UNIT 3 INTRANET PROTOCOLS

Structure **Page Nos.**

3.0 INTRODUCTION

Protocols are the rules guiding communication over networks. In the context of Intranet and Internet, protocols have greater significance since there are a number of networks trying to communicate to one another, trying to talk in different languages and formats, etc.

Protocol's are called as set of rules

This is similar to the situation where there are different people trying to talk to one another but there are a number of barriers separating them including language, culture, nationality, etc. Protocol helps in translation from one format to another and one network to another.

While there are a number of protocols available for performing varied tasks, only certain important protocols have been listed and described in this Unit. Some protocols are used for communication, some for conversion from one form to another, some for specific tasks, and some even for carrying out cash transactions (also called e-commerce). New protocols are being created for making mobile computing a reality.

It is important that without ensuring proper customer protection, commerce and trade over the Internet cannot function at all. Hence, methods should be evolved to protect the consumer/customer interest, for which proper protocols would be required.

For detailed information about other protocols, text references of computer networking and data communications related subjects may be referred.

The list of protocols is very long. However, an attempt has been made to cover details of most of the protocols in this Unit. It will be of academic interest to note a partial list of well known protocols as following:

ARP, TCP, IP, FTP, Telnet, HTTP, Gopher, WAIS, TFTP, SPX, IPX, UDP, POP, LDAP, SMTP, HTTPS, PPP, SLIP, NNTP, CGI, NetBIOS, IMAP, SOCKS, ISAPI, NSAPI, DMSP, WAP, WSP, WTP, WTLS, WDP, Agora, MilliCent Protocol, SET Protocol, ICMP, IGP, EGP, BGP, IIOP, etc. Further, the details of these protocol's are given in different sections of this Course.

3.1 OBJECTIVES

Almost all the protocols that can be used for the Internet can be used for the Intranet as well. This Unit attempts to bring out the list of those protocols and additional protocols specific to Web servers. Special emphasis is given to protocols such as ISAPI, NSAPI, CGI, etc.

After going through this Unit, you will be able to:

- understand latest protocols;
- understand different communication methods;
- understand mobile communication;
- work on different protocols;
- define the working of Wireless Application protocol (WAP);
- know about the applications of WAP, and
- define E-commerce protocols.

3.2 BASIC INTRANET PROTOCOLS

For the sake of convenience, the protocols have been categorised into two sets, viz., the communication protocols and the service protocols.

3.2.1 Communication cum Mail Protocols

In this Section we will discuss about communication protocols like Address Resolution Protocol and some other Communication Protocols used in mails like Simple Mail Transfer Protocol Post Office Protocols and Internet Message Access Protocol.

Address Resolution Protocol (ARP)

One of the basic communication protocols is the ARP that resolves the IP addresses used by various networking equipments into network usable format that is used by LANs. ARP provides two basic services to the clients viz., it obtains the media access control address for the requesting device, and it records the media access control address in a table called the ARP cache for future use.

The Address Resolution Protocol is situated at the bottom half of the Network layer. It can be considered as a mechanism for mapping or translation of addresses between the Network logical addresses and MAC (Media Access Control) layer physical addresses. For instance, the MAC layer uses a 48-bit address whereas the Ethernet uses a 32-bit address. ARP provides the mechanism to translate the MAC addresses to IP addresses and vice versa using a lookup table like data structure called the ARP cache.

The format of an ARP message is as given below:

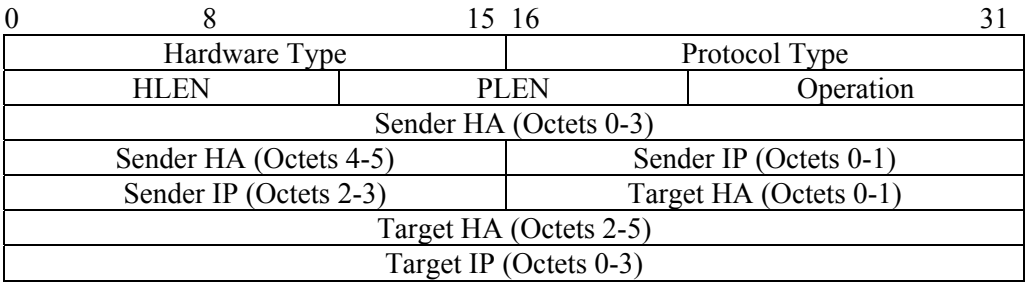


Figure 1: ARP massege format

The greatest advantage of using an ARP is its simplicity since it does not have to perform any kind of computations or otherwise, except that to use the look up table and assign each machine an IP address and decide about subnet masks.

Simple Mail Transfer Protocol (SMTP)

The SMTP protocol is used in the TCP/IP based networks for transferring mail messages between user computers. Most popular freeware for Unix-based SMTP mail programs are Elm and Pine. The other Windows-based software, such as Netscape or Eudora have also become very popular. The Microsoft Outlook that comes with the Windows operating system also uses SMTP to transfer messages and is very popular.

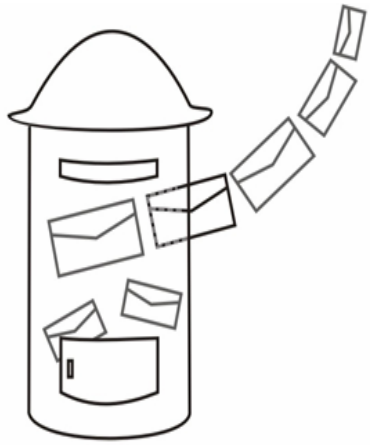
The most notable aspect is that the SMTP works only when both the mail sender and receiver are ready to transact at the same time. Suppose that the receiver computer is not connected or available at that moment, then the messages are stored in a temporary server (may be the nearest gateway or hub). A post office protocol (such as IMAP or POP) must then be used to retrieve the mail.

Since the mail messages cannot have control characters in them, the binary files must first be converted into ASCII. A program called unicode usually does the process of this conversion. Once the mail is sent to the other end, it is converted back to binary or ASCII or whatever format required using another utility program called the unicode.

It should be clear that two separate protocols are used for sending and receiving email (or mail messages). For sending messages, the SMTP is used whereas for receiving at the other end either POP or IMAP is used at their local server. While configuring the email accounts, certain addresses are exclusively declared, viz., the addresses of an SMTP server, a POP server, the address where returned messages are to be sent, and the basic server where the user has his email account.

