

स्वाध्याय

स्वमन्थन

स्वावलम्बन

UTTAR PRADESH RAJARSHI TANDON OPEN UNIVERSITY
(Established vide U.P. Govt. Act No. 10, of 1999)



Indira Gandhi National Open University



UP Rajarshi Tandon Open University

BCA- 20
Intranet Administration

FIRST BLOCK : Fundamentals of Intranet Administration

Shantipuram (Sector-F), Phaphamau, Allahabad - 211013

Block

1

FUNDAMENTALS OF INTRANET ADMINISTRATION

UNIT 1

Fundamentals of Intranet 5

UNIT 2

Intranet's Security 21

UNIT 3

Choosing Intranet Hardware and Software 37

UNIT 4

Configuring Intranet 53

UNIT 5

Intranet Authoring and Management Tools 72

UNIT 6

Intranet Protocols 93

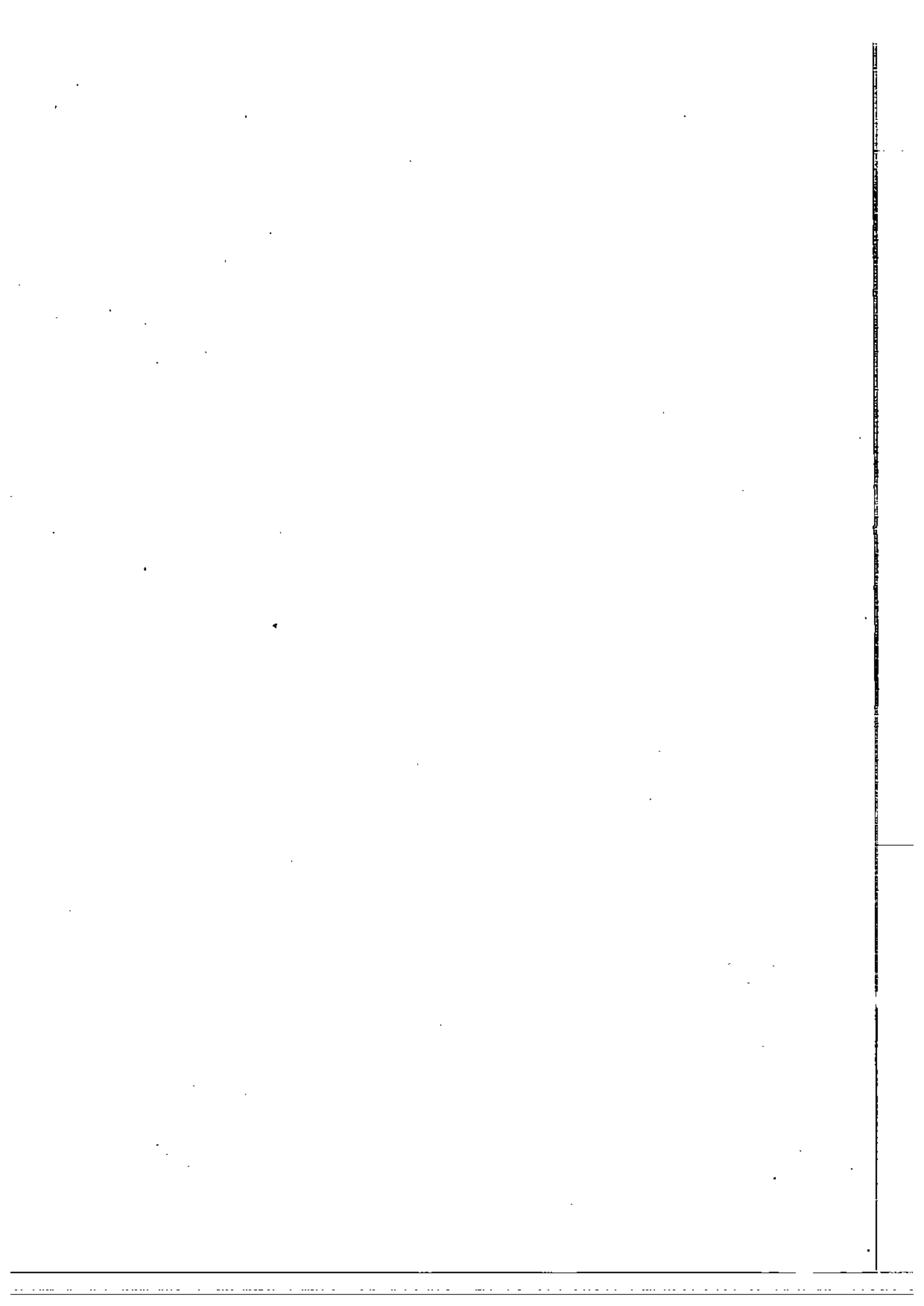
COURSE & BLOCK INTRODUCTION

An Intranet can be as simple as a web server and some HTML pages which users access from their desktop or as complex as several specialized servers running multimedia applications, a technical support Help Desk or Collaborative meeting software converting several remote locations over private networks.

This course (CS 75) deals covers information ranging from the fundamentals of intranets to planning and constructing the intranet. It includes the topics namely :

- **Web browser to access Intranet:** In addition to the fundamentals of the Intranet, various other basic issues related to Intranet, the services offered on it, benefits and limitations has been described thoroughly in this unit. The student is expected to have acquired sufficient knowledge from this unit about intranets, their types and in what way it differs from Internet and local networks.
- **Intranet's security:** Security of the contents put on an Intranet could be of great concern. While highlighting the various kinds of threats to an Intranet, security measures and other related issues essential to protect the Intranet from the threats have been discussed in this unit. It is expected that the student is broadly aware of various technologies available for protecting the intranet and its server through various solutions.
- **Choosing Intranet hardware and software:** A number of software tools are available in the market today. Similarly, hardware of various specifications are available to choose from for building and maintaining an Intranet. Concepts on how to select appropriate hardware and software for running a successful Intranet are dealt with in this unit. At the end of this unit, the student must be capable of making a requirement analysis for setting up an intranet or a helpdesk or a search engine portal.
- **Setting up Intranet Sites:** Once the requirement analysis has been made, it is expected that the student becomes competent to install and configure the intranet after completion of this unit. This unit contains information on how to set up an Intranet site, offer various services/facilities to the users and how to tune them to sustain it successfully.
- **Intranet Authoring and Management Tools:** This unit contains information on various Intranet authoring as well as management tools available in the market. These are the tools that help in improving the look and feel of the information to be hosted on the Intranet and can be used for Internet also. Tools with lots of features are available which can improve the productivity of the professionals as well.
- **Intranet Protocols:** Almost all the protocols that can be used for Internet can be used for Intranet as well. This unit attempts to bring out the list of those protocols and additional protocols specific to Intranet. Special emphasis is given to protocols such as ISAPI, NSAPI, CGI, etc. In addition, certain information on the latest protocols and communication methods through CDMA, WAP, etc., those enable mobile communication have also been incorporated.

This Course contains only one Block.



UNIT 1 FUNDAMENTALS OF INTRANET

Structure

- 1.0 Introduction
- 1.1 Objectives
- 1.2 The Intranet
 - 1.2.1 How Intranet Works?
 - 1.2.2 How big can an Intranet be?
 - 1.2.3 How it is different from Internet?
 - 1.2.4 Intranet vs Internet vs LAN
- 1.3 Advantages of the Intranet
- 1.4 Types of Intranet
- 1.5 Software and Hardware Requirement for Intranet
 - 1.5.1 Hardware
 - 1.5.2 Operating System for Server and Clients
 - 1.5.3 Language Support
- 1.6 Application Areas
- 1.7 Future of the Intranet
- 1.8 Key Intranet Terms
- 1.9 Summary
- 1.10 Model Answers
- 1.11 Further Readings

1.0 INTRODUCTION

The history of Intranet started right from the days when networks came in; however, it found a name and place for itself quite lately. The Websters dictionary defines network as:

Network = The sharing of resources between two or more people - Websters

It is well known that the Internet has been in existence since the mid-70s, and was developed initially by the government as a medium of using communication channels at the time of war. It did not gain substantially in popularity until 1989, when for the first time Web Browser software was introduced and the use of the (HTML or Hypertext Markup Language) came in. Slowly the concept of websites and web hosting picked up. The system was designed from the start, to be very robust, quick, and easy to use. Additionally the system was built to be available cross platform, a fancy way of saying that all computer systems would be able to understand it.

Very quickly, this massive network was destined to become a milestone for the much talked about "information superhighway." This has led to an increasing number of commercial organizations struggling to get to the use of the information technology services, and since mid-1990, the number of businesses connecting to the Internet has multiplied by over 30 times.

Many of these are using the Internet as a source of information and reference material, browsing the World Wide Web (WWW) and Newsgroups for the latest gossip or sharing/known facts on a whole range of issues ranging from life style to technology and spirituality to current affairs. Others use the Internet for transfer of information through the use of messages and data files via e-mail, File Transfer Protocol (FTP) or Gopher sites.

The latest has been the Web commerce that is currently making big news, and many businesses are setting up electronic shops on the Internet in anticipation of safe/secure payment techniques poised to become widely available is being followed. This shall undoubtedly result in an increase in consumer confidence and in turn the customer would look forward for better, reliable and quality service.

Some of those businesses are also using Internet technologies, such as Web browsers and Web servers, in order to provide easy and widespread access to company's information to internal users only. Such networks have been termed as "private Internets", could be considered as sometimes having no connection at all to the outside world, were later became popular as "intranets". Despite the fact that intranets are for internal use only, the challenges for its use and maintenance are no different to those that can be found with the Internet itself. Indeed, building intranets and connecting corporate networks to the Internet is not a simple task.

Companies are turning to the Internet as an established, easily available, yet cost-effective resource that will allow them to gain a competitive edge over other players in the field. The benefits of adopting Internet technology range from lower communications costs (since transporting data across the Internet can cost much less than using a private network) to greatly improved communication speeds. However, it would be notable that there are many different risks involved in having an Intranet in place.

1.1 OBJECTIVES

In addition to the fundamentals of the Intranet, various other basic issues related to Intranet such as the services offered on it, benefits and limitations, applications, etc. has been described thoroughly in this unit. For the benefit of the novice, a list of common terms related to Intranet has been placed at the end of this unit.

1.2 THE INTRANET

The first web browser was called Mosaic, and the HTML concept, although not a new one, has accelerated data access and research. In short, the idea was that although books presented information in a linear fashion, people more often than not have a need to follow it in a three dimensional pattern. Taking an example of a person who might be reading a paragraph on fractals, and then came across a reference to an XYZ Company using this technique for developing software on artificial life. Lot of desired material could be obtained and the person doesn't have to even know what the XYZ Company is. Before the advent of HTML, either the person would have turned to the index page at the back of the book to look for XYZ Company, or even had to go for finding another book to learn about the fractals. Now with the use of HTML, a simple click on the word XYZ Company would take him to an entirely different reference that explains what the company is and what it does. After reading, a hit on the back button would navigate him back to the exact place in the document he had been reading earlier.

Every portion of Internet was designed with the forethought to make it robust and easy to use. It is assured that a number of mistakes have been made during the way, and some back tracking is necessary, but generally speaking Internet has proven to be one of the easiest to use systems ever evolved till date. This could probably be due to the reason that Internet has grown so fast and so vast. The Internet has grown to over 250 million users within 12 years and has already become an integral part of our daily lives.

The literal meaning of the term Intranet as given in various dictionaries is as follows

In' tra net - n.

- 1) A network connecting an affiliated set of clients using standard internet protocols, especially TCP/IP and HTTP.
- 2) An IP-based network of nodes behind a firewall, or behind several firewalls connected by secure, possibly virtual, networks.

An Intranet is the use of Internet technologies within an organization (or company) to achieve better results than the conventional means of data access and transfer. Intranet helps in cutting costs, easy and fast accessibility of day-to-day information. It could refer to a collection of networks at different locations, but catering to the requirements of the same organization.

1.2.1 How Intranet Works?

An Intranet can be defined as a private network, which uses Internet tools. The principal tool is the Web browser, but there are other Internet tools such as ftp and telnet that are useful. The resources defined as private may be protected physically (with a firewall or a separate physical network), geographically (by restricting access to computers with a network address on the local network), or personally (by username and password).

Typically, resources will be private either because they are confidential to the organization (for example, an internal telephone directory), or because they are covered by restrictive licenses (for example, if the Library subscribes to a bibliography whose license restricts its use to members of the University).

