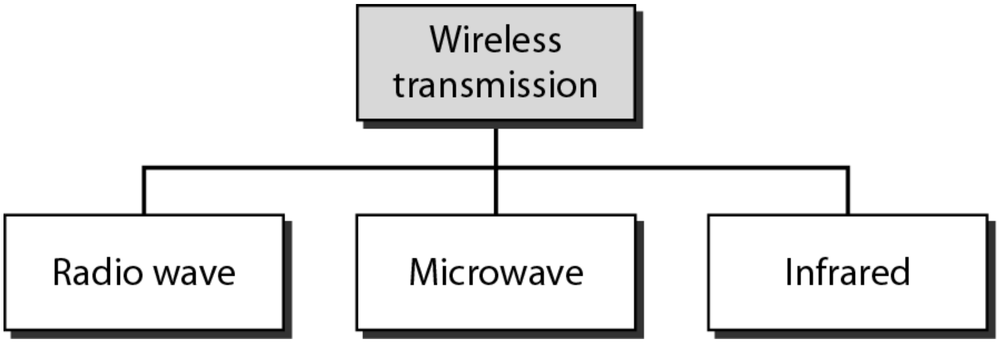
Unguided media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Signals are normally broadcast through air and thus available to anyone who has device capable of receiving them.

Unguided signals can travel from the source to destination in several ways:

- **Ground propagation** – waves travel through lowest portion on atmosphere.
- **Sky propagation** – High frequency waves radiate upward into ionosphere and reflected back to earth.
- **Line-of-sight propagation** – Very high frequency signals travel in a straight line



Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

Properties

- Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

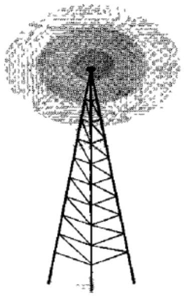


Fig:Omnidirectional antenna

Disadvantages

- The omnidirectional property has a disadvantage, that the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

- As Radio waves can penetrate through walls, we cannot isolate a communication to just inside or outside a building.

Applications

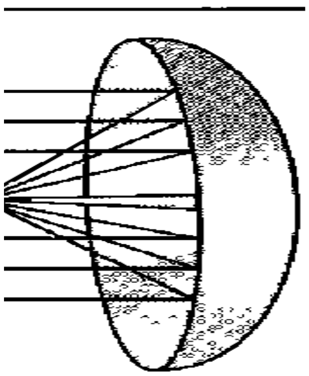
Radio waves are used for multicast communications, such as radio and television, and paging systems.

Microwaves

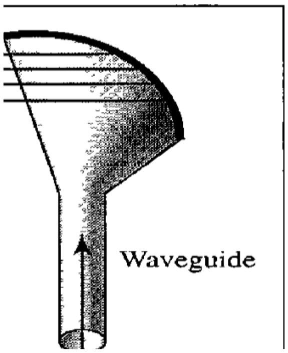
Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Properties

- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned
- Microwave propagation is line-of-sight
- Very high-frequency microwaves cannot penetrate walls



a) ParabolicDish antenna



b)Horn antenna

- Parabolic Dish antenna focus all incoming waves into single point
- Outgoing transmissions are broadcast through a horn aimed at the dish.

Disadvantage

- If receivers are inside buildings, they cannot receive these waves

Applications

- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Infrared

- Electromagnetic waves with frequencies from 300 GHz to 400 THz are called infrared rays
- Infrared waves, having high frequencies, cannot penetrate walls.

Applications

- Infrared signals can be used for short-range communication
in a closed area using line-of-sight propagation.

10. Discuss in detail the concepts of Packet Switched Networks (Packet Switching)

Introduction

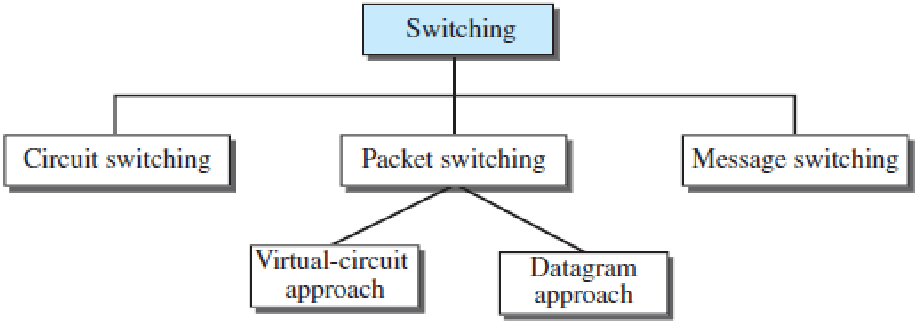
SWITCHING

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

Type of switching

- Circuit Switching
- Packet Switching
- Message Switching

Figure 8.2 *Taxonomy of switched networks*



Advantages of packet switching over circuit switching are as follows:

- Circuit switching is suitable for **voice communication**. When circuit switched links are used for data transmission, the link is often idle and its facilities wasted.