There are two main difficulties using the SMTP protocol, i.e., the message of size more than 64 KB cannot be handled and the second is the time out. Whereas the first problem could be overcome with newer implementations of the operating systems as well as attaching files as attachments to the main messages, the second problem continued as both the client and server can have different timeouts, and quite naturally, one of them may timeout very quickly keeping the other busy or unexpectedly terminate the conection.

Post Office Protocol (POP)



Post Office Protocol

As the name indicates, the POP delivers all the messages stored on the server to the user's email account. It can be configured in such a manner that the user can obtain emails from his multiple email accounts into his only email software installed on the computer such as the Microsoft Outlook or Outlook Express. This facility is also available on almost all the Internet-based email Web sites such as Hotmail, Yahoo, etc.

Like the SMTP, the POP is also a very simple protocol and can be easily written for a command-line-based application. With the advent of a number of Windows based applications, the difficulty of writing such command-line based applications has totally vanished and the work of the user has become much easier. Similar applications have evolved over the Unix-based implementations as well.

Note that it is easy to write code for simulating a client by use of telnet to connect to the server, and then enable the client to do email-related tasks such as logging into the account, logging off, downloading the emails, deleting them, etc.

The transactions begin with the initiation of a session when newly logged in, and it is possible to do only three things, viz., get the username, get the password or quit the session. Once logged into the mail server, the transactions allow doing the following tasks:

Table 1: Transaction on mail Server

STAT	Gives the number of messages in the box as well as total size of those messages in bytes.
LIST	Gives the list of messages in the mailbox
RETR **msg**	RETR retrieves a message. It uses the message number as generated using the LIST command
DELE **msg**	Deletes a message. Message would be permanently deleted with the sessions ended using the QUIT command. Messages can be undeleted using RSET command
TOP **msg n**	Returns the headers of desired message and also **n** lines of its body

Internet Message Access Protocol (IMAP)

Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mail from the local server. The method of functioning of IMAP is very much similar to that of POP but there is a little difference between the two.

While both POP and IMAP deal with the receiving of e-mail from the local server, POP just stores and then sends the messages whereas IMAP acts totally as a remote file server.

IMAP is more popular for the Internet-based email services but the POP is gradually taking up the lead. IMAP acts more or less like a client/server type protocol wherein the messages are kept on a server and the user connects to it for viewing. In order to download the mail message, the user has to decide it by viewing only the header part and name of the sender. The only interesting part of IMAP services is the creation and use of folders (also called mailboxes), delete messages, or search for certain parts. The downside is that the IMAP requires continuous access to the mail server while the user is in session in order to keep the content and connection alive.

IMAP has the ability to view the mail messages not only by arrival number but by using attributes as well. In this kind of output the folder or the mailbox looks like a relational database table rather than just a collection of messages.

3.2.2 Service Protocols

Many Internet users are familiar with the protocols such as TCP/IP to connect to the Internet. These include those protocols that permit the users to logon to remote computers, such as the following:

- World Wide Web's Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Telnet (Telnet)
- User Datagram Protocol (UDP)
- Simple Mail Transfer Protocol (SMTP).

These and other protocols are often packaged together with TCP/IP as a "suite." Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. In combination with the IP, it is known as the UDP/IP suite.

Though not very well known otherwise, other protocols are used by network host computers for exchanging router information such as:

- Internet Control Message Protocol (ICMP)
- Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP)
- Border Gateway Protocol (BGP).

Personal computer users connect to the Internet through the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). These Protocols use the Internet

Protocol (IP) at the base so that the data can be sent over a dial-up phone connection to an access provider's modem.

Transmission Control Protocol (TCP)

It is well known that the Internet uses different types of topologies, data transfer rates, packet sizes, and other related technologies. Keeping these issues in mind, the TCP has been specifically designed to provide a reliable end-to-end service over an unreliable connection. The TCP was initially designed for either proprietary or Unix-based operating systems so that they communicate with one another avoiding unreliable and slow physical transport of data. It attained such great popularity that it has become the standard protocol for every software and hardware to communicate with one another.

The entire message or data to be sent over the Internet is divided into various Units or packets for efficient routing through the Internet. The TCP is a protocol that is used in conjunction with the Internet Protocol (IP) to send the data in the form of message Units between computers over the Internet. While IP takes care of handling the actual routing or delivery of the data, TCP keeps track of each individual Units of data.

Even though every packet has the same destination IP address, they arrive at the destination through different routes over the Internet and are finally reassembled at the destination to make it a complete message or data as was sent. This breaking of message or data into packets before transmission and then rearranging at the destination in proper order after receipt of all Packets is called disassembling and assembling respectively and done by a specific portion of TCP called the Packet Assembler and Disassembler (PAD).

TCP falls under the category of connection-oriented protocols, which means that a connection or session is established and maintained until the message or messages has been exchanged totally.

Internet Protocol (IP)

The Internet Protocol (IP) is responsible for sending data from one point to another (may be through different routes) on the Internet and is also used for intranets. Every point or computer must have a unique IP address that gives an identity to that particular computer on the Internet. This unique address of the sender as well as the destination machine is put on the data packet before sending and the Internet gateway decides where to send this packet based on this IP address. The packets keep travelling through gateways to smaller networks till reaching the nearest machine or the immediate neighbourhood or server and then are finally delivered to the destination computer. When all the packets have arrived at the destination, the TCP (which is a connection-oriented protocol) keeps track of the sequence and puts all of them into a proper order so that the message or data is built up as was sent originally.

IP falls under the category of connectionless protocols, which means that there is no permanent established connection between the sender and receiver of the message or data. In other words, each packet is permitted to pass through the Internet as an independent Unit of data. In the Open Systems Interconnection (OSI) communication model, IP sits in the third layer called the networking layer.
It is the responsibility of the Internet authorities to assign the appropriate range of IP numbers to different organisations. Thereafter, it becomes the job of the organisations to assign IP numbers to its departments and users.

For an organisation, there are two sets of IP addresses. This is where the difference between the Internet and the Intranet come into the picture very clearly. One is used to communicate with the outside world, also known as the static IP. This is, in other words, used for Internet connectivity, whereas the other is the one used for internal use. The internal IP is not communicated outside the network limits and is usually

called the internal IP address or subnet address. The internal IP identifies a network component for use over the Intranet or sometimes on the LAN. The server handles the task of network address translation (NAT) using which the IP address for external use is translated or mapped onto the one for internal use and vice versa.