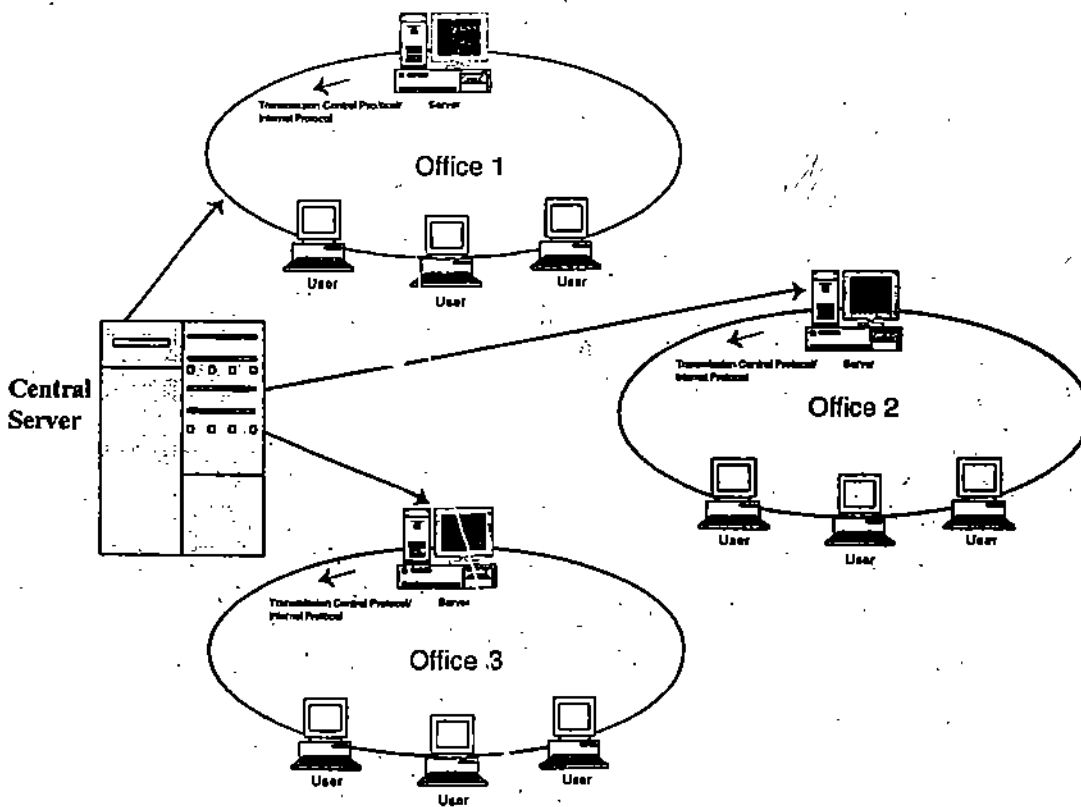


Figure 1 : Intranet is more than a LAN but less than Internet

For an Intranet to work, all computers connected together in a network must speak and understand the same language, or protocol. The language used is HyperText Mark-up Language (HTML) and the protocol that both intranets and the Internet uses are called Transmission Control Protocol/Internet Protocol or TCP/IP. A network server supports all the activities of an intranet. On the clients' side, software known as a browser is used, usually Netscape Navigator or Internet Explorer.

The browser when invoked seeks a server computer through the communication medium that has the first or Home Page of the Intranet, which is usually seen in the folders as 'index.htm'. This is the default page for accessing the intranet from any computer attached to an internal network. This is what automatically appears on the screen when a user logs in and clicks on the browser icon on the desktop for accessing Internet also. The hyperlinks to specific files or databases requests for files send the control from anywhere on the network to the browser. The server accesses the file and sends back a copy of what it contains to the computer or client that has requested for it.

It is the simplicity of TCP/IP that makes Intranets so easy to set-up. Web browsers can be used to connect to virtually any information source, from Structured Query Language (SQL) databases to highly proprietary information systems.

1.2.2 How big can an Intranet be?

As big as a community of interest. Scale is an important factor in web implementation, but it has no bearing on the logical association of clients that make up an intranet. *For example*, a workgroup with one web server, a company with several hundred web-servers, and a professional organization with ten thousand web servers can each be considered an intranet.

While nothing constrains these webs to be "inside" or bounded in any physical sense, size is a significant from a network design perspective.

1.2.3 How it is different from Internet?

Generally an Intranet is different from an Internet in the following ways:

- i) Intranet is a network within the organization whereas Internet is a worldwide network.
- ii) Intranet has access to Internet but not vice-versa.

Once the difference has been defined, the immediate possible question in everyone's mind would be: Is an intranet faster than getting data over the internet? The answer to this would be mix of features of local area network (LAN) as well as that of Internet. Clear answer depends on the possible ways of connecting the client to the network that could be as follows:

- If the network is totally contained within a LAN, then it will get LAN speeds. i.e. the web server is connected via LAN to the client computer.
- If users are connecting remote locations, and use the Internet as backbone / transport, then the speed becomes dependent on the Internet itself, and the speeds by which it is connected.
- If performance is really the issue, users could also run the Intranet over private lines, such as frame relay. Then it can actually contract with the phone company for actual performance levels of speed. i.e. 56 kbps, 256 kbps, etc.
- Approximately Intranet operates at 10 Mbps – 100 Mbps internal and 33.6 kbps for remote access employees.

Answer to question such as "Which is right for the business? Intranet or Internet?" purely depends on how the application is viewed as. The major difference between the Internet and an Intranet is focus: An Internet site looks outward from the company; and an Intranet site is usually for internal use only.

1.2.4 Intranet vs Internet vs LAN

It is certainly possible that both Intranets and the internet can coexist. As spelt theoretically, the entire intranet could be located at a remote site and users who are spread over a number of geographical locations can be permitted to access the data using secure links. Though cutting off the intranet from outside world physically would make it function like a local network, it has its own advantages. The main advantage being a higher level of security. The immediate disadvantage is that if the organization has remote locations it will have to evolve methods for permitting the employees or users to log on to the intranet.

When it comes to comparison between Intranet and LAN, it can be clearly observed that an Intranet is a network within the organization whereas LAN is a campus wide network; geography plays a vital role. Intranet may be considered as a group of LAN's of an organization connected together, could be through a WAN. Naturally, all the facilities that are available in client/server architecture are also applicable here.

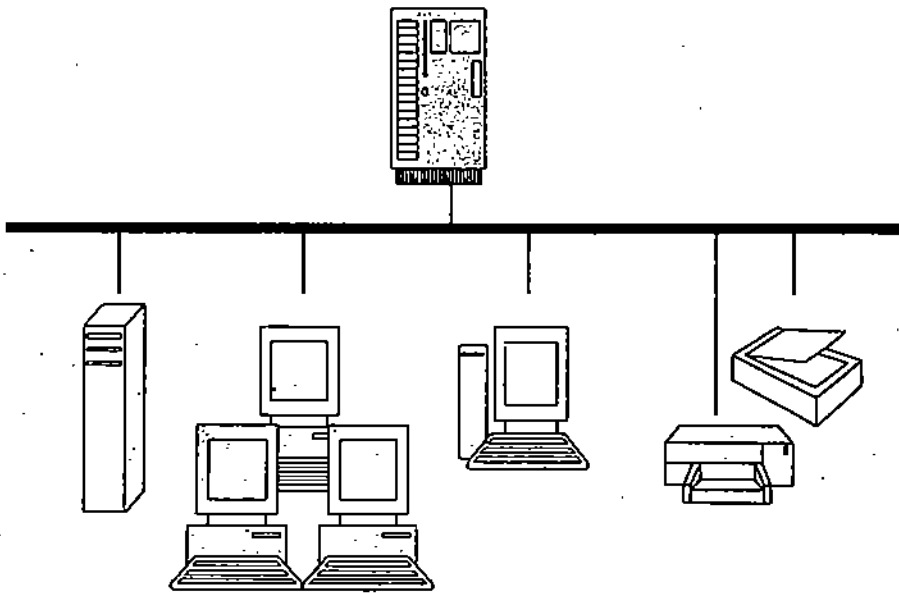


Figure 2: Intranet is a group of LANs interconnected (may be at different locations)

1.3 ADVANTAGES OF THE INTRANET

The most easily noticeable difference between an Internet server and a "collaborative" computing solution such as Lotus Notes (also called groupware, could be used for Intranet server) is the design philosophy. The Lotus Notes has been designed as a proprietary system for areas lacking proper connectivity, it uses a proprietary database structure, which replicates data and does not provide quick access to remote databases.

The real-world benefits and applications of intranets can be many in number. One major benefit of intranets is that it could be used to enhance communication, which in turn could lead to improved linkages within the organization. This communication could happen between various workgroups, departments, or even within entire organization, simply by hosting the contents on the intranet server.

Intranet can largely eliminate paper-based documents, which otherwise become outdated over passage of time. Increased communication will also lead to tremendous reduction in expenditure for numerous publishing services such as creating, printing, and distributing information for internal use. Besides these benefits, Web and conferencing technologies can be easily provided to improve

synergy amongst the employees; still further, collaboration can be enhanced by use of internal newsgroups and mailing lists. Information posted to the newsgroups and distributed via mailing lists can be made available to selected groups within the organization and archived as a repository of information.

Using Internet technologies on an intranet means that organizations can deploy integrated applications that connect public and private networks using the same applications and data. Hence, straightaway standardization of activities or process will find its place. It could be possible that all users have to use the same environment in such an event thereby causing a fear for loss of freedom or creativity, but it has its own advantages.

Examples of successful intranet applications

Bharat Petroleum Corporation Limited (BPCL), a major oil company of India (<http://www.bharatpetroleum.com/>) uses an intranet to provide their employees with an efficient way to share the internal company information and let a number of workgroups to share and work on various projects. However, using the Internet, they also distribute financial data and news announcements to customers, shareholders, and others outside the company. The BPCL Web site also offers prospective customers an opportunity to conveniently apply for its Petro credit cards and to purchase merchandise offered in their Web-based catalogue.

The product development teams at Maruti Udyog Limited, India's leading car manufacturer (<http://www.marutiudyog.com/>) use the company's intranet to get their products to market conveniently and faster. The intranet also facilitates communications between sales, service, and remote field teams around the world, allowing the company to capitalize on areas of expertise in various locations. As with BPCL, the MUL employs Internet technologies in addition to the intranet solutions to educate customers and their worldwide sales force about new products. Prospective customers can easily find product information including photographs, datasheets, comparison of various models and success stories, as well as check on the availability of the latest car releases. Back in the server room, the intranet runs safely behind their firewall, the company connects its dealers and vendors to use the benefits of intranet for minute-to-minute update of inventory levels for maintaining a balance of supply-demand chain. The company publishes an electronic sales guide with important information their sales network can use to sell their products.

Broadly speaking, the benefits can be enumerated as follows:

- **Cheaper:** Use of client browsers with one standard Window interface, offers easy integration with a number of other applications, such as electronic mail, faxes, videoconferencing, calendaring, and linkages within messages. As a single interface to a variety of information sources, the browser is cost-effective, highly efficient, uses minimal resources, and very easy to use.
- **Versatile:** An Intranet server eliminates the need to replicate database by providing users with easy access to source data. A single WWW server platform can support both internal and external applications for both internal information - sharing and external marketing on the Internet. In contrast, the Lotus Notes application is costlier and purely an internal application.
- **Flexible:** The Intranet provides the users with access to centralized information resources on a single point-and-click basis through the browser, which is available on a variety of client platforms (Windows, Mac, Unix, etc.), at any location. With Notes, data distribution is in realtime, on an as-requested basis, over a public (or private) network.

Intranets obviously have many advantages to both the organisation and its personnel.

- The most obvious advantage is that everyone with access to a computer terminal can obtain the entire store of information that can be easily updated at regular intervals. It is essential to note that even a simple database like an organization telephone directory gets outdated quickly, sometimes even before it is printed on paper whereas an on-line directory can be updated immediately whenever there is a change needed.
- Intranets encourage integration of applications; such as the simple word-processing application could be easily linked with e-mail services, and as such this redefining of the ways and possibilities could be used more efficiently and effectively.
- Intranets provide access to electronic databases, documents, electronic training manuals, office circulars, internal job vacancies, etc. Any type of information the company feels is informative and useful can be hosted on the central server or databases, which can be extracted by browsers when needed without the employees having to leave their work area. This feature provides a further benefit, i.e., freedom from the work area. The employee is free to travel anywhere without having to worry about what are lying on his desktop, since every information required is available on the Intranet site which could be easily hooked up from his laptop computer and a mobile modem.
- The ease of use of the end user would be the most noticeable because of the similarity of intranets to the Internet. Since the intranet technology is based purely upon the user-friendly atmosphere of the World Wide Web (WWW), the system is very easy to use. It does not matter that users do not necessarily understand the intricacies of how the information flows up and down to their workstation or to the centralized server; it is the ease of obtaining required right information at right time, which matters the most.

Several other factors contribute to increasing the profitability of a business. For companies that are highly dynamic and rapid in action, the primary factors among those are:

- Increased market share
- Increased product margins
- Cutting expenses
- Utilizing existing resources more efficiently.

Increasing market share and product margins leave to the Marketing and Purchasing personnel. The cost cutting however can of help to the central office or headquarters. The last factor is crucial to the company's Planning department since profitability the company's most crucial and bottom line consideration. Most companies today are suffering with inefficiencies, redundant operations, and unproductive tasks. Many of these can be greatly reduced or eliminated with a well-designed Intranet.