- The **data rate** of circuit switched connections for data transmission is very slow.

- Circuit switching is **inflexible**. Once a circuit has been established, that the path taken by all parts of the transmission whether or not it remains the most efficient.

- Circuit switching treats all transmission as equal. That means, there is no priority among the transmission of data.

The mostly widely used switching technique for data transmission *is packet switching.*
In this, the data are transmitted in the form of *packets*.
If the length of the packet is too long then it is broken-up into multiple packets.
Each packet contains data and also a header with control information.

PACKET SWITCHING:

There are two popular approaches to packet switching:

- Datagram approach and

- Virtual circuit approach

Datagram Approach:

- In the datagram approach, each packet is treated independently from all others.

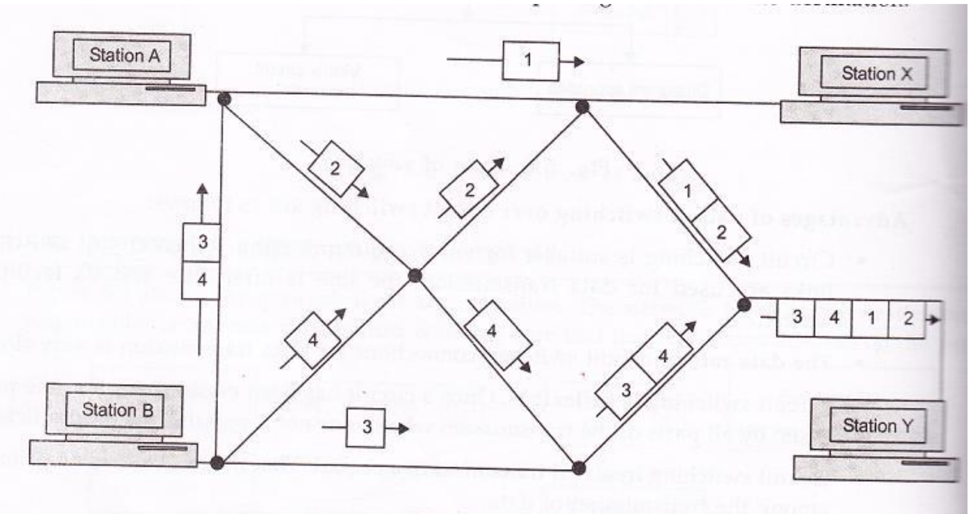
- A datagram is a multipacket of the same message and it works on the principle of ‘send’ and ‘forget’.

The features of datagram are as follows:

- Circuit setup is not needed.
- Each packet contains both source and destination address.
- Each packet routed independently.
- Few packets are lost during crash.
- No effect or router failure.

Example

- The below figure shows how the datagram approach can be used to deliver four packets from station A to station Y.
- In this example, all four packets belong to the same message but may go by different paths to reach their destination.
- This approach can cause the datagrams of a transmission to arrive at their destination out of order.
- In most protocols, it is the responsibility of transport layer to reorder the datagrams before passing them on to the destination.

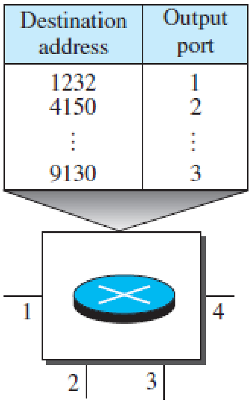


Datagram approach

Routing Table

In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network (discussed later) in which each entry is created when the setup phase is completed and deleted when the teardown phase is over

Figure 8.8 *Routing table in a datagram network*



Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

A switch in a datagram network uses a routing table that is based on the destination address.

Virtual Circuit Approach:

- In the virtual circuit approach, the relationship between all packets belonging to a message or session is preserved.
- A single route is chosen between sender and receiver at the beginning of the session.
- When the data are sent, all packets of the transmission travel one after another along that route.

Virtual circuit transmission is implemented in two formats:

- Switched Virtual Circuit (SVC)
- Permanent Virtual Circuit (PVC)

Switched Virtual Circuit (SVC)

- In the **switched virtual circuit (SVC)** method, a virtual circuit is created whenever it is needed exits only for the duration of the specific exchange.
- If the station A wants to send four packets to station X, first it requests the establishment of a connection to station X.
- Once the connection is established, the packets are sent one after another and in sequential order. When the last packet has been received, the connection is released and that virtual circuit ceases to exist.
- Only one single route exists for the duration of transmission. Each time that station A wants to communicate with station X, a new route is established.