The purpose and benefit of a second set of IP addresses for internal use is that the second set makes it possible to address a large number of computers and other network devices or a group of LANs that further have a number of devices installed within an organisation by the method of pooling the IP addresses. With a broad view, it looks as if a number of devices and subnets might be using one single (static) IP address to communicate with the outside world. Compare this with the concept of an EPABX of an organisation. The organisation, instead of leasing 300 direct telephone lines for internal use, prefers to have an EPABX installed so that the 30 direct lines from the telephone exchange are properly utilised or pooled among a large number of users as well as all the internal communication costs are reduced to zero.

When it comes to computers trying to connect to an Internet Service Provider or ISP such as VSNL, MTNL, etc., it becomes difficult to manage thousands of users at a time. Hence, a mechanism has been developed wherein an IP address is allocated to the user when he logs on to the ISP's network dynamically. This IP address is also called dynamic IP address and it changes everytime the user logs on to the ISP's server.

The IP addresses are divided into four classes as shown in *Figure 2*. since networks vary in size, which the organisations decide when applying for a static IP address:

- Class A addresses are for extremely large networks or gateways, usually given at the level of one per country.
- Class B addresses are for large networks, or extremely large organisations.
- Class C addresses are for small networks (fewer than 256 devices) or may be for those at the level of organisation.
- Class D addresses are also called multicast addresses, normally for representing devices and computers on the networks.

The class of addresses used by a device or network is identified by the first few bits of each IP address. The address structures look like this:

Class A

0	Network (7 bits)	Local address (24 bits)

Class B

10	Networks(14 bits)	Local address (16 bits)

Class C

110	Networks(21 bits)	Local address (8 bits)

Class D

1110	Multicast address (28 bits)

Figure 2: Four classes of the IP addresses

The IP address is usually expressed as a combination of four octal numbers with each number representing eight bits, all of them separated by periods, such as 202.64.15.30. The number 202 represents the class A network (usually for India), the second number would represent a large organisation or a service provider (in this case it is VSNL), the third number represents a server (here it indicates a server of the VSNL at New Delhi) and finally the fourth number would indicate a particular user connected to that server.

The present version of IP is IPv4 that supports 32 bits. Very clearly, it is possible to address only $256 \times 256 \times 256 \times 256$ computers or devices or networks on the Internet. In short this amounts to 2^{32}. But the actual number of all devices or networks is

many times more than this. The Internet's explosive growth made it possible to address (or pool or multiplex) many subnets for each IP address. However, it is proposed in the new version of IP called as IPv6 to use 128 bits thereby enabling the addressing of many more networks and computers to communicate simultaneously over the Internet without any difficulty.

TELNET

When it is required to develop and test software for another operating system such as Sun Solaris or SCO Unix while working on a Windows NT based computer, it is preferable to connect to the computer that is actually running on Sun Solaris or SCO Unix and run all the commands on that while viewing the output at this Windows NT based computer. This situation resembles something like a terminal emulation kind of working and is possible through the telnet protocol. It is possible to work on the ISP's server by connecting to it as a regular user (from a remote computer) and run all the Unix based commands on it even though the user might not be having Unix installed at his location.

The Telnet protocol is used to establish an on-line connection (or connection oriented service) to a remote machine. It gives the impression that the user can access someone else's computer (also called a host computer) and that all the required permissions have been given.

A Telnet command for requesting connectivity to the Roorkee University (now IIT Roorkee) might look like the following:

telnet rurkiu.rurkiu.ernet.in

Once the connection is granted by the host computer, the user will get an invitation message to log on with a proper username and password pair. If the pair is acceptable to the host, the user would be logged on like any other regular user. Telnet is mostly used by program developers and anyone who needs to use specific applications or data located at the required host computer.

Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is an application level protocol and has become the standard Web service protocol. It enables transfer of files that may include text, graphic images, sound, video, and other multimedia files on the World Wide Web.

Essential concepts that are part of HTTP include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests.

A Web server is a computer that has a certain amount of space allocated separately and contains a lot of information in the form of HTML files along with other files such as images, voice, etc. An HTTP daemon or HTTPd is a program that is designed to wait for a number of incoming HTTP requests and respond to them when they arrive. The standard Web browser installed at the clients' computers generates requests that are handled at the server by this HTTPd. On users demanding to see the Web pages by typing in the Uniform Resouce Locator (URL) of the organisation or Web server such as *http://www.hotmail.com* or clicking on a hypertext link, the browser generates an HTTP request and sends it to the IP address indicated by the URL. This URL is translated to IP address by ARP or NAT at different stages to and from the client. The HTTPd at the server receives the request and after any necessary processing, the requested file is transmitted. It should be remembered that the HTTPd has the capability to handle multiple requests at a time.

In short, it can be said that the concept of HTTP is based purely on Request-Response combination, with the client "requesting" and the server "responding" to the requests. The server straightaway processes the request, generates a response, and closes the connection. Thereafter, the server keeps waiting for other requests.

The HTTP protocol consists of two distinct items viz., the set of requests from browsers to server and the set of responses going back to them. All the newer versions of HTTP support two kinds of requests: simple requests and full requests. A simple request consists of just a single GET line pointing to the page desired, without the protocol version. The response is just the raw page (with no headers, no MIME, and no encoding) whereas in full requests the protocol version along with the GET request line is present.

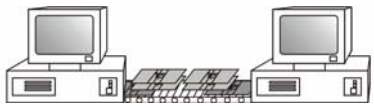
Although HTTP was designed for use on the Web, most widely known methods are GET, PUT and POST. There are other methods also that offer greater flexibility of usage and have been put keeping in view future applications. Some of these methods, are given in Table 1 .The details of usage of HTTP methods are not being dealt with here as they are beyond the scope of this Unit the relevant HTML programming reference should be referred to for further information. The built-in methods of HTTP are given below:

Table 1 : Methods of HTTP

Method	Description
GET	Request to read a Web page
HEAD	Request to read Web page's header
PUT	Request to store a Web page
POST	Append to a named resourse (e.g., a Web page)
DELETE	Remove the Web page
LINK	Connects two existing resources
UNLINK	Breaks an existing conection between two resources

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a standard Internet protocol that offers the simplest way to exchange files between computers on the Internet. Just as the HTTP transfers Web pages and related files and the SMTP transfers e-mail, the FTP is an application protocol that uses the TCP/IP protocol suite. FTP is used to transfer files from one computer to another on the Internet. It is a very popular and commonly used protocol to download and upload applications and other files from the client computers to servers.