The following activities can help the companies for building up a well-designed Intranet site for themselves that will improve the overall profitability:

- Improved and more efficient employee training
- Decreased orientation time before new employees become productive
- Improved employee and departmental morale
- Better project management
- Increased inter-departmental communication channels

- Faster and improved dissemination of information to all departments
- Inter-department collaborative efforts
- Decreased production costs if currently publish information for internal use.

1.4 TYPES OF INTRANET

Intranets have been broadly classified into three types based on their functionality, viz., the Bulletin board, database management and information access.

- **Bulletin board:** This type of Intranet allows everyone in an organization the capability to review or update information that would normally be placed on an organization bulletin board, such as, a calendar of events, a status board, pictures of events or employees, policy changes, etc. It just acts like a broadcast system or notice board of the company in which updates may be or may not be frequent.
- **Database management:** This type of Intranet allows everyone in an organization with the capability to maintain a "real-time" interactive database. The database can be used to support the tracking of products, inventories, bidding, or provide information on a particular subject any time of day, from any location. The information is kept updated as quickly as possible since time and information is money for the organization.
- **Information Access:** This type of Intranet is the type commonly found on the World Wide Web. The static web page may include information on any subject. The static page can then be accessed from a simple search engine provided free as part of the Internet.

This "free service" networks are now-a-days making good money through advertisements, even major newspaper companies and news agencies have started using this type of intranets of late for proper organization of news items and finally hosting of entire content to the internet with a click of the mouse button. Information access is the key to making the Intranet commercially feasible. While individuals within an organization may have secure access to particular parts of an Intranet, the marketing and promotion of an organization is the accepted norm. By advertising on the Internet the organization is available to a broader customer base, via the global structure of the Internet.

Some experts have taken a lead and have categorized intranet into four different types based on their application or usage as well as its architecture. They are as follows:

- **The Communications Intranet:** Intranets of this type tend to feature in geographically dispersed organizations. The motivation for its implementation is greater efficiency and cost saving, through the reduction of fax and telephone calls. This intranet is common with franchises or organizations that have a large number of salespeople or agents in the field, for example, Maruti Udyog.
- **The Integrating Intranet:** These intranets are designed to replace the complexity of in-house communications and processing systems that in large organisations often use. Different interfaces commonly lack means of interconnection. Such intranets offer organisations a common interface (through browser) that can link-up its different divisions through hypertext links. It follows that standardisation is paramount in an integrating intranet. for example, IGNOU.

- **The Catalogue Intranet:** intranets of this type are often more accurately described as extranets. They are designed to give access to a large catalogue of information, like a multimedia catalogue. Example, a news agency or companies offering search engines like the Yahoo.
- **The Single Sign-On Intranet:** This intranet, if managed efficiently, allows maximum security by firewalling anyone from inappropriate sites automatically, for example, the railways.

It would be notable that any of the above intranets can be controlled or firewalled through passwords and user IDs to safeguard security throughout an organisation. The fourth type of intranet dispenses with individual log-ins or passwords opting instead for a single sign-on for all users and letting each system look-up the appropriate access privileges for each user.

1.5 SOFTWARE AND HARDWARE REQUIREMENT FOR INTRANET

The Software and Hardware requirements for setting up an Intranet are as follows:

1.5.1 Hardware

An Intranet is simply a standard Wide Area Network (WAN). The use of the term Intranet recently to describe using software developed for the Internet on the company's WAN. Web servers are an example.

To setup a WAN, one will need to have some type of communications between the different sites. National ISDN, Very Small Aperture Terminal (VSAT) connectivity or a long distance Frame Relay could be the best choice. It will be essential to install a router at each site. Each router would connect back to a central site over dedicated phone lines. Note that the hardware should be configured for the following protocols/ services.

Protocol/Service	To be installed on
IP	Network
HTTP	Server
SMTP/POP3/IMAP4	Server
LDAP	Server
X509 Certificate	Server
Java	ORB
Document Server	Server

Scientists also describe how optimal performance of intranets is associated with a number of key hardware factors. In order to optimise performance, servers with fast processors and large amounts of memory are essential. They also noted how good multi-tasking and multi-threading ability is also crucial for most of the Web applications. In addition, sufficient memory and disk capacity at the user workstation would improve performance through increased caching. The limitation of large image files can also be considered important to improve performance, but images may be equally important to expand and illustrate data, and pages of text can be discouraging, especially in an educational context. Finally, the database itself, which forms the foundations of almost every intranet, can have a significant effect on performance.

1.5.2 Operating System for Server and Clients

On the Server

Since 1994, when the original pair of web servers — NCSA HTTPd and CERN HTTPd, dozens of commercial and shareware programs have been developed. While the Netscape Enterprise Server defines the commercial high end, the other is Microsoft's Internet Information Server (IIS) Netscape Enterprise Server and lightweight Fast Track Server.

On the Clients

All of the clients running popular operating systems such as Microsoft Windows, MacOS, Unix, etc. could be used to function as backbone software for the Intranets.

Only one software is sufficient for working with the Intranet viz., the browser software that should be loaded on all the clients. This software serves as a single interface to both the Intranet as well as the Internet. At present, Microsoft Internet Explorer and Netscape Navigator both remain the top web browsers available. Apart from these, various other web browsers are also available to access the information such as NCSA Mosaic.

1.5.3 Language support

Intranet works on the basis of scripts written in any of the following languages, viz., SGML, HTML, DHTML, XML, ASP, CGI, Perl, UML, VRML, etc. Though almost all are variants of the basic markup language or development over it, all provide flexibility to program the needs of the organizations. It is essential to test minutely how the output looks when published on the central server, by using different browsers on different operating systems.

1.6 APPLICATION AREAS

The uses of an Intranet are only limited by imagination. Some of the larger sectors where Intranet can be easily and successfully implemented are as follows:

- **Education Sector**
 - ✓ Universities
 - ✓ Colleges
 - ✓ Institutes
- **Industry Sector**
 - ✓ Small and large scale manufacturing
 - ✓ Automation and control
- **Service Sector**
 - ✓ Hotel
 - ✓ Tourism
 - ✓ Travel
 - ✓ Transportation
 - ✓ Communication
- **Research & Development**
 - ✓ Laboratories

✓ Organizations

✓ Space

● **Government Sector**

✓ Ministries

✓ Departments

✓ States

✓ Law & order

The following is a partial list of many potential uses of the Intranet, both commonly used and not so commonly used.

● **Company Documents**

✓ Manuals

✓ Building Maps

✓ Airport Directions to other Company locations

✓ Approved Vendors list

✓ Company Newsletters

✓ Procedures library

✓ Product Manuals

✓ Daily Bulletins

✓ History graphs

✓ Knowledge Base

✓ Competition products, news and web sites

● **Customer related**

✓ Controlled Responses

✓ Feedback Forum

✓ Company Bulletin Boards

✓ Company Store

✓ News Flashes

✓ Supplies Ordering

✓ Database Queries

● **General Administration and Management**

✓ Department Budgets

✓ Departmental FAQs (Frequently Asked Questions)

✓ Employee Attendance

✓ Intercompany Chatting

✓ Internal Postings

✓ Employee Orientation

✓ Online Collaboration Projects

✓ Organizational Charts

✓ Security Policies

✓ Trend Graphs

✓ Equipment Checkouts

- Training
 - ✓ Employee Proficiency Training
 - ✓ Training Materials
 - ✓ Video Training
- Coordination and Control
 - ✓ Form Routing
 - ✓ Forms Library
 - ✓ Help Desk Submission Forms
- Meetings related
 - ✓ Meeting Minutes
 - ✓ Meeting Schedules
 - ✓ Online Meetings
 - ✓ Meeting Room Schedules.

1.7 FUTURE OF THE INTRANET

At present, the world of information technology is guided by the C³ paradigm that stands for command, control and communication, which is normally used for military applications and strategies. These techniques are poised to become obsolete with the advent of Intranets and shall no longer remain the driving forces in companies.

The talk of the day start with another C³ paradigm that stands for coordination, cooperation and collaboration. And this is what available in store for the future. It emphasizes better support and interaction towards common goal between various activities within an organization.

And this is possible through the Intranet technologies, which is helping in redefining the whole new world of computing thereby making integration a buzzword for everyone.

As stated by experts that it is 'because the browser has evolved far beyond its original uses, it may well become the universal interface to all information resources in the future'. As Internet technology expands, then it follows that intranets must necessarily benefit from these advances since the technology is shared. 'The result will be the increased integration of corporate data-access systems with inter-corporate communication systems and corporate-customer communications'.

1.8 KEY INTRANET TERMS

Following is list of most widely used terms, which come in-way during study of Intranets:

Applets: Little programs that can make the Web pages more aesthetically beautiful by means of animations, text, and graphics moving across the screen.

Bits, Bitmap: Many tiny dots, which are put together to make a picture. Bits are combined to make a graphic image called a bitmap. GIF and JPEG files are the most popular kinds of bitmap files.

Bookmark: A list of pages a user likes to frequently visit. Netscape® Navigator and Explorer® have a "bookmark" menu item which allows users to add favourite sites via the Bookmark option. A term equivalent to the conventional bookmark used by readers to indicate position in a text book where they left it while reading it last time.

Browser: A program that allows the user to access and read information on the World Wide Web. Netscape® Navigator and Microsoft Explorer® are the best known browsers.

Counter: A software code that indicates how many times a site has been visited. It gets automatically updated and is usually represented by a small rectangle with numbers normally visible at the bottom of web pages. something like the odometer of a car.

Cyberspace: The conceptual or virtual area where pages, data, images, and all the rest are stored. It is the area from where requests are accepted and fulfilled from computer to computer, user to user.

FAQs stands for Frequently Asked Questions. Common questions and their answers that occur regularly within a user group. FAQs also appear as a hot link on many web sites and sometimes acts as reservoir of knowledge about the company or its products. FAQs are a time-saving feature for all kinds of users.

Firewall: A protection of the internal company network against unauthorized access via the Internet.


Frame: A presentation format, which enables Web page designers and users to mark a part of the screen for links to other pages. Frames usually appear on the left side, top, and/or bottom of the screen. Frames contain icons and hot links.

File Transfer Protocol (FTP): A very common method of moving files between two Internet sites. FTP is a special way to log in to another Internet site for the purposes of retrieving and/or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP by logging in using the account name anonymous. Thus, these sites are called anonymous FTP servers.

Graphics Interchange Format (GIF): A type of graphics file found frequently on the net. A picture of a vice-president, for example, may appear on the Intranet as a GIF.

Home Page: The primary Web page for an individual or organization. These pages link to other related pages.

Hot Links: A connection from one Web page to another. A hypertext link. Hot links are frequently indicated by coloured, underlined text and/or an icon. Hypertext markup language (HTML), the language used in writing pages for the World Wide Web. No knowledge of HTML is necessary for using the Intranet, or for maintaining pages.

Hypertext Transfer Protocol (HTTP): The way Web pages are transferred over the internet or an Intranet. *Icon* A small picture or graphic used to represent a location in the inter- or Intranet (for example a flow-chart graphic to take the user to the departmental flow chart); an action (a mailbox as a place to send feedback); or a program (a  to indicate Microsoft Word).

Daemon: A daemon is a Unix background process that implements the server side of a protocol. Daemons are unique to Unix. For example, FTPd stands for the File Transfer Protocol daemon.

HTTPd: It stands for HTTP *daemon*. HTTPd is the program run on a Unix platform to establish a web server. On other platforms, such as Microsoft Windows NT, the web server is a background process implemented as a system service.

ISDN: Stands for Integrated Services Digital Network. It is a way to move more data over existing regular phone lines. ISDN is rapidly becoming available to almost every country and every one who need it, at affordable charges and data transfer rates. In most countries it is available at a price comparable to standard

analog phone line connectivity. It can provide speeds of roughly 128 kilobits per second over regular phone lines.

Java: A programming language that in particular, allows browsers to download and run applets (very small programs allowing animations and the like).

JPEG: Stands for Joint Photographic Experts Group. A standard format of storing digitized, colour, or black-and-white photographs. JPEG files are smaller than corresponding GIF files.

LDAP: Stands for Lightweight Directory Access Protocol. LDAP is preferred for creating directories. LDAP provides a standard way for Internet clients, applications, and servers to access directory services using TCP/IP, regardless of the hardware/software platform.

Network: A number of computers connected together.

Internet: Lots of networks all over the world are connected to make the Internet.

Intranet: Lots of networks connected within an organization (locations could be geographically distant) such as a university or company.

Search Engine: Software used to find information on the Web. Examples are Google, Lycos and Yahoo.

Server: A computer with the capacity to provide connectivity (sharing) to multiple personal computers or clients.

Surfing: Going from page to page, link to link, via a browser. Surfing can be called "clicking" for the mouse clicks that make the process possible, or "linking" from the program logic, which makes the process happen.