Permanent Virtual Circuit (PVC)

- In the **permanent Virtual Circuit (PVC)** method, the same virtual circuit is provided between two users on a continuous basis.

- This circuit is dedicated to the specific users. No one else can use it, because it is always in place.
- It can be used without connection establishment and connection termination.

Two SVC users may get a different route every time they request a connection whereas two PVC users always get the same route.

Comparison between Virtual circuit and Datagram

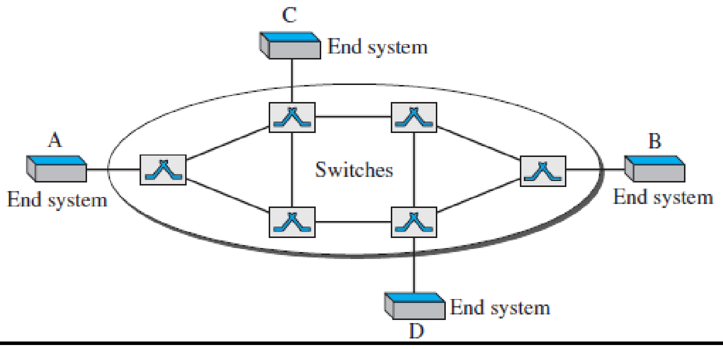
Datagram approach	Virtual circuit approach
In datagram approach, each packet is treated independently, thus they can follow different routes.	In virtual circuit approach, all packets follow the same route.
Packets can arrive at the destination in different order.	Packets should reach the destination in the same order.
Connection establishment is not required before transmission	Connection establishment is required.

Virtual-Circuit Networks – characteristics

A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are **setup and teardown phases** in addition to the data **transfer phase**.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual-circuit identifiers in the next section.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.

Figure 8.10 *Virtual-circuit network*



Addressing

In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

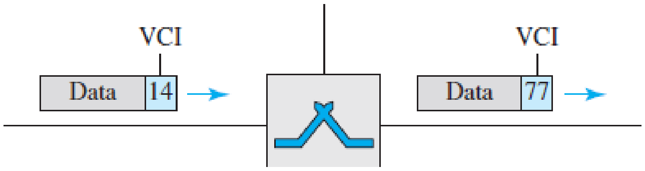
Global Addressing

A source or a destination needs to have a global address—an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the ***virtual-circuit identifier*** **(VCI)** or the ***label*****.** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches.

Figure 8.11 *Virtual-circuit identifier*



Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: **setup, data transfer, and teardown**.

- In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
- In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
- Data transfer occurs between these two phases.

11. Compare circuit switching with packet switching Nov/Dec 2011

Circuit Switching Vs Packet Switching

Introduction

- In circuit switching dedicated communication path is available between two stations.
- It is easier to double the capacity of a packet switched network than a circuit network.
- A circuit network is heavily dependent on the number of channel available.
- It is easier to expand a packet Switching System.
- Circuit switched technologies takes double the cost for more boxes.
- Example: Internet Traffic of the telephone network

Circuit Switching:

Advantages

- Circuit is dedicated to the call-no interference, no sharing
- Guaranteed the full bandwidth for the duration of the call

- Guaranteed quality of service

Disadvantages

- Inefficient-the equipment may be unused for a lot of the call, if no data is being sent, the dedicated still remains open
- Takes a relatively long time to set up the circuit
- During a crisis or disaster, the network may become unstable or unavailable.
- It was primarily developed for voice traffic rather than data traffic.

Packet Switching:

Advantages

- More security
- Bandwidth used to full potential
- Devices of different speeds can communicate
- Not affected by line failure(redirects signal)
- Availability-do not have to wait for a direct connection to become available
- During a crisis or disaster, when the public telephone network might stop working, e-mails and texts can still be sent via packet switching

Disadvantages

- Under heavy use there can be a delay
- Data packets can get lost or become corrupted.
- Protocols are needed for a reliable transfer
- Not so good for some types data streams.