File Transfer Protocol

The FTP service is widely popular among Web site developers as well as the students'commUnity for downloading or uploading documents or information to and from desired servers.

Initially, it was available through Unix-based computers only, when the users had to remember a number of commands and their combinations to use the FTP services, but with the advent of Windows-based computers and tools, it has become much easier. Now, one does not need to remember all those commands. Many browsers support FTP-based URL such as *ftp://www.abc.com* (a fictitious address); the idea being that the protocol reference like http can be replaced by ftp if file transfer or file-based operations are desired by the user.

User Datagram Protocol (UDP)

The User Datagram Protocol is a connectionless transport level protocol supported by the IP. It offers a limited service as compared to the conventional TCP and can be used for transferring messages between computers in an IP-based network. In short, it can be said that UDP is more or less an alternative to the TCP and it functions in a suite like TCP/IP called the UDP/IP. Unlike the TCP where the basic Unit of data is called packet, under UDP a data Unit is called a datagram.

0 7 8 15 16 23 24 31	
Source Port	Destination Port
Length	Checksum
Data octets	

Figure 3: User Datagram Header Format

UDP does not divide a message into small packets (or datagrams) and then reassemble them after receipt as it is done with TCP/IP. The basic philosophy behind use of UDP is that the entire message is sent and ensured that the receiver has received the message properly without any errors. UDP is highly useful in those network-based applications that aim at saving a lot of processing time spent on breaking and reassembling them.

It may be remembered that a specific protocol called the Trivial File Transfer Protocol (TFTP) is based on UDP support rather than the conventional TCP. UDP can also be employed for Internet name server applications and usage. UDP offers two additional services not provided by the IP layer. First, it provides the port numbers wherefrom the request has actually been received so that different user requests can be distinguished, and secondly, it provides a checksum that can be used to check whether the data has been received properly or not.

3.3 WEB SERVER SPECIFIC PROTOCOLS

Even though there are a number of protocols available for communicating over the Internet, there are certain protocols available specific for use on Web servers that can be crucial for successful Intranets as well. Special mention goes to protocols such as ISAPI, NSAPI and DMSP. These can also be termed as protocols that handle the requests and are embedded in the server side scripting. Many of them also provide thread management capabilities that are essential for handling multiple requests simultaneously.

3.3.1 Common Gateway Interface (CGI)

It is a well established fact that an HTTP server is used as a gateway to a large repository of information related to an organisation, a product or a concept. The repository could further include massive database applications. The Common Gateway Interface or CGI provides mutual agreement between various HTTP servers on integrating information exchange through gateway scripts and programs as shown in Figure 4.The CGI scripts are used in conjunction with HTML forms to build database applications and query processing.

The following are the two most noticeable disadvantages of a CGI-based application:

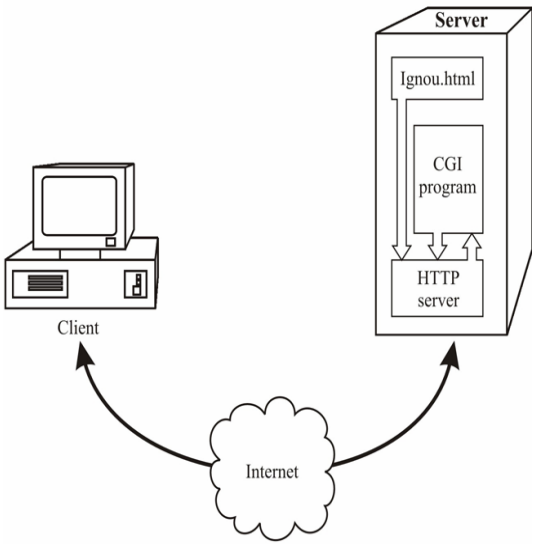
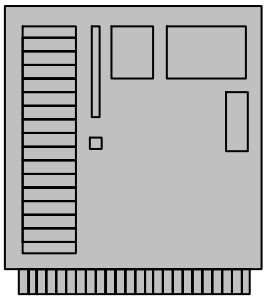


Figure 4: Common Gateway Interface

1. That each time the application is executed, it runs as a separate process with its own address space resulting in execution of unnecessary extra instructions.

This could be troublesome especially when many instances of the same application are running.

2. That the execution speed is extremely slow. It could be due to the references made by the applications, communication speed, the extremely slow compile/execute time and other factors.



Server

A number of good text references are available on the CGI scripting that can be referred for in-depth information.

3.3.2 Internet Server Application Program Interface (ISAPI)

The Internet Server Application Program Interface is purely based on the Windows technology of the Microsoft. It consists of a set of program calls that can be used to include while writing a Web server application. The advantage of ISAPI is that the applications run faster than the counterpart CGI-based applications.

It is possible to create a dynamic link library (DLL) application file using ISAPI that can support the process and address space of the HTTP application. The DLL files are loaded into the computer memory when HTTP request is received and the application is started. They continue to remain loaded as long as they are needed, hence eliminating the chance of locating, reading into storage and executing as frequently as a CGI application does. This increases the processing speed many times.

The existing CGI applications can be easily converted and configured into ISAPI application DLLs without having to rewrite the entire logic. But it is essential to make changes to accomodate the thread management part so that a single instance of the DLL application can support multiple users. In other words, the ISAPI supports the Component Object Module (COM) and Distributed COM (DCOM) concepts. An ISAPI filter is a special kind of ISAPI DLL application file that can be used to receive control of every HTTP request and thereafter they can be used for many purposes such as encryption or decryption, for logging, for request screening, etc.

Since the ISAPI supports COM/DCOM technology, it naturally provides a vendor-independent way of providing many features of the Web server. Quite naturally, it offers far more flexibility than the general CGI interface avoiding all performance limitations. Some of them have been given below:

- An ISAPI code or filter is compiled to a binary-shared library, which is loaded into the Web server itself. For this reason ISAPIs must be compiled separately so that it becomes a position-independent shared library.

- An ISAPI extension or code can provide dynamic content on a Web site. The functionality of an extension is defined by two required interface functions, *GetExtensionVersion* and *HttpExtensionProc*.