T-1: A leased-line connection capable of carrying data at 1,544,000 bits per second. Theoretically, a T-1 line could move a megabyte at maximum capacity in less than 10 seconds. This transfer rate is still not fast enough for full-screen, full-motion video, for which at least 10 Mega bits per second would be needed. T-1 is the fastest speed commonly used to connect networks to the Internet.

TCP/IP: Stands for Transmission Control Protocol/Internet Protocol. This is the group of protocols that define the Internet and communication method used by it. Originally designed for the UNIX operating system, TCP/IP software is now available for every major operating system. In order to be compatible to the Internet, the computer must have TCP/IP compatible software.

Uniform Resource Locator (URL) : Address of location for accessing Web pages. Clicking on an icon or "hot text" is the most common means of accessing and using a URL. Typing the URL in the "Location" on Netscape® Navigator or Internet Explorer®, (for example, {INTRANET NAME}@[COMPANY NAME].com) is another way of getting to a Web page.

Web or Net: The World Wide Web (a server) consisting of a hypermedia system (linking sounds, text, pictures, video) that the computer (a client) can access.

Web Page: The basic unit of the World Wide Web. Information on a Web page can include graphics, audio and video. A number of properly linked web pages make up an Intranet or internet.

Web Server: A host computer that stores Web pages and responds to requests for viewing. Web servers communicate with Web browsers (by HTTP).

Webmaster: The supervisor ensuring that the system is up and running; the coordinator of access; the administrator for communications between users and hosts to sites.

Check Your Progress

- 1) The browser when invoked seeks a server computer through the communication medium that has the first or Home Page of the Intranet, which is usually seen in the folders as _____.
- 2) The most easily noticeable difference between an Internet server and a "collaborative" computing solution such as Lotus Notes (also called groupware, could be used for Intranet server) is the _____.
- 3) _____ allows everyone in an organization to review or update information
- 4) _____, if managed efficiently, allows maximum security by firewalling anyone from inappropriate sites automatically
- 5) VSAT stands for _____.

1.9 SUMMARY

Intranet is a network of networks meant exclusively for an organization. The networks could be spread over a number of locations. Intranet uses the concepts of client/server technology, Internet, WAN, LAN and many others.

Intranet implementation are usually highly inexpensive, except the communication connectivity cost between different locations. Intranets support everything that Internet supports but vice versa is not true. Users can connect to their company's intranet through a web browser, which provides a single interface to a reservoir of information.

Though there are a number of strong advantages of using intranets, security of information could be highly concerning since the information has to flow through WAN.

There are two ways of using specialized software on the intranets, viz., through intranet server software or through groupware. The latter is considered costly but have its own advantages.

In future, one can see a fusion between the intranet and groupware thereby bringing lot of benefits. Similarly, the intranets are expected to bring in better coordination and control within any company and consequently, the existing work pattern of the employees is also likely to change.

1.10 MODEL ANSWERS

- 1) Index.htm
- 2) Design philosophy
- 3) Bulletin Board
- 4) Single Sign-on Intranet
- 5) Very Small Aperture Terminal

1.11 FURTHER READINGS

- 1) *Intranet and Web Databases for Dummies* by Paul Litwin, Hungry Minds Inc. (Publisher).
- 2) *The ABCs of Intranets*, BPB Publications.
- 3) *Building the Corporate Intranet* by Steven L. Guengerich, John Wiley & Sons.

Reference Websites

- 1) <http://www.sun.com>
- 2) <http://www.microsoft.com>
- 3) <http://www.intel.com>
- 4) <http://www.motorola.com>

UNIT 2 INTRANET'S SECURITY

Structure

- 2.0 Introduction
- 2.1 Objectives
- 2.2 Security Concerns
- 2.3 Threats
 - 2.3.1 Internal Threats
 - 2.3.2 External Threats
- 2.4 Security Solutions
 - 2.4.1 Hardware
 - 2.4.2 Software
 - 2.4.3 Information
 - 2.4.4 Certification
 - 2.4.5 Firewalls
 - 2.4.6 Encryption/decryption methods
 - 2.4.7 Security Policy
 - 2.4.8 Multiple Layers of Intranet Security
 - 2.4.9 SOCKS
- 2.5 Advice from Security Experts
- 2.6 Summary
- 2.7 Model Answers
- 2.8 Further Readings

2.0 INTRODUCTION

Every company starts its operations with a genuine and honest thinking. As the time passes, based on the need of its employees as well as customers, a number of processes evolve automatically, which form the core of experience as well as strong standing of the company.

Through the security breaches, companies lose highly valuable information. What is the most valuable thing any company has with it? Truly, it is the ideology of how to implement its creativity in to the market and see that the experience and services reach customers properly so that both the customers as well as the company prosper simultaneously.

Imagine a situation when a company develops a major new product secretly using its Intranet. Hackers break the security and take away all the details or even cause certain damage to the software products. They can even sell the details to the competitors or blackmail the company.

Security has long been seen as a major threatening point in the implementation of Internet or intranet technology in any enterprise. As networks have grown and connected to the Internet, a huge variety of hackers have haunted the professionals responsible for both delivering information within the enterprise and to its partners, and protecting it from unauthorized outsiders.

A good security technology should be powerful enough to support the features administrators need, including rules validation to inform the administrator of potential security back doors, automatic incident reporting to inform administrators when a security breach has occurred, and secure management of the firewall itself so hackers cannot reconfigure the firewall and create security problems.

2.1 OBJECTIVES

Though computerization helps a lot in proper organization of the rich experience, it also opens Pandora's box simultaneously. On one side lies the benefits of proper organization and quick access to the experience and on the other side there are hidden problems of dishonesty, distrust and a number of unforeseen and unwanted conditions.

Security of the contents put on an Intranet could be of great concern since information in this Information Age is as valuable as money. This unit deals with various kinds of threats to an Intranet, and security measures to protect the Intranet from them.

2.2 SECURITY CONCERNS

The history of security concerns is not new to any one. They have been of great concern to man and since many centuries man has been endeavouring to devise new techniques for strong security measures.

Every time the technology updates itself, new techniques evolve, but at the same time the thieves or intruders (in the information technology line, they are called "hackers") also get equivalently intelligent since they too must be using increasingly sophisticated tools. Hence, in order to prevent them from intrusion, the companies who manage Internet and intranet sites full of voluminous information and experience must do proper policing as well in addition to their existing day-to-day activities.

Even though the security capabilities of the latest Internet and intranet technologies have enabled the companies to control the availability of information and its authenticity in a much better manner than ever before, still many things have been left for completion. The increasing sophistication of both server and client software means that extremely strong levels of security has provided built-in without actually requiring users to undergo complex measures to control the access as well as even to hack them down.

In order to prevent the intruders to enter into the house, it is necessary for the house owner to look after the behaviour of internal and external people (usually who deal with the owner directly or indirectly). Similarly to prevent the data from the hackers, the Internal or External security concerns, possibility of attacks and their measures have to be carefully analyzed well before hand in order to avert any eventuality.

Access to the intranet site can be broken down into:

- Those who can enter the site;
- The who can access the various secured areas; and
- Those who can update the site's content.

Out of the above three, the first two could be considered safe whereas the users who fall under the third category could cause the company's professionals to have sleepless nights.

2.3 THREATS

It must be clearly understood that the source of threat and the likely target could be many in number but all of them can be classified as either major or minor threats. Similarly, they can be organized into two groups viz., internal and external threats.

Details of threats have been dealt with in subsequent paragraphs.

2.3.1 Internal Threats

Internal security problems are probably the most common. One never knows what someone is going to do. Even the most loyal employees or workers can change their tune and turn malicious, wreaking havoc on the computing environment.

By thoroughly scrutinizing the workers' backgrounds, references, and previous employers carefully, and changing and auditing security methods, especially observation of the work pattern or behaviour of the employees (may be on day-to-day basis), it would be possible to know about the possibilities of internal threats before hand. Still further, this information would be useful to track down the line easily when any attack takes place.

2.3.2 External Threats

External security threats are the most problematic ones. Till date the greatest threat was the virus menace. Now, with the sophisticated technology, a number of new threats have also developed. It becomes difficult to know when an outsider will attempt to hack down the systems or who the intruder may be. There are a number of examples in the past, the recent being hacking of Indian government's servers by certain terrorists and foreign nationals.

Some people go to great extremes to gain access to the systems and information. If intranet is connected with outside world via the Internet, it will discover a whole new set of potential problems and subject to a number of attacks.

Complete and proper security configuration and administration is indeed a complex issue. One should think carefully about the security breaches before connecting to the Internet. One of the simplest and crudest methods could be that too many system administrators connect to the intranet first assuming that Internet should be treated as the potentially hostile environment and consider security at a later stage. This method could be highly useful in detecting possible loopholes in the system before hand.

2.4 SECURITY SOLUTIONS

Though there are a number of security solutions available due to sophistication in technology, there are a number of risks and difficulties attached to them. The attacks could be momentary but the aftermath could be so much disgraceful that it may take many months or even years to get back to the normal. History is evident that many such attacks have led to total shutting down of the company itself.

The prime most could be the unwilling overhead in the form of huge investment on extra hardware and software. It is quite possible that while implementing various security measures, the company ends up with investment more than the actual cost of the hardware and software.

Additionally, sufficient training for concerned personnel would also have to be added up to the expenditure statement. Hence, keeping all these issues in view, the company has to plan in such a manner that the investment on providing basic computing infrastructure and that of its security are properly balanced.

Security models

The first and foremost thing one needs to do is to chalk out a security plan and policy based on any security model. The term security policy shall appear a number of times while dealing with different security measures since it forms the foundation for the measures.

It is essential to distinguish between public knowledge information and the more detailed pieces of information relating to specific groups, departments, or projects. Very obviously, there is no need at all to keep documents such as web site material, press releases, product information, etc. that can be found anywhere is public. They can be found in any newspaper or Website, care must be taken to review and protect the intellectual property.

A classical case study: *With due acknowledgements to a security exponent who proposed this theory.* He has carefully classified the security models by giving striking analogies to the real world in the form of following five generalized examples that happen to everyone during day-to-day activities:

- **The Open House:** In this case, the front door and all the rooms are unlocked. Visitors will be free to move around anywhere from any room to any room. This resembles to an unprotected site where users do not require any special authentication to view the information.
- **The Owner:** A case where the front door is locked but all the rooms are unlocked. The owner lives in the house and locks the front door in order to keep the neighbours out but once anyone gets into the house, they will be free to go into all other rooms. This is a useful security model if any company gets a lot of outsiders (i.e., customers, visitors, consultants, etc.) passing through but only want to have its employees access the site.
- **The Garden Party:** An excellent case in which the front door is unlocked but certain rooms inside the house are locked. Anyone may wish to allow people to help themselves to the bar on the front lawn and get into the washrooms but not necessarily into the bedrooms where the owner has kept all of his personal things.
- **The Paying Guest:** This is a most stringent measure than the above in which the front door is locked and certain rooms are locked. The guest has a key to enter the house and is able to get into his room only but the other rooms are off his limits. This model will verify whether or not a user should be allowed to enter the site. Once this user is authenticated, only then he or she may move freely throughout the other rooms as long as they have access to them.
- **The Fort:** A locked massive iron gate with barbed wire, front door locked, all rooms also locked, and there is a watchman guarding the house. Simple, unless the users have the proper credentials or certificates or entry passes, they will not be allowed to get in.

Any one can select any of the above security model or a combination of them. While selecting it should be borne deep in mind that every model have its own cost factor and other considerations.

2.4.1 Hardware

The first component in the computer system vulnerable to attacks or threats and most important to be protected is the hardware. The following are some of the common threats to the hardware:

- Theft of a computer, printer, or other resources.
- Tampering by a disinterested or frustrated employee who takes every chance to manipulate with control switches, tampering the network or cuts the cable.
- Destruction of resources by means that can cause terrific problem like fire, flood, or electrical power surges. Since some of them are natural attacks, they may or may not be in the control of the human alone, however, protection should be thought of well in advance.
- Ordinary wear and tear.

In order to implement solution to the above threats, it is advisable that the company should maintain proper password protected hardware wherever necessary, it should also consider keeping the other peripherals and networking components out of the reach of common users and employees. Further, the provision of keeping hardware backup (extra computers and servers, may be of lesser capacity) as standby when the one working generates trouble due to attack or wear and tear; it is likely that the company may find this option a costlier, it is strongly recommended to consider it seriously.

The cabling should be properly laid out in conduits and only few "trusted" personnel should be entrusted the work of overseeing the activities. It is also to be ensured that the passwords, firewalls, etc. measures are not handled by only one person and also that communication of confidential information such as change of passwords and documents do not fall into the hands of unauthorized personnel.

2.4.2 Software

The second component vulnerable to the threats to the system is software. Threats to software may include but not limited to the following:

- Deletion of a program, either by accident or by malicious intent.
- Theft of a program by the user.
- Corruption of a program, caused either by a hardware failure or by a virus. Usually, it has been observed that more of the attacks are due to virus attacks that cause terrible destruction in moments.
- Bugs in the software (intentional or unintentional).
- Virus attack.