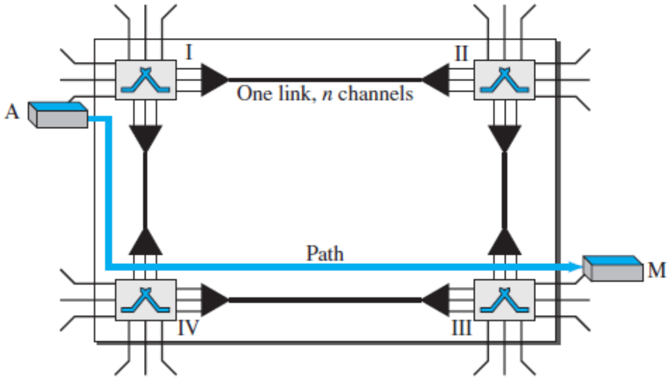
  Example: Real-Time Video streams can lose frames due to the way packets arrive out of sequence.

12. Explain in detail about circuit switched networks

A **circuit-switched network** consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link.

Figure 8.3 shows a trivial circuit-switched network with four switches and four links. Each link is divided into *n* (*n* is 3 in the figure) channels by using FDM or TDM

Figure 8.3 *A trivial circuit-switched network*



We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric.

The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the **setup phase;** a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, the **data-transfer phase** can take place. After all data have been transferred, the circuits are torn down.

We need to emphasize several points here:

❑ Circuit switching takes place at the physical layer.

❑ Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the **teardown phase.**

❑ Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

❑ There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to end addressing used during the setup phase,

Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure 8.3, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

Data-Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

OLD REGULATION - UNIVERSITY QUESTIONS

B.E/B.TECH NOVEMBER/DECEMBER 2014 (2008 regulation)

2 MARKS

1. What is meant by framing (Q.NO 44)
2. Define hamming distance (Q.NO 50)

16 MARKS

1. Discuss the issues in the data link layer (16) (Q.NO 9)
2. Explain in detail the error detecting codes (16) (Q.NO 10)

B.E/B.Tech April May 2015

2 MARKS

1. What do you mean by error control?(Q.NO 34)
2. Define flow control (Q.NO 27)

16 MARKS

1. Discuss in detail about Internet Architecture (16) (Q.NO 6)
2. What is the need for error detection? Explain with typical examples. Explain methods used for error detection and error correction (16) (Q.NO 10 & 13)

B.E/B.Tech Nov-Dec 2015

2 MARKS

1. State the issues of data link layer (Q.NO 37)
2. Define the term protocol (Q.NO 45)

16 MARKS

1. Draw the OSI network architecture and explain the functionalities of every layer in detail (16) (Q.NO 5)
2. Explain the various flow control mechanisms (16) (Q.NO 11)

B.E/B.Tech April-May 2016

2 MARKS

1. Define flow control. (Q.NO 27)
2. Write the parameters used to measure network performance (Q.NO 3)

16 MARKS

1. Explain any two error detection mechanism in detail (16) (Q.NO 10)
2. Explain in detail about HDLC & PPP (8+8) (Q.NO 9)

B.E/B.Tech Nov-Dec 2016

2 MARKS

1. List the services provided by data link layer (Q.NO 37)
2. Write the mechanism of stop and wait flow control (Q.NO 46)

16 MARKS

1. Draw the OSI network architecture and explain the functionalities of every layer in detail (16) (Q.NO 5)
2. a)Discuss in detail about the network performance measures (8) (Q.NO 8)
   b) Explain selective-repeat ARQ flow control method.(8) (Q.NO 11)

B.E/B.Tech April-May 2017

PART A

1. Distinguish between packet switched & circuit switched networks. (Q.NO 51)
2. What is meant by bit stuffing? Give example (Q.NO 40)

PART B

1. i) Explain the challenges faced in building a network (10) (Q.NO 4)
   ii) Obtain the 4-bit CRC code for the data bit sequence 10011011100 using the polynomial x^4+x^2+1 (3) (Q.NO 14)

2.i) With a protocol graph explain the architecture of internet (7) (Q.NO 6)
ii) Consider a bus LAN with a number of equally spaced stations with a data rate of 9 Mbps and a bus length of 1 km. What is the mean time to send a frame of 500 bits to another station, measured from the beginning of transmission to the end of reception? Assume a propagation speed of 150 m/s. If two stations begin to monitor and transmit the same time, how long does it need to wait before interference is noticed? (6) (Q.NO 15)

B.E/B.Tech Nov-Dec 2017

PART A

1. Define the terms: Bandwidth & Latency (Q.NO 52)
2. Compare Byte oriented versus Bit-oriented protocol (Q.NO 53)

PART B

1. With a neat sketch, explain the architecture of an OSI seven layer model (13) (Q.NO 5)
2. Discuss the approaches used for error detection in networking (13) (Q.NO 10)

PART C

1. Outline the steps involved in building a computer network. Give the detailed description for each step (15) (Q.NO 4)