The first interface function, *GetExtensionVersion*, is called to check the version numbers and get information about the module. The file is then compiled as a shared library, and placed into relevant directory. If the file was installed then the server will load in the module, and then run the *HttpExtensionProc*, which will automatically send output to the browser.

- Filter is another type of ISAPI module that makes it possible to implement customised logging, encryption, and authentication or path-mapping support. Filters allow users to alter the behaviour of the server whereas extensions can be used for generating content.

The process of serving a request is broken into a number of stages: a filter can ask to be 'notified' as a request reaches each of these stages, intervening at that point to modify the request and the Web server's response. Some notifications come up a number of times for specific requests; some come up for a group of requests and some

others take place just for once-in-a-while for each request. The ISAPI notifications are broadly put as follows:

- Read Raw Data
- Send Raw Data
- Preprocessed Headers
- Authentication
- Access Denied
- On URL Map
- Logging
- End of network session.

3.3.3 Netscape Server Application Programming Interface (NSAPI)

Just as ISAPI is specific to the Microsoft technology, its arch-rival in the market, Netscape has developed the Netscape Server Application Programming Interface. NSAPI. It was created as a more efficient and robust replacement for the CGI. It can also be used to develop applications involving customised authorisation, encryption, or to change certain behavioural or functional aspects of the server operations.

It is an API provided with Netscape Web server to help developers build faster and more complex Web-based applications by extending the server capabilities. NSAPI, CGI and Java (along with JavaScript-based server API) are the three major components of the so-called Netscape's Internet Application Framework.

While the underlying technologies used for ISAPI and NSAPI are similar, the method of handling the addresses the request-response varies slightly. The HTTP transactions in the form of request-response process is handled on the Netscape Enterprise Server through the NSAPI functions, called the built-in server application functions (SAF). Once initialised, the server waits for the HTTP requests from the clients for a file such as a HTML file, a CGI program, or an image file, etc. The following sequence of six steps constitute the request-response process which the SAF executes step-by-step and each step may involve more than one operations.

- *AuthTrans* (authorisation translation) verifies request information (i.e., username and password).
- *NameTrans* (name translation) translates request into a local file system path.
- *PathCheck* (path checking) checks validity of the path and authorisation of the user for path access.
- *ObjectType* (object typing) determines the type of MIME (Multi-purpose Internet Mail Encoding) resource requested by the client.
- *Service* (service) in the form of response to the client.
- *AddLog* (adding log entries) adds related entries to the log file.

NSAPI was basically designed by the designers at the NCSA and CERN Web servers. Thereafter, it has been under continuous observation and development by software developers so that the users may take advantage of its speed, tight integration with the server, and flexibility. The only downside of the NSAPI is that it requires an in-depth understanding of the server processes and their execution.

Unlike the ISAPI, for converting a CGI code or extension, the developers do not need NSAPI, rather than Web Application Interface (WAI) should be used. This WAI is a concept similar to COM/DCOM of Microsoft, but has not got wide popularity even though Netscape products are doing well on the Internet and intranet grounds. Just as COM components can be put in a distributed environment under the concept DCOM, the NSAPI can run in a distributed environment as well since it is based on Internet Inter-ORB Protocol (IIOP).

3.3.4 Distributed Mail System Protocol (DMSP)

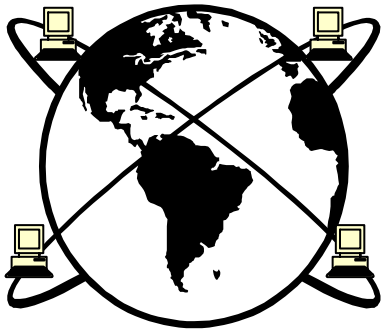
Distributed Mail System Protocol (DMSP) is a lesser known message delivery protocol of the Intranet. The most interesting feature behind its philosophy is that it does not assume that all email messages are placed only on one mail server, as is the case with POP3 and IMAP.

It also offers the facility of multi-session connection for message delivery. In the first instance, it permits the users to download all the email messages from the server to a workstation, computer, or laptop and then disconnect. Now, the user is free to read and answer the email while the session remains disconnected. Whenever the user wishes, the session is established, emails are transferred and the system is automatically resynchronised.

3.4 LATEST PROTOCOLS

The latest technological developments in the field of Information Technology has brought new technologies, concepts, protocols and products, in addition to the numerous protocols discussed above. Though some of them are central to telecommunication technology, they have a greater say in the computing line also since the IT field is formed by overlapping of computing and communication technologies.

The world has been ushered into an era of electronic trading and mobile computing. This section brings out information about such technologies and protocols that guide these latest trends.



3.4.1 Code Division Multiple Access (CDMA)

The CDMA technology spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal. This technology offers a number of benefits to cellular operators as well as to subscribers. To name a few, the following are the benefits of CDMA:

- Capacity increases 8 to 10 times of an analog system.
- Improved call quality, with better and more consistent sound as compared to analog system. It provides voice service very close to wire-line quality.
- Simplified system planning through the use of the same frequency in every sector of every cell.
- Reduced installation time, error rates, inventory of components, maintenance, and many other related benefits.
- Enhanced privacy.
- Improved coverage characteristics, allowing for possibility of fewer cell sites or minimum number of fixed radio sites.
- Increased connectivity time for portables.
- Bandwidth available on demand.
- Near-universal geographical coverage.
- Low equipment cost, both subscriber stations and fixed plant.

CDMA falls under the category of spread-spectrum technology, a family of digital communication techniques used in military applications for many years. The basic principle behind the technology is the use of noise-like carrier waves and bandwidths much wider than those used for point-to-point communication.

There are two philosophies behind the evolution of CDMA derived from military applications,viz.,

- that the enemy'sfforts to jam communications system should be prevented by use of anti-jam or AJ techniques.

- that the enemy should not know that communication was even taking place, by the use of a concept sometimes called Low Probability of Intercept (LPI).

The history of CDMA can be traced to World War II when the application of this communication method was theoretically evolved. Somehow, the method did not get greater acceptability for civilian use but was put to use for military or defence purposes. In spite of the fact that the technology is so strong that it is poised to take over even the conventional mobile communication system, it found limited market in countries like the US and Germany, and interestingly, it is yet to get wide acceptance world wide.