The software developers have wide experience of tackling such issues. Students who develop software project spending days and nights struggling with software code to make things happen suddenly find that their files do not open or are missing. Reasons could be many, it could be disk drive media failure, virus attack, unintentional deletion, cross-linking of files, corrupted file allocation table, bad sectors, and many more.

Assume only one attack out of the above list i.e., the virus attack. Though the present anti-virus software solutions can detect and clean as many as 50000 viruses, it becomes extremely difficult to detect a new virus numbered 50001.

The recent happenings of I Love You, Love Bug, Dinner Party with CEO, etc., viruses have virtually spread all over the world not leaving any type of system. As reported at many places, the casualty has been extremely high and the organizations could not come to a stable state till date. It would be notable that even for developing an antidote it would take many man-hours of research and testing before the things are set right, and in the meanwhile the virus would have done all the damage it can.

Numerous corporate offices do their day-to-day work on-line. A simple task like sending messages, circulars, interview, meeting, promotions, etc. all are dealt on the corporate intranet. The NIC, Indian Oil, Bharat Petroleum, VSNL and many more does work "electronically". Assume that a new virus enters the network passing through the stringent anti-viral tests successfully (and of course, undetected). The story starts then and ends in few more moments.

2.4.3 Information

The third and major component of the system liable to be attacked is the data and data files used by the company. It is the most serious of all the threats. Threats to

the hardware and software are considered negligible in comparison with the threats to information since it is this information that acts as the knowledge about the organization. Hardware can be replaced and software can be reinstalled, but information once lost cannot be obtained back. Threats to information can include:

- Deletion of a file or files.
- Corruption, caused either by hardware problems or by a bug in the software.
- Theft of company data files.

A surge in electrical pulse can cause colossal damage to the data. Dishonesty and distrust as well as frustration have already been discussed in the beginning of this unit, which can be potential threats to the company's information base.

Making and testing backups regularly could be the simplest and easiest of all the security measures. But a new question will immediately arise – “how many backups and where”. Clearly, it is possible that the backup could contain virus or there was a media failure or bad sector. Still a step further, the entire building collapses due to earthquake or fire. Solutions lie in terms of maintaining a number of backups, some put at a remote server or site (may be few thousand kilometers away from the location).

Such issues of security threats and management can be found separately as “Disaster Management”

2.4.4 Certification

One solution for the protection of the computing infrastructure is to use digital certificate-based solutions. Users can be given access based on their possession of certificates signed or authorized for access by or on behalf of the server to which they intend to have access. There are a number of certification solutions available in the market today. In India, the Ministry of Communication and Information Technology has even set up a whole new organization to oversee various security related concerns and certification under the title Controller of Certification Authority.

The certificate acts as an evidence of the user's digital identity. Certificates can also be combined with other access control mechanisms, such as e-mails, money transactions, tokens (a form of identification hardware carried by users) or only accepting visitors from certain controlled group or authenticated addresses.

At present, the certification is most easily implemented with a custom solution combined with a server called the certification authority (CA). It is an external or third party service, which can issue and revoke certificates and authenticate any certificates presented in order to gain access. This could be implemented by use of a simple public key infrastructure (PKI), a system that establishes a hierarchy of authority for the issuance and authentication of certificates and users presenting them.

Digital certificates provide excellent means of controlling and monitoring access to the intranets. The certificate itself acts as a token for access control. The user must present it in order to access the intranet or Internet site. The certificate could contain a series of digits and alphabets combined together. The best example can be the use of cash card or the prepaid mobile phone card. The customer pays for the required number of hours of mobile phone usage well in advance and scratches the card to obtain the “certificate”. The customer then connects to the intranet site of the phone company by dialing it and then enters the “secret” code. Upon entering this code, the phone company updates the usage records and permits the customer to use the services for the extended period.

A similar service offered by the popular Internet service provider (ISP) of India called the Videsh Sanchar Nigam Limited (VSNL) offers e-mail services for which the customers are handed over a card containing the secret code for the number of hours of usage. Those cards are available at many stores or shops. The customer has to log into the VSNL server and create a new account with the given code number and thereafter use it as long as it permits. Such services are available for ordinary telephone services where prepaid.

While in many implementations this is done automatically, in many other implementations the certificate is stored on a separate database or token such as a smart card which the user has to present to the local client in order for it to pass it to the server to gain access. Some other implementations use a number of certificates (or multi-level certificates) to ensure proper security measures.

2.4.5 Firewalls

For intranet developers, restricting access of unauthorized users to the web site has been the greatest challenge. In addition to preventing external users, a watchful eye on the users within the company may also have to be maintained. There are various tools to provide protection against unwanted intruders into the corporate wide networks, but the most popular amidst all security measures is the firewall.

The simplest way to restrict the users to peek inside the internals of the web site is to use firewalls, where the information cannot be seen or accessed from the Internet at large. Simple firewalls consist of software that prevents access to internal networks from the Internet. While general traffic such as e-mail is allowed in to the mail server, programs such as FTP clients, telnet users or search engine queries cannot access machines beyond the safety premises of the firewall.

Firewalls also offer additional protection to local users who like to browse or surf out from the intranet to the Internet, by acting as proxy to obtain web pages so that the name and IP number of machines on the network are not revealed to other web sites that the users visit. Not revealing the IP address would help preventing hackers from knowing about the details of the structure of the intranet.

While firewall remains the basic foundation of Internet and intranet security, for many users getting into the corporate intranet would require increasing levels of technology. The intranet technology would need to be expanded beyond those physically present on the same intranet from time to time.

There are drawbacks of permitting users to access the intranet as well as not permitting them. A simplest consideration such as allowing users to use dial-up access behind the firewall by violating basic security principles could amount to inviting numerous unwanted security concerns; however, restricting them to the same access offered to the rest of the Internet users by denying permission at the firewall level would deny them of valuable and essential services.

In order to implement a successful firewall, the first and foremost activity to be done is that the company's security policy has to be clearly defined.

Though there exist a number of definitions of firewall, in simplest terms it can be defined as "a mechanism used to protect a trusted network from an entrusted network". It can also be defined as "A firewall is a system, or group of systems that enforce an access control policy between two networks, and thus should be viewed as an implementation of policy". From the above two definitions, it can be understood that a firewall is only as good as the security policy it supports.

It should be very clear right from the beginning that a firewall is not simply for protecting a corporate network from unauthorized external access via the Internet, but it can also be used internally to prevent unauthorized access to a particular subnet, workgroup or LAN within a corporate network.

It would be highly interesting to note that more than 70 per cent of all security related problems start from within inside an organization. Thus, for example, all the branch offices of a big company should have separate servers each protected behind a firewall, while still allowing the users of all branch offices to remain well connected and form an integral part of the global corporate-wide network.

Types of Firewall Architectures

For the sake of simplicity, the firewall technologies have been categorized into three types based on the kind of role they are expected to play. Types of firewalls are:

a) Packet filter firewalls

They remain the most common type of firewall in use as of today. They were the earliest firewalls developed and were capable of permitting or denying traffic based on certain simple field-level filters which could determine such things as source or destination packet address, or the protocol being used. The greatest advantage is that they are fast since they have minimum processor overheads, and are transparent as well as highly inexpensive. On the down side, they are not strong enough at the application level. This is because these firewalls work purely at the level of network layer, making them difficult to configure and manage effectively.

Most of the present day routers include capabilities of such firewalls as a standard feature in their system. This kind of packet filtering can be found in almost every major firewall available today.

b) Proxy servers

These types of firewalls have been further classified into two types: application level gateways and circuit level gateways.

The application level gateways establish a connection to a remote system on behalf of specific applications. This type of firewall is usually a collection of application proxies, with a one-to-one relationship between the application used and its proxy.

Whereas the circuit level gateways provide the proxy or relay capabilities in a much-generalized form, which is not limited to specific applications. The primary advantage of such firewalls over application level gateways is that they do not require a specific application proxy for each new application that needs to be communicated outside the internal network.

Although in terms of security measure the proxy servers are very secure, they require a lot of programming which can result in a delay in release of new proxies for application level gateways as well as tend to be highly CPU intensive, thereby directly having impact on the overall network performance.

c) Stateful multi-layer inspection (SMLI)

They are considered as the third generation of firewall technology and usually combines the facilities of the above two. They are further classified into two types.

The Stateful multi-layer inspection (SMLI) firewall is similar to application level gateways in the sense that all levels of the OSI model are inspected carefully right from the network wire to the IP application layer.

The SMLI firewalls are different from the conventional "stand in" proxies in a way that the stand-in proxies are used for the applications when communicating to the outside world, thus putting a heavy processing load on

the processors. In contrast, the SMLI firewall just examines each packet and compares them against the known states (i.e. bit patterns) to know about the behaviour pattern of the acceptable packets.

The term stateful implies that the firewall is wakeful and is capable of remembering the state of each session of packet exchange across it, allowing it to monitor all the packets for unauthorized access while maintaining high level of security, even with connectionless service protocols such as UDP, SMTP, etc.

A firewall such as the SMLI remains completely transparent to both users and applications. Consequently, SMLI firewall does not put extremely heavy processing overload on the host computer. Since it is rule based, SMLI firewall has the disadvantage that new applications may require new rules to be defined and implemented. However, the efforts are far lower than that involved in writing new proxies all together, thus allowing SMLI firewall vendors to support a broad range of new Internet applications very quickly (may be as quickly as almost overnight).

2.4.6 Encryption/decryption methods

One of the best method of ensuring security is to change the form of communication. Let the messages be encoded in such a pattern that it becomes almost impossible to decode for other while the actual user should be able to decode with the use of a simple certificate or key. There are three well known implementations of the encryption/decryption methods:

- Public key infrastructure solutions,
- Web server security through SSL. and
- Virtual private networks.

Even though there are a number of other solutions available, the encryption/decryption methods have remained most popular and economical in contrast to the others. Details about each of the security solution have been discussed in detail in the following paragraphs.

- **Public key infrastructure solutions**

The use of public-key based security systems requires great attention and due care in design and management of security features. The security of entire system is dependent on the security of the key since it is the key that will be used for signing certificates of various messages and documents.

This is done at the top of the public key infrastructure also commonly called the root. The encryption and decryption is done by specialized hardware.

Usually, all the keys used for accessing the server are held at a secret location in the primary memory of the server. This area or location is highly prone to attacks (for example, in a server core memory dump). It is obvious that a higher degree of protection is required for this target location.

Specialized hardware such as protected memory or cryptographic memory module for storing and protecting the keys proves to be a good solution. The keys are stored in a highly encrypted format. When loaded for signing, the keys are decrypted using complex encryption/decryption algorithms and loaded into the memory of the secure server, which then performs all the signing operations required on behalf of the server. It should be noted that the keys are never displayed in their unencrypted form to the server or any other user, so even if an intruder manages to access the network, the keys remains safe.

Physical security of the cryptographic modules is also built in order to provide

total security of the whole system and protect from unauthorized tampering or any kind of manipulation. The physical security is ensured by use of advanced manufacturing technology wherein strong systems are fabricated to protect the sophisticated security hardware.

Since digital certificates are highly dependent on hardware computations, it is essential that mechanisms are evolved to increase the speed of computing by various means such as parallel processing, provision of additional processors, separate hardware for protection, etc. Assume that a number of users log on to the server, then in such an event it is sure to face a bottleneck at the security gate since it would take considerable time in processing encryption/decryption of the keys or certificates. Now-a-days, in order to reduce this kind of difficulty, a separate server called firewall server is placed in front of the main server. Any one willing to access the main server has to get through this gate.

- **Web server security through SSL**

As it is well known that the Intranets and extranets are purely based on use of powerful web servers to deliver information to the users, the username/password authentication pair has been a highly popular method for preventing access to the web servers. Problem arises with use such pairs when these keys are sent in the form of character/text strings, which are prone to be intercepted, read and converted with simple tools.

A significant enhancement was achieved when communications between the user and the server was sent in encrypted form and later decrypted at the other end. The enhancement went step by step and today it has stood as one of the most secured and popular method of secured communication called the Secure Sockets Layer (SSL). Today, almost all commercial web sites are using SSL to ensure or guarantee the authenticity of the server and integrity of the data delivered to web site users.

SSL has become fundamental to the spread of Internet community, and commerce and trade over Internet. Over years, the spread of its use for an increasing range of transactions across the Internet has gone manifold.

Finally, it should be noted that by default most SSL implementations on web servers do not support or authenticate the client web browser. Therefore, SSL is at present best suited to the largely anonymous requirements of retailing and definitely requires lot of enhancements to actually pickup worldwide.

- **Virtual private networks (VPN)**

In order to encrypt/decrypt all the communication network traffic that passes through the Internet or intranet, a VPN uses software or hardware. This kind of implementation is considered the best when limited access to an intranet is needed, for example, when two branches of the same company want to use the same information, or suppliers and customers trying to hook up their supply chains. Best example is that of Maruti Udyog Limited that uses a similar kind of solution.

The greatest disadvantage of a VPN implementation is its non-flexibility to accept unknown locations. VPN works extremely well for two fixed known points, but less well suitable the needs of groups of users and situation becomes worse if they are from unknown locations.

Implementation using the combination of a public key infrastructure, secure web server and virtual private network technologies is considered the most powerful solution for data security. The addition of suitable physical security solutions such as cryptographic keys can further ensure that the security is perfect as well as robust.

2.4.7 Security Policy

In the United States, the government has a separate organization looking after the security measures and providing guidelines to all departments through the Computer Security Institute (CSI), which works in close association with the Federal Bureau of Investigation (FBI). CSI does not support just the governmental servers but provides every type of guidance to private networks as well. It conducts a number of surveys on many US corporations, government departments, universities, financial institutions, and medical institutions and brings out the importance of forming and implementing a proper security policy.

The scope of security policy depends on aspects such as the size of the intranet site, type of information hosted on it, and the number of users accessing the site. Each policy is based on a number of parameters like the companies' business rules, objectives, intranet type, content, and existing security infrastructure. It should be noted that a security policy made for some other intranet cannot be used for a different intranet by merely changing the name.

Although, an intranet security policy is a very broad topic and it cannot be covered easily in few pages since it differs from situation to situation, there are some general principles that can be found similar in almost all policies. Some of them are as follows:

- Identification of
 - The content, and needs to be secured
 - User groups or categories
- Procedures
 - Access authorization procedure
 - Backup procedures
 - Disaster recovery procedures
- Action against misuse
 - Course of action in the event of misuse or attacks
 - Ensuring employees exercise proper etiquette so that they do not misrepresent the company
 - Handling sensitive or secured documents stored on the intranet site
 - Copyright policies for intellectual properties developed by the company.

While every organization prepares a well documented IT policy, it should also endeavour to prepare an equally comprehensive security policy too.

The security policy should cover aspects such as network service access, physical access, limits of acceptable behaviour, company's procedure for dealing with cases of security violations, responsibility for the maintenance, enforcement of the policy, etc. in addition to those described above.

Security policy for networks and firewalls, for instance, has two levels of that directly affect the design, installation and use of a firewall system:

Network Service Access Policy : A high-level, issue-specific policy which defines those services that are allowed or denied from the restricted network. It also contains clear guidelines giving instructions detailing the way in which these services will be used, and the conditions for exceptions to this policy, if any.

Firewall Design Policy : A lower-level policy that describes how the firewall will handle prevention of access and filtering of services as defined in the above network service access policy.

Classification of data is an important requirement of the company's security policy. The company should in proper and clear manner define various types of information used within the company and the relative value associated with it. The low value information would consist of general product information, specifications, turn over, etc. that may be placed on a web server, whereas high value information would consist of information specific to new product designs, tender quotes, investments, plans and other commercially sensitive information.

An organization should consider three characteristics concerning the classification of important data:

- **Confidentiality** : Whilst some corporate data is for public consumption, the vast majority of it should remain private.
- **Integrity** : What (if any) data can be amended by external sources. In most cases, corporate data should remain unchanged by third parties, so the system should be capable of ensuring that only authorized personnel can effect changes. Integrity also concerns the subject of non-repudiation - once an order is received, for instance, the customer should not be able to claim later that it did not come from him. Digital signatures allow us to verify the originator, as well as ensuring that data has not been tampered with in transit.
- **Availability** : What data needs to be available continually, compared to data which can be "off line" for limited periods.

The security policy must be part of an overall organizational security scheme by which everyone abides from the Chairman down to the peon, whose focus must come from the top management. For example, a case as simple as a Chairman trying to turn off virus scanning because he finds it inconvenient to see the e-mails could be viewed seriously. This kind of policies could stand as acid test of an organization's commitment to its security policy. In case of emergencies, suspending certain aspects of the security policy, even temporarily can be risky since a security breach could result in total data or business loss, and consequently could cost many times more to recover.

The implementation of a security policy should invariably cover all parameters of security such as physical access to the server, method of storage and disposal of confidential documents, including access to the network and Internet usage.

2.4.8 Multiple Layers of Intranet Security

Security requirements vary from organization to organization, and also vary based on the content organization's intends to place on its servers. While for certain intranets simple security solutions are enough, for many organizations solution could be in the form of implementing more than a firewall or multi-layered security architecture.

A company can implement a wide range of security models but the most useful ones are those that are organized in multiple levels. Implementation of a multi-layered or multi-tiered scheme is easier and flexible than using all or no security approach in which a user allows either total access or provides a total denial.

In addition not just to access, security methods also protect information from accidental or intentional modification, manipulation or destruction. Most security experts opine that a security breach is more likely to come from within a company's own staff rather than from outside. These may be frustrated employees, or enthusiasts who are after the thrill of breaking the code.

As one can see that in the physical world, there are many layers of security. For instance, a bank maintaining lockers has strong vaults, good locks, alter guards, and highly sensitive alarms, etc. Each security measure tries to compensate the

limitations of others. Similarly, assuming information is cash, Intranets also follow the same suite and have a similar layered approach.

Most commercial servers use a powerful operating system as base that provides good methods of file-system security. Some servers require additional software to control access to server resources and files. The immediately next higher level is the software tool that monitors the system logs, serious looking out for any suspicious activity. When any intrusion is detected, the software generates an alert message. The response could be spontaneous and automatic, with an option to generate the alert message manually. The history recorded in the server logs is usually used to assess damage and for planning restoration from the damage.

Use of firewalls and proper alarm systems can act as complement to above security measures, which can be added to network routers to detect or block potential threats. These devices help in filtering, detecting and then permitting the user requests and have tendency to scan the IP packets for blocking suspicious behaviour or patterns. A proxy server also helps a lot since it hides the real IP addresses of users requesting resources outside the firewall.

Finally, software run outside the firewall tries all known security tricks of hackers, thus scanning for vulnerability points. The security implementation also should be supplemented with regular process audits by an independent security expert.

2.4.9 SOCKS

As it is well known, each different type of network security protects data at a different layer of the OSI model. Built-in at each layer lies the protocol that filters, scans and checks the access. These protocols are usually easily configurable.

SOCKS is an open, industry-standard protocol advanced by the Authenticated Firewall Traversal working group of the IETF (Internet Engineering Task Force). It defines a protocol, which allows TCP applications to access firewalls in a secure and controlled manner, gaining authenticated access through that server to an external network. It can be straightaway used to construct a firewall on a TCP/IP based server.

SOCKS is a networking middleware: a circuit-level gateway, acting as a proxy and is placed at the session layer to mediate client/server connections. It can be used to connect or establish connections between two hosts and perform transactions on an intranet or the Internet. Since it functions at the lower layer than application layer, it is clearly application-independent.

There a number of products based on SOCKS specifications such as Auto SOCKS available in the market. The latest version is SOCKS 5, which is backward compatible with previous versions as well as supporting key features such as authentication, encryption, the UDP protocol, DNS and IP addressing.

The main problem with SOCKS is that it lacks transparency to software developers and users.

Implementation requires a change to all existing client-based software so that all of them use the SOCKS libraries. This process of changing the client code is known as "socksifying". This could be extremely cumbersome since it is also expected that at both sides similar level of programming should be available since the entire process takes place at the sessions layer (i.e. at the level of routers).

SOCKS combine powerful features of circuit-level proxies without the programming overhead of traditional application-level firewalls. A number of companies, including IBM, DEC, Cyberguard, etc. have commercial firewall products deploying the SOCKS protocol.

2.5 ADVISE FROM SECURITY EXPERTS

Intentional hacking helps in maintaining better security: Several companies employ professional security specialists whose basic job is to detect and cover loopholes in the security systems of the company. It would be highly astonishing to ask why would a company pay someone to hack its intranet system. The answer would be obvious, that they intend to improve the security of its intranet as well as to identify where from the possible risks can crop in. It should be always remembered that majority of the threats come from inside the company.

Good resources: Books such as "Intranet Security: Stories from the Trenches" by Linda McCarthy, which also happens to be her first book could prove to be a bible to the current day security specialists.

Qualifications of security professionals: For the security professionals, it is essential that they have too much power to check the security measures or enforce them and simultaneously they should know how to use it effectively. It is also essential that the personnel though being competent do not have a striking ego. Egoistic personalities can be very harmful to the security systems; the firewall experts, security managers, etc., all personnel should be bound by the sense of responsibility, trust, loyalty and above all cool nature in tackling complex security issues.

Firewall configuration makes all the difference: The greatest blunder any company does is to just install a firewall and to finally think that they have ensured perfect security. While firewalls protect from outside threats, it requires updating from time to time. Poor firewall configuration has been considered the cause of the biggest security breaches that took place until this date.

Motivation behind hackers to hack: Good security people are usually broad minded, for instance, even if there is a small loop way made in the fence, the security personnel will try level best to make a way out only through the loop even though one could easily walk a few meters to where the fence ends and go around. This means that the security personnel attempt to locate and isolate the loopholes rather than go around a big way to reengineer the problem. They also tend to be alert regarding such holes either in the fence or in the software. Hackers also work in the same fashion. Even though both are motivated by the challenge, the difference is that both have opposite goals, i.e. good vs. bad. The solution lies in asking a question to oneself "what causes someone to do a bank robbery? Why does one person grow up and become a police officer while another person with a similar personality and traits becomes a bank robber?" It is to be remembered that information has the same value as money. Until everyone start to think about it that way, data will continue to be at risk.

Lot of care required while programming: It is a common and well-known saying that many developers of "secure systems" leave a "back door" way for themselves so that they can get into the system bypassing the secure front door.

The big problem is that often the companies owning the web servers or intranets have so many contractors and newly recruited programmers writing critical code who do not know the intricacies of the system security. The code never being reviewed causes the greatest concern (may be due to ignorance).

Security risks present on the networks: Lots of risks are present everywhere on Internet as well as on intranet, if it is not known what is being done. Every day a number of servers get connected to the global community but it is less than one percent companies who seriously think about the security issues. A study of security of web servers reveal that out of 2,000 high-profile web servers consisting of various kinds such as commerce servers, banks, industries, government and so on, only three companies noticed the breaches.

Routine security audits are essential: It is essential that regular security audits are conducted to find out physically which computer is connected and permits access to which networks. Also, the profiles, browser permissions, certification, passwords, location of the computer in the network layout plan, firewall configuration, etc. for each computer and user on the intranet has to be carefully studied during the audits. There are a number of other issues that cannot be dealt with directly such as integrity of the personnel. It is essential that the personnel be requested to fill up a questionnaire or they are interviewed briefly about the security measures using indirect questions.

Example of security audit as case study: Linda narrates one of her experience about a security audit. She was performing a spot audit where she was checking certain systems. It was noticed that there could be systems that was not even part of the audit. The exact location on the network layout plan was found out and it was noticed that it had an extra connection to it but she could not make out by the network map where the connection lead to. Consequently, she decided to audit that system and found that it was connected to the Internet, to that company's intranet as well as to a customer network. Still ahead, it was found that a hacker had broken into the system and replaced the system files and put them back in proper place. Nobody in the company even knew that that system had been broken into and only two people knew that it was even connected to the Internet.

Check Your Progress

- 1) The Open House resembles to an _____ where users do not require any special authentication to view the information
- 2) _____, a system that establishes a hierarchy of authority for the issuance & authentication of certificates and users presenting them.
- 3) ISP stands for _____
- 4) A firewall is a system, or group of systems that enforce an _____
- 5) The _____ establish a connection to a remote system on behalf of specific applications.

2.6 SUMMARY

As everyone is moving forward into the world of Internet commerce, it is important to remember that there have always been barriers to any kind of commerce. Earlier there were troubles with pirates, bank robbers and dacoits in the past, everyone with swords and guns; and now there is a new community preparing fast called the modern-day "electronic gangsters" or simply, the hackers.

It is to be always remembered while going for a security system that the security technology proposed to be implemented should be inexpensive, easy to implement, and transparent to end users.

Whatever the risks, business practices must continue to evolve. In order to move forward, it must accept some of those risks, while doing the utmost to minimize risks, as far as possible, are humanly and technologically possible.

Finally, it is advisable that instead of just one security solution, the company intending to implement one should think of a combination of security measures as people do in their lives by using security latches, closed circuit televisions, etc. in addition to the conventional locks and burglar alarms.

2.7 MODEL ANSWERS

- 1) Unprotected website
- 2) Public Key Infrastructure
- 3) Internet Service Provider
- 4) Access Control Policy
- 5) Application Level Gateways

2.8 FURTHER READINGS

- 1) *The Elements of Intranet Style* by Eric Brown, Cyberpress (Publisher).
- 2) *David Linthicum's Guide to Client/Server and Intranet Development* by David S.Linthicum, John Wiley & Sons.
- 3) *Building your Intranet with Windows NT 4.0* by Stephen A.Thomas, John Wiley & Sons.