The following factors of CDMA technology are altering the face of cellular and ordinary communication:

- Greatly enhanced telephone traffic capacity (Erlang capacity).
- Greatly enhanced the voice quality by eliminating the audible effects of multipath fading.
- Minimised incidence of dropped calls due to handoff failures.
- Providing reliable transport mechanism for data communication, such as facsimile and Internet traffic.
- Reduced the number of sites needed to support any given amount of traffic.
- Simplified site selection.
- Minimised deployment and operating costs because fewer cell sites are needed.
- Greatly reduced average transmission power.
- Reduced interference to other electronic devices.
- Reduced potential health risks.

The availability of low cost, powerful digital integrated circuits, has reduced the size, weight, and cost of the exchanges or subscriber stations to minimal level. The two major breakthroughs of this technology that made commercial applications possible are that the CDMA technology drives all operators, and it enables the users to use lowest transmission powers.

Since CDMA supports digital technology, it changes the method the subscriber station operates. Programming the features has become extremely easy. Core technology has changed from extreme analog system to extreme digital system. CDMA receivers do not eliminate analog processing totally, but communication channels are separated by means of certain kinds of modulation techniques that are applied and removed in digital form and not on the basis of frequency while all users occupy the same frequency band.

The original system evolved was called the Advanced Mobile Phone System, or AMPS. It is the system everyone uses throughout North America even today. Similar systems with slight variations are used in European and Asian countries.

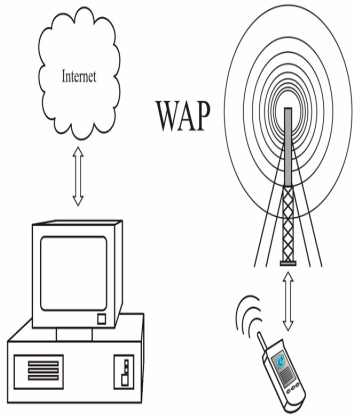
Technically speaking, the spectral allocations for the channels are in the range of 800-900 MHz which can be used for several hundred channels. One channel of one base station is used for each conversation. Upon handoff or change of cell area, the subscriber station is informed via switching message to discontinue the old channel and switch to a new one. Reuse of frequency is the core concept and central to cellular telephony. The channel vacated at a particular cell area can then be dynamically allocated to another user. Contention could arise when all the millions of users try to use the services from one particular cell at a time, which otherwise is a rare or almost impossible situation.

3.4.2 Wireless Application Protocol (WAP)

The Wireless Application Protocol (WAP) is client/server architecture based technology and has been one of the landmark developments in the communications

industry because of the attempt to develop an open standard for wireless protocols, independent of vendor and air link.

The WAP is developed for the micro-browser of the mobile or cell phone. These phones can be considered as hand-held terminals. The WAP servers are programmed to provide simple services to the users since it is not possible to provide complete flexibility of an ordinary browser. Limited services such as providing the result of an examination, the amount balance in the bank account, the temperature and humidity of the day, a simple message service, etc. can be easily provided on the phones. Day by day, new services are being added to the features.



Wireless Application Protocol

WAP is the talk of the town due to the wide hype in the telecom industry as well as outside it. WAP is a standardised method wherein a mobile phone user talks to a server installed in the mobile phone network or exchange. The features of the phone are controlled by software and the phones themselves control switching. The growth in this industry has been so rapid that it has forced all telecom and IT companies to open up departments for producing WAP based technologies in less than a year. WAP is in the news for the reason that it provides a standardised way of linking the Internet and mobile phones, thereby linking two of the largest and most dynamic industries anywhere. The forum that founded the protocol includes major wireless corporates such as Nokia, Ericsson, Motorola, and Phone.com.

Mobile Communication

While some companies support non-voice based services only, some others provide voice mailing, and cell broadcast service also. Some major players in this line are CMG, Siemens, Ericsson, Hutchison, Materna, Motorola, Nokia, NTT DoCoMo, AT&T, Spice and many others

Initially, it was expected that mobile information services would be the most important application for wireless-based applications and would be a grand success as many network operators envisaged but it did not happen. It was with the advent of WAP that the entire scenario changed. However, it has its own limitations which may be listed as follows:

- WAP phones are very difficult to configure for new WAP services, with about 18-20 different parameters requiring to be entered to get access to simple WAP service.
- WAP is a protocol that functions in conjunction with an underlying bearer service protocol. The WAP has been actually developed to provide services in conjunction with wireless service protocols such as the Short Message Service (SMS), Circuit Switched Data (CSD), Unstructured Supplementary Services Data (USSD) and General Packet Radio Service (GPRS). It is notable that almost all these existing bearers have not been properly configured for WAP.
- The greatest difficulty is that the WAP standard, even with the latest WAP version (i.e., ver 1.2) that came in 1999, is not yet complete.
- New protocols such as SIM Application Toolkit and Mobile Station Application Execution Environment (MexE) have already evolved before the proper standardisation of WAP and this could be disastrous for WAP as they are widely supported and aimed to go ahead of WAP.

From the above discussion, it should be clear that WAP could not attain great success due to the launch of the technology much ahead of actually being properly standardised globally, and the blame obviously goes to the wide publicity of the protocol while in its development or infancy stage.

WAP Technology

The basic philosophy behind the WAP approach is to utilise fewest resources possible on the handheld terminals and to utilise all the functionality of the network. Micro browser-based services and applications reside temporarily on servers as well as on phones. In the design of the WAP the standard, application part has been kept

separate from the bearer being used. This separation helps greatly in the switching over from ordinary applications like SMS or CSD to GPRS. In addition, the most important features of WAP are given below:

- Compatibility with any mobile network standard such as Code Division Multiple Access (CDMA), Global System for Mobiles (GSM), or Universal Mobile Telephone System (3GSM). WAP has been designed to work with all cellular standards and is supported by almost all major wireless leaders such as Siemens, AT&T and NTT DoCoMo.
- Support for multiple input terminals such as keypads, keyboards, touch-screens and styluses is provided.

WAP has a layered architecture as shown in *Figure 5:*

Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)
Bearers e.g., Data, SMS, USSD

Figure 5: WAP Protocol Stack

Wireless Application Environment (WAE): The WAE defines the user interface on the phone through the use of the Wireless Markup Language (WML), WMLScript is a scripting language similar to JavaScript and the Wireless Telephony Application (WTA).

Wireless Session Protocol (WSP): A layer that links the WAE and the Wireless Transaction Protocol.

Wireless Transaction Protocol (WTP): Responsible for ensuring proper wireless enabled transaction using protocols such as Wireless Datagram Protocol or standard suite of TCP/IP protocols. WTP offers three types of services: unreliable one way request, reliable one way request and reliable two way request respond.