Reference Websites

- 1) <http://www.intranetjournal.com>
- 2) <http://idm.internet.com>
- 3) <http://www.cio.com/forums/intranet>
- 4) <http://www.gooddocuments.com>

UNIT 3 CHOOSING INTRANET HARDWARE AND SOFTWARE

Structure

- 3.0 Introduction
- 3.1 Objectives
- 3.2 Selection of Computing Infrastructure
- 3.3 Hardware
 - 3.3.1 Servers
 - 3.3.2 Clients
 - 3.3.3 Security Systems
- 3.4 Network Environment
 - 3.4.1 Local Area Network (LAN)
 - 3.4.2 Address Translation
 - 3.4.3 Firewall
- 3.5 Software
 - 3.5.1 Operating System – Server and Client
 - 3.5.2 Groupware
 - 3.5.3 Database Connectivity
 - 3.5.3.1 Basic Connectivity
 - 3.5.3.2 Middleware Support
 - 3.5.3.3 Open Database Connectivity (ODBC)
 - 3.5.3.4 Java Database Connectivity (JDBC)
- 3.6 Other aspects
 - 3.6.1 Protocol Support Tools
 - 3.6.2 Web Based Tools
 - 3.6.2.1 HTML, XML, CGI and other Open Standards
 - 3.6.2.2 Web Authoring Tools
 - 3.6.3 Security Tools
 - 3.6.3.1 Firewalls
 - 3.6.3.2 Virtual Private Network (VPN)
 - 3.6.3.3 Encryption/decryption using by SSL
- 3.7 Summary
- 3.8 Model Answers
- 3.9 Further Readings

3.0 INTRODUCTION

Intranets not only provide a secure environment for the companies, but also provide excellent working environment that is full of information and resources for the users as well as decision makers in the company's management. Intranets use a greater part of the system and networking resources. If the data is bulky and consisting of audio or video then they must have broader bandwidth as well as higher throughput for transmission of data. Whereas general messages and documents forming major part of textual information require less time and transmission speed, the multimedia files require more than 10,000 times the transmission bandwidth. This bottleneck must have been faced by almost everyone accessing the Internet via modem, and the difference it makes when accessing the Internet through ISDN or leased line connectivity. Evidently, the amount of time it can take from the moment a web page is requested, gets loaded along with all the graphics until the user actually sees the affect on the computer can be considerable.

Now that many organizations are demanding higher services (also called value added services) such as faxing, minimal cost call routing, connectivity to the corporate EPABX, chatting, video conferencing, IP telephony, etc. would on one side require heavy investments but on the other side assure value for money. These value added services though seems to be costly at the first instance, provides reduction in recurring expenditure of communication costs while enhancing productivity. Installation of such services requires one time high budget. The companies are realizing that videoconferencing over an intranet can offer a highly cost-effective alternative to many face-to-face meetings, especially where the members or decision makers are located at far of places.

Just few years back, when analog audio and videoconferencing systems were used, the procurement and installation was complex, less reliable as well as costly. With the advance of technology and reduction in communication costs, it has become possible to send and receive voluminous amount of information much quickly and at almost negligible costs.

3.1 OBJECTIVES

A number of software tools are available in the market today. Similarly, hardware of various specifications are available to choose from for building and maintaining an Intranet. Concepts on how to select appropriate hardware and software for running a successful intranet are dealt with in this unit. In addition to the hardware and software, other aspects that are essential for a good intranet such as database tools, connectivity, security, etc. have also been covered.

3.2 SELECTION OF COMPUTING INFRASTRUCTURE

Since an intranet can be defined as simply a standard WAN limited to an organization, powerful hardware should be made available for web server. The computing equipment must be selected in such a manner that they do not get obsolete very quickly or become too costly for the company.

It is also important that other points such as the following along with their specifications should essentially be considered and drawn carefully:

- Communication medium/services that provide connectivity between different locations of the company should use technologies such as ISDN, leased line, etc.
- Network equipment and connectivity should address various networking equipment such as routers, types of cables, as well as the topology behind the network.
- It is a must that the hardware should be configured for protocols such as IP, HTTP, SMTP, POP, X509 Certification, etc. in order to provide security to the intranet server.

For an intranet to work smoothly, the following tasks should be properly synchronized:

- All computers connected together in a network must communicate using the same language and protocol. Inability to do so may leave the users disconnected to the repository of information and resources.
- It must be always remembered that the language used is Hyper Text Markup Language (HTML) and every thing that is developed for and intended to be hosted on the intranet must follow HTML invariably.

- The protocol suite applicable for both intranets and Internet are called Transmission Control Protocol/ Internet Protocol (TCP/IP) and every computer should be compatible to TCP/IP. Though, TCP/IP evolved initially on UNIX based computers, it became a standard for data communication and more recently for every type of communication across intranet and internet, especially supported by every major operating system in use.
- The intranet is driven by a network server that uses a browser, like Netscape Navigator or Internet Explorer.

3.3 HARDWARE

Hardware forms the greatest asset of the company, but it reaches the obsolescence rate very quickly. Normally, it is said that every six months technology in the electronics, telecommunication and computing discipline changes. With such rapid rate of obsolescence, it is very important how the professionals select hardware equipment including the server, clients, peripherals, etc. while maintaining a proper balance between cost and the obsolescence rate.

Care must be taken to ensure that proper spare parts are available even after about five years of commissioning. In addition to this it should also be ensured that proper and reliable service backup is available throughout for keeping the intranet at maximum uptime.

Whenever any component of the entire intranet system breaks down or any extra component of higher capacity is required to be added, proper compatible component must be selected.

3.3.1 Servers

The success or usage of the intranet server is measured by the number of operations it handles per unit time. The selection of a good server depends on how many connections per hour it is expected to handle.

While most of the parameters are too general, the most important checkpoints for selection of a server would be the type and speed of processor, its memory capacity (both primary and secondary), number of connections it can handle easily, etc. Typically, a mid range or high-end server with following specifications would be sufficient for a medium to large organization:

A Pentium III Xeon based server (dual processor recommended).

2 x 40 GB HDD (one extra recommended for backup).

128 MB RAM (256 MB recommended).

As it is, normally, there is absolutely no restriction or limits on number of nodes within an Intranet; any organization with 10000 web servers can form an Intranet. Limits exist only on use of licenced software or on user restrictions on the network environment.

If anyone intends to have higher configuration such as installation of four processors in the place of conventional one processor, the cost factor for each processor should be considered first. It is possible that each processor of server range may cost anywhere from Rs. 1.25 lac to Rs. 2 lac, thereby taking the cost of server straight up between Rs. 12 lac to Rs. 15 lac.

The hardware i.e. the server or computer has a direct relationship on performance in the following areas:

- Reliability and Recovery,
- Service Support, and
- Speed of information access.

The reliability of the machine can be dramatically improved by installing the best components. Hot swapping is a concept through which components can be replaced or repaired while the server is on-line and there is no necessity to switch it off. After replacement, the server automatically configures the newly added component. Hot swappable hard disks, processors, power supplies, etc. are currently available components.

Very powerful and mass store back-up devices help in ensuring recovery of data from hardware failures with minimum efforts.

Service Support must be considered as a strong point for hardware, especially for servers and should be available readily. Many branded products such as HP, Compaq or Dell servers come with good and strong network of support services. The hardware are usually bought with service contracts or warranties, which could be extended for further periods as needed.

It is obvious that the information can be retrieved faster if the processors are faster, RAM is bigger and hard disk drive access is faster.

Once the server is configured the cost of connecting the machine to the Internet plays a vital role. The connectivity is usually priced in two ways viz., an amount of data downloaded per unit of time e.g., 1-5 GB per month; or a fixed bandwidth or (data transfer speed) of 64 kbps, 128 kbps, etc.

A peculiar situation arises when the existing server arrives at a stage when it can not handle the requests quickly and most of its time is spent handling the threads or tasks as well as swapping the processes between primary memory and hard disk for want of more and more memory space. This is an indication that the server immediately requires more resources and that it has become overloaded. In order to provide more computing power, the following steps may be taken:

- Add more processing power by addition of more number of processors. But there is a limitation to this also. In most servers, it may not be possible to add more than six processors. The number of processors required should be carefully decided keeping in view the future requirements of the company. The Xeon based Intel processors are of extremely higher capacity as compared to the traditional processors.
- Add more memory (both hard disk as well as primary memory). This means that extra memory cards for primary memory may be added. Usually, the main memory is doubled and kept in terms of any value raised as power on 2, for instance, 8 MB, 16 MB, 32 MB, 64 MB, 128 MB, 256 MB, 512 MB, 1024 MB (or 1 GB), etc. are acceptable memory space indicators. It may also be necessary that the amount of cache be enhanced based on the need. The cache memory is normally counted in terms of kilobytes. The hard disks come in different capacities like 8 GB, 18 GB, 40 GB, 72 GB, etc. to choose from. Addition of more memory indicates that there will be lesser read/write operations on the hard disk as well as the processing speed would be higher as the primary memory is faster than the secondary.

It also happens that addition of more computing power or more memory space does not make much difference and the server remains overloaded. During such circumstances, the entire hardware requirement should be carefully reviewed. It is recommended that more number of servers be added after proper arrangement in the form of separate servers for database, application, email, security, etc. There could be three database servers connected as a cluster to the main server to provide better connectivity and services.

The basic software required for the server should be capable of handling NCSA HTTPd and CERN HTTPd. Products such as Netscape Enterprise Server, MS IIS, FastTrack Server, etc. are well known products in this line. They are available (both free as well as commercial) for variety of OS such as UNIX, Windows NT, MacOS, etc.

3.3.2 Clients

The most interesting thing is that almost every computer can be connected as client to the intranet server. The client could be based on any architecture whether Intel, AMD, Motorola or any other well known processor or operating system such as Unix, Windows NT, Mac OS, etc.

In addition to the operating system, a client would require only a browser such as MS Internet Explorer, Netscape Navigator, NCSA Mosaic, Lynx, Emacs, Midas WWW, etc. to work comfortably with the intranet. It must be ensured that the browsers have the following:

- Browser is of latest version,
- It supports TCP/IP, and
- It is compatible to Microsoft and Java technologies.

3.3.3 Security Systems

If the company intends to connect to the Internet, then it should pay great attention to the configuration of firewalls. Just as no one would leave the house unlocked at night, it is also expected that no one would leave the computer system or intranet open to various attacks from the outside.

As already covered in the Unit 2, securing an intranet is not a simple task. Mere installation of firewall hardware and software would not help the intranet to protect itself. Proper configuration as well as updation from time to time is also as essential.

Some firewalls are available in form of ready-made hardware equipment whereas some are available as customizable program, but some firewalls are sold as features of hardware routers or combination of both hardware and software.

All the units entering the intranet must be scrutinized to ensure that they are not coming from the unauthenticated sites or users. It also helps in checking whether someone of the company is not trying to go beyond the intranet system to access prohibited sites or competitors' system.

Proper programming of the ports of the company's web server through detection of IP addresses could be an excellent strategy or solution for preventing every unauthorized access. For example, it is possible to set up a firewall policy that will exclude everything sent to port 80 (that is mostly used by hackers) except those sent to the public Web server. It may, however, be noted that this kind of filtering can only act as a good first level of security.

In addition to the above method, the company should install additional levels of security measures since it is possible for hackers to generate and send data with headers of the data looking like those send from authorized users. Difficulties start when the hackers or attackers obtain information regarding the server, certain hosts and subnets of the intranet.

The best method to protect the web servers or intranet servers is to use application gateways or simply "proxies". These gateways act as intermediaries between users' systems and external systems and handle identification or authentication at a higher level than at hardware level. Every request, whether from outside or from within the intranet system, would first be received by the proxy server, which scrutinizes the requests and prevents the undesirable and unknown ones.

Even the destination web site or user would not be able to know that the interaction being done was with the proxy or gateway server and not the actual server, thus sending and receiving data "on behalf of the user". This kind of proxy or gateway can be useful for providing secure services encompassing HTTP, FTP, Telnet, email, etc.

Another best methods to keep the attackers at bay is known as network address translator or NAT. The philosophy behind the design of NAT is that the more an attacker knows about the intranet, the easier it would be attack and cause damage to it. It is sufficient to know the IP addresses of a server to open it and destroy every important data posted on it.

There is a separate set of IP address for a company's internal use, more popularly known as "internal IP address" or subnet IP address. This IP address is never passed on to outside. It is useful for every communication within the organization.

For dealing with external communication, the web server must have a static IP. Having a static IP could also be a problematic issue. As far as web servers generate dynamic IP addresses (those addresses assigned to users when they connect to the server and this changes every time they log into the intranet), the entire network is safe as the hacker or attacker would never be able to detect from where the request or information has actually originated. The NAT equipment serves as address translator from internal to external IP address and vice versa and routing them within these private addresses.