Wireless Transport Layer Security (WTLS): Just like the transport layer of the OSI model, the WTLS also provides security features that are based upon the established Transport Layer Security (TLS) protocol standard. It also extends services such as data integrity checks, privacy on the WAP Gateway to client, and authentication.

Wireless Datagram Protocol (WDP): This is a protocol very much similar to the UDP except that the WDP uses wireless communication techniques.
The SMS, CSD and the USSD are the three most important of the WAP's underlying bearers:

- Short Message Service: Supports a maximum length of 160 characters per short message.
- Circuit Switched Data: Since CSD has very few users as of today, the WAP could not have a good start with the CSD as well.
- Unstructured Supplementary Services Data: USSD is a means of transmitting information or instructions over a GSM network. USSD has some similarities with SMS since both use the GSM network's signalling path. Unlike SMS, USSD is not a store and forward service and is session-oriented such that when a user accesses a USSD service, a session is established and the radio connection stays open until the user, application, or time out releases it. USSD text messages can be up to 182 characters in length.

Hardware

The type of hardware platform for running the WAP usually consists of a Unix server and other networking devices. Most operators use a Unix platform rather than the Windows NT or other such operating systems.
Even though many majors such as Nokia, Materna, CMG, etc. function on Unix-based platforms, many others such as Ericsson, Siemens, etc. function on platforms based on Windows NT. Yet some others use one with a blend or option of the other.

The most important of all the activities of such powerful platforms are account management and billing system. While the former controls all the details of incoming and outgoing processing and other services, the latter manages to generate subscriber wise reports for billing.

Applications of WAP

Corporate applications that are being enhanced and enabled with a WAP interface include:

- Remote Point of Sale
- Customer Service
- Remote Monitoring such as Meter Reading
- Vehicle Positioning
- Corporate Email
- Remote LAN Access
- File Transfer
- Web Browsing
- Document Sharing/ Collaborative Working
- Audio
- Still Images
- Moving Images
- Home Automation

Consumer Applications that are being enhanced and enabled with a WAP interface include:

- Simple Person to Person Messaging
- Voice and Fax Mail Notifications
- Unified Messaging
- Internet Email
- Prepayment
- Ringtones
- Mobile Commerce
- Mobile Banking
- Chat
- Information Services.

Days are not far when WAP would be used to control airconditioners and refrigerators installed at home directly from anywhere in the world. Users would be able to switch on and regulate airconditioners much before coming back home. Similarly, it would be possible to program washing machines remotely.

3.4.3 General Packet Radio Service (GPRS)

The General Packet Radio Service (GPRS) is a new packet-based service that has been introduced on many GSM and TDMA mobile networks from the year 2000 onwards. It is immediate as there is no dial up connection, relatively fast (up to 177.2 kbps in the very best theoretical high side) and supports virtual connectivity, allowing relevant information to be sent from the network as and when it is generated.

It is expected that the WAP based networks shall also support the GPRS services very soon. It is also possible that if the initial pull from the WAP side were strong through

SMS and Circuit Switched Data services, then SMS would take over GPRS. It is also possible that both the WAP and GPRS services can be provided on the same network and it is left to the user to select the one s/he intends to use.

By any means, it should be rememberded that WAP will play an important role for the development of GPRS-based applications due to the specific nature of WAP stack. The separation of bearer level from the application layer in the WAP protocol stack provides for the ideal, organised and standardised way to use the same application on different bearers.

3.4.4 Protocols for E-Commerce

Technological development has been so rapid in the field of IT that developments did not stop after the design of wireless communication and related services. The standardisation looked ahead towards performing commerce and trade in the virtual world with the use of various technologies available.

Electronic commerce is one of the foremost fields that would straightaway be redefined to suit the needs of the world. This field is relatively very new and a good amount of development has already taken place with the deployment of certain e-commerce based protocols such as Agora, Millicent, etc.

Agora

Agora is a simple and inexpensive Web protocol for electronic commerce. The feature that makes the protocol most attractive is that it supports a high volume of transactions with low incurred cost. It has the following properties:

- **Minimal:** The incurred cost of Agora transactions is close to free Web browsing, where cost is determined by the number of messages.
- **Distributed:** Since Agora is fully distributed, traders and merchants can permit customers without access to a central authority. It becomes possible for the customers to purchase from any merchant provided that they have valid accounts.
- **On-line arbitration:** It is obvious that a number of disputes may arise in trade and commerce. With this property, an on-line arbitrator can settle certain customer/merchant disputes.

The MilliCent Protocol

Just Agora, MilliCent is also a secure protocol for carrying out inexpensive electronic commerce and trading over the Internet. As the name indicates, this protocol was designed to handle purchases and other transactions costing less than a cent.

This protocol is based on decentralised validation of electronic cash at the vendor's server, and that too without incurring any additional processing for encryption, or communication delays or costs, etc. The greatest application has been from brokers for taking care of operations during scrip fluctuations. This helps brokers to check frauds including forgery and double spending. The most notable point is that this protocol is vendor specific.

There are a number of other existing and proposed protocols for electronic commerce that support e-commerce for higher denominations (i.e., of values $1 and above) such as those from DigiCash, Open Market, CyberCash, First Virtual, and NetBill.

The concept of accounts for carrying out transactions is not new in India as Internet users, credit card users as well as telephone users have accounts with the concerned offices that maintain proper account of usage, authenticity of users as well as transactions, provision of additional value added features, and many more. The

customers are billed according to the monthly usage or any other method that suits them well. But the concept of a protocol in line with MilliCent is yet to make an opening in India.

MilliCent reduces the overhead of managing accounts in the following ways:

- Communication costs are greatly reduced by verifying the scrip locally at the **vendors** site since there are almost no MilliCent-specific communication costs for a normal transaction. Moreover, no centralised server for account management or authentication is required.
- Brokers handling all accounts and billing related activities further reduce the accounting costs. After the customer opens an account with a specific **broker**; it becomes the responsibility of the **broker** to maintain and manage the accounts.
- In normal practice, especially in account-based schemes, the vendor maintains the account whereas in MilliCent, the **customer** himself maintains the account.

Millicent is a server protocol for e-Commerce it uses an electronic currency called "scrip". Scrip can be used on the internet to buy electronic good from vendors.

MilliCent assumes a triangular trust relationship among the three entities of the system consisting of customers, brokers and vendors. In trustworthiness, brokers are assumed to be at the top followed by vendors and finally customers. The only time customers need to be trusted is when they lodge complaint about service related problems.

Even though certain security measures are provided, it would be interesting to note that this protocol offers almost no security. Anyone can intercept the scrip and with very little efforts can change the scrip value. From the vendor's side there is absolutely no risk since a digital signature prevents the customer from changing and manipulating the scrip value.

The following precautions can put a check on brokers' malpractices.

- It is possible for the customer and vendor software to independently check the scrip and maintain account balances, so any fraud by the broker can be detected instantaneously.
- The customers should not keep large scrips at any one time. Thus the broker may have to perform a number of fraudulent transactions in order to make even a little profit.
- With fraudulent transactions, the reputation of a broker would also be at stake. A good broker should be attracting more customers and would work for increasing the customer base. It is very clear that a broker would quickly lose the entire business and reputation if any customer has trouble with the broker.

Mostly vendors make the fraud by not providing desired goods for valid scrip. In such a case, customers would lodge a complaint to their brokers, and in turn the brokers may drop the vendors against whom a number of complaints have been lodged. This kind of third party evaluation also helps in policing on the one hand and good vendor rating on the other.
There are three types of MilliCent Protocols with the "Scrip" as the basis of all other protocols:

- "scrip in the clear" is considered the simplest and most efficient protocol. It is the basis for the other two protocols, but it may not be practicable as it is highly insecure.
- "private and secure", offers good enhancement of security and privacy over the earlier, but it is expensive.
- "secure without encryption", is a mix of the above two wherein security restrictions are available, but it also looks for privacy versus efficiency.

This protocol can straighaway be implemented for simple transactions involving articles like those in print and information services that will be available in an online format – journals, articles, magazines, newspapers, encyclopaedias, newsletters, and databases. It can also be used to take care of purchase-sale of general items and essential commodities of use in day-to-day life.

Secure Electronic Transactions (SET) Protocol

The SET is based purely on the science of cryptography that speaks of encoding and decoding messages for communication. This science is not new to us rather it has been in use since the evolution of man. Preserving the secrecy of transactions through strong encryption algorithms, especially for applications like the military, trade and banking, has been described infinite number of times in history books. There has been tremendous advance in the field of encryption with the advancement in computing and mathematics.

Secure Electronic Transactions (SET) is a protocol developed jointly by Visa and MasterCard, involving other computing majors like IBM. SET is an open standard for protecting the privacy and ensuring the authenticity of electronic transactions, especially applicable to the banking sector where the transactions could be in terms of few cents to a millions of dollars.

For the purpose of protecting the interests of the customer/consumer as well as of the traders, methods such as privacy, authentication, encryption, etc., have evolved to provide back to back support for carrying out electronic commerce over the Internet.

The SET protocol is based on two different encryption and one authentication mechanisms. SET uses symmetric encryption using the well known Data Encryption Standard (DES) and asymmetric or public-key encryption to transmit keys for DES transactions. The DES algorithm has been used since the 1970s. An advancements that took place later reduced the key size from the original 128-bits to 56 bits. The SET protocol also uses another popular encryption algorithm, RSA, known after the three scientists who developed it.

The difficulty with the 56 bit key is that it can be easily cracked in a few hours and with an investment of less than a million dollars, which is within the reach of big companies. And this is possible for almost all security and military organisations as well. However, the algorithms and mechanism is proving to be highly useful for banking and commerce applications.

The customer can keep surfing through Web sites and get every information about the products or services of the company, but when it comes to the money transactions, SET comes into play. The customer who intends to place an order for certain products on a company makes payment through credit card number that is authenticated by a third party, usually called as authenticator or intermediary. The third party does not carry out any financial dealing but its responsibility is only to authenticate the transactions. They, in turn, communicate with the banks or vendors and also enable debiting of the amount from the customer's bank account and immediately crediting into the vendor's account. Any failure to do so is also suitably handled during the process and it is ensured that the transaction takes place smoothly and without any fraud.

☞ Check Your Progress 1

1) The _____is situated at the bottom half of the Network layer.

2) Media Access Control Layer uses a _____whereas the Ethernet used a 32-bit address.

3) The SMTP protocol is used in the TCP/IP based networks for _____ between user computers.

4) _____is a standard protocol for accessing e-mail from the local server.

5) UDP stands for _____.

3.5 SUMMARY

There are a number of protocols available for performing varied tasks. Some protocols are used for communication, some for conversion from one form to another, some for specific tasks, and some even for carrying out cash transactions (also called e-commerce). New protocols are being created for making mobile computing a reality.

The world is fast changing. Technology is following the suit. If it is intended to transfer any information directly to a mobile, it should be possible in a few years. Users would be able to connect to the Intranet server through mobile computers or phones and extract whatever they desire. The meaning of life and computing is all set to be redefined.

The day is not far when it would be possible to literally "talk" to various devices like the refrigerator or washing machine installed at home directly from anywhere in the world and program them according to the needs of the user.

The world is setting the stage for carrying out all transactions related to trade and commerce in the virtual world. Though there are certain difficulties in the initial stage, many feel that this kind of transactions would bring them tremendous savings on the one hand and increase business manifold on the other.

Though, the Govt. of India has permitted trading over the Internet, a lot of work is requird in this line to slowly make a shift from the physical world to cyber world. The success of commerce over the Internet or Intranet lies in the success of the protocols. Whether the transactions are done through ordinary leased lines or through wireless connectivity, the protocols have to be used and honoured. While honouring trade and commerce ethics, the protocols should be robust enough to handle every kind of eventuality that might occur due to intentional or unintentional manipulation.

3.6 SOLUTIONS/ANSWERS

Check Your Progress 1

1) Address Resolution Protocol
2) 48-bit address
3) Transferring Mail Messages
4) Internet Message Access Protocol
5) User Datagram Protocol.

3.7 FURTHER READINGS

1) www.martindalecenter.com/Reference-1-Internal html
2) www.iorg.com/intranetorg/
3) www.datex.net/bookstore/internet.html
4) www.hopcottebooks-com/ebooks/intranet.html.
5) *The ABC of intranets* by Refer Dyson, Pat Coleman, Len Gilbert, BPB publiciation.
6) *Computers Network* by Andrew.S.Tanenbaum PHI Private Limited Publication