The firewalls available today do all the things like filter the data packets, provide proxy services and do stateful inspection of packets. Now-a-days, the firewalls are providing additional services like detection and cleaning known viruses, as well as prevent unwanted Java or ActiveX programs.

3.4 NETWORK ENVIRONMENT

Since intranets as well as the Internet are based purely on networks, the company intending to install intranet must consider a number of aspects before hand ranging from network planning to final implementation, security, storage and backup. Some of the issues necessary are:

- Network planning should be carried out study of network requirements covering the following important issues:
 - Preparation of list of components
 - Planning network topology
 - Task of conduit laying
 - Task of cable laying. Cable planning should include the comparative study of
 - Using Twisted-Pair Cable
 - Using ThinNet Coaxial Cable
 - Using Fiberoptic Cable
 - Testing of the points
 - Testing of the entire network through various clients
 - Planning for Network Hubs
 - Estimating time schedule
 - Estimating manpower required
 - Estimating total cost of components

Network installation

- Buying the components
- Cabling the network
- Installation of networking components such as hubs, switches, routers, gateways, etc.
- Expanding the network

Security

- Choosing a gateway or proxy server
- Installation and testing of proxy
- Choosing security measures especially the firewall
- Installation and testing of firewalls

Other essential services

- Installation of anti-virus measures
- Testing connectivity to databases
- Testing connectivity to Intranet and the Internet
- Installation and testing of connectivity to other network peripheral devices
- Installation and testing of network-attached storage.

14.1 Local Area Network (LAN)

LAN stands for **Local Area Network**. A LAN is an interconnection of computers and associated peripherals as well as to the communications system that allows users to access and share resources (computers, printers, servers) with other users.

Text, images, audio, full motion video, fax, and many other value-added services can now be shared over the LAN. They are great time and money saving electronic components for the companies to share resources and information. They are simple, inexpensive, and support a number of protocols. Though there are a number of types of networks, the networks are designed in such a manner that one supports the other. The exact number of benefits accruable from networks cannot be enumerated easily in terms of monetary benefit.

In order to understand the LAN system, one must first become familiar with the basic terminology and concepts. The most common terms and concepts that are specific to LAN are as follows:

- LAN transmission media
- LAN technology and topology
- Network protocols
- Network management
- LAN applications
- LAN networking devices.

Detailed study of the networking and various technologies available under it are beyond the scope of this unit and hence not being covered. It is advised that in order to acquire complete information on networking technologies, relevant course material may be referred.

14.2 Address Translation

When a web site address or URL is typed in the web browser, email or other web related service, note that it is typed something as www.startv.com and not as series

of numbers. It is essential for the server to know where exactly the data has to be sent to or received from, this address is mapped on to (or translated into) a series of numbers. The translation is called "domain name resolving", "host name resolving" or "name server lookup". For instance, the VSNL site address ~~www.vsnl.net.in~~ would translate to a group of four octets like 202.30.15.30. The translation is done on the whole name and not on each byte between the periods.

The task of number translation is done solely by a domain name server (DNS) on the intranet server. Like all devices, it has its own IP address (e.g. 194.62.15.20).

The router must have an IP address of the same network (194.62.15.x in this case) for the convenience of the entire network to use the services of the router. The NAT router also has a separate IP address that would be used for external communication through the Internet. Note that all IP addresses are unique and any duplication would result in collision. For example, a NAT router may have IP address of 194.62.15.2 for internal use and 202.63.10.15 for external or public (or internet or ISP) IP address.

If the request is for a computer outside the LAN, it is just sent to the router. A normal router would just route everything via the Internet to the server computer, however, a NAT router would replace the IP of the source compute with its own IP address so that while receiving acknowledgement or any error response, NAT may handle it first and then permit it to the LAN.

3.4.3 Firewall

The NAT router allows receiving of number of data streams. If it receives a transmission in the form acknowledgement or data streams or error responses from an external server due to a particular request from an internal user, then it will receive the data, translate the address to local IP address and forward it to the requesting user.

By preventing all incoming requests or connections except those expected or permitted, the router acts as a "firewall"

3.5 SOFTWARE

For an intranet to be successful, it must have strong software support. In this section, brief description about the operating system, groupware and databases has been discussed. Though there are a number of tools supporting the intranet such as web authoring and management, they have been put up in a separate unit in this block.

3.5.1 Operating system – Server and Client

Various operating systems that support intranets are all variants of Windows and Unix. In addition to these, certain other software relevant to intranet operation are required. For instance, a range of Microsoft products for intranet operations available are as follows:

- Back Office Server 4.5
- Back Office Server 2000
- Site Server 3.0
- SNA Server 4.0
- SQL Server 7.0
- SQL Workstation 6.5

These above software contain a number of components such as SQL Server for database connectivity, Systems Management Server for easy web management, FrontPage for web authoring, Visual Interdev 6.0 for web programming, etc.

They also contain a whole lot of value-added software such as a BackOffice Server Manager console, branch office setup and various other deployment tools, and the intranet starter site and starter applications.

3.5.2 Groupware

Groupware are collection of software tools that encompass a broad range of applications. Even though groupware broadly consists of applications like calendars, project planning, sharing documents, emails, etc., it is many times costlier than intranet e.g. a Lotus Notes application can cost over Rs. 8 crore for a big group whereas for same group corporate intranet could be easily served with about Rs. 8 lakh.

These application are many but not limited to the following:

- Communication tools
 - Voice mail
 - Email
 - Fax
 - Video conferencing applications.
- Project management
 - Project planners
 - Project management
 - Project scheduling.
- News and general services
 - Electronic bulletin board services
 - Electronic calendar service
 - News service
 - Reminder services.
- General office management tools
 - Document management
 - Office productivity tools
 - Spreadsheets
 - Word processors
 - Graphical editors.
- Web tools
 - Authoring
 - Publishing
 - Content management
 - Other graphical tools
 - Simple security tools.

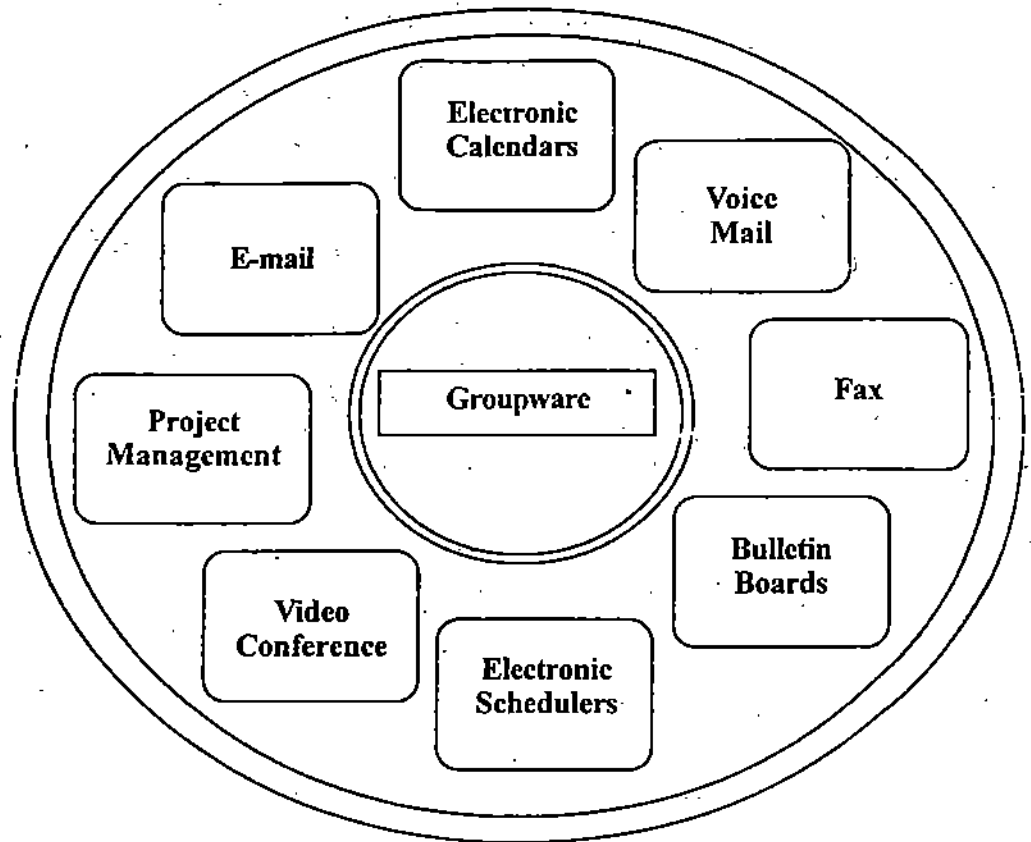


Figure 1: Contents of a groupware

With the use of groupware, users can easily do most of the office related management work, which otherwise would be extremely difficult. For instance, it would be possible to edit, analyze, share, store and retrieve document. Still further, they can be very comfortably translated, or published in no time. They help a lot in increasing the productivity of every user as well as of the organization as a whole.

The downside of groupware is that they are very costly and with the increase in complexity or additional features, the cost too increases proportionately.

However, since intranets work purely on inexpensive browsers as front-ends and actual applications on the web server as back-end, many-a-times the groupware proves to be cheaper, but such implementations are rare.

As long as same operating system and hardware were used, there were no problems, but maintenance and technical support cost was extremely high. Additionally, the software team has to learn every bit of things related to computers. Since different users work on different platforms and application, which in turn use different protocols and services, there was no coordination or collaboration between one another.

With the advent of intranet, users were free to use any platform they like on any computer architecture. In order to eliminate every kind of barrier, all they had to have is a HTML and Java support through browser that remains the only requirement. Now, the users do not have to learn everything and can comfortably concentrate on their line of working leaving the intrinsic details to the intranet software or groupware.

It may be noted that the most difficult part of any intranet is document management. Whereas document generation, delivery and distribution, etc. phases are relatively easier as compared to any earlier methods, the management of huge amount of day-to-day documents still remain a problematic issue. Not just storage but context based search also has been troubling the groupware developers.

Many developers have found solution to this problem through a specialized tool called the content management tool. These tools were initially developed for use of web site management, it found suitable place readily on the intranets as well and has now fast becoming the strong feature of all.

The latest technology in the line of intranet tools has been the Web-based Distributed Authoring and Versioning (WebDAV), which is an extension to the existing HTTP services. A number of functionalities have been added to the WebDAV thereby making it the ultimate for web authoring, publishing and collaboration. It is now like to evolve a new file system like NTFS, FAT, etc. called the web file system. WebDAV is one of the best-used server modules and many companies developing intranet software or groupware as well as various publishing and office management tools are going ahead to incorporate its support features to their products. For example, Dreamweaver, Director and Flash support the intranet, enabling even more disciplined approach and association among the designers and developers who create powerful and massive web sites. A number of developers of service tools like the FTP, Telnet, etc. are also supporting the cause of intranet.

3.5.3 Database Connectivity

3.5.3.1 Basic connectivity

A number of database management systems are available today such as the Oracle, Sybase, Ingres, Gupta's SQLBase, etc.

Most of the databases that are used to store massive data for use through Internet deploy Relational Database Management System (RDBMS) designed for PC class hardware. They are also available in both server (workgroup) and local engine (standalone) configurations, and are usually bundled with the power of Structured Query Language (SQL), transaction processing, and distributed processing for building business applications. By supporting client/server architecture, these software achieve a higher level of scalability, which makes them suitable for a wide range of applications; from a standalone, single-user environment to a multi-user workgroup environment.

To build the client side of applications, developers use various tools. Some of the popular software development environments include Visual Basic, C/C++, Power Builder, Java, Delphi, etc. It must be ensured that the databases can connect to these programming languages, or in other words, these database management systems should support these languages by being backend support.

3.5.3.2 Middleware support

All the connectivity interfaces related tools come under the category of middleware. Middleware provides the link for data exchange between the different points of processing in a distributed application. In an intranet application, the points of processing are the database software the server software and the client application.

Many of the popular databases also provide support of and to the middleware and consequently, the term middleware has become lesser known. Though software like the ASP, Perl, etc. have got wide popularity, a lot of work is being done to integrate a number of features of the traditional software made available in the middleware also.

During processing of any request, the client/server architecture is maintained and the database and client applications are processed separately eventhough running on the same platform or machine. For certain middleware, a connectivity interface is not required to support data exchange between the application and middleware or database.

3.5.3.3 Open Database Connectivity (ODBC)

It happens that in addition to conventional or most popular database management systems, many companies go for proprietary software creating problem for themselves as well as for the clients. It is strongly recommended that companies should use that particular DBMS software which is most popular and widely used.

If this is not followed, a number of difficulties arise with database connectivity and the company may have to shell out enormous amount of money on obtaining proper connectivity tools.

It must also be ensured that whenever any DBMS or middleware is procured, all relevant database connectivity tools are also bundled. Most important of all of the connectivity tools or drivers is the ODBC, which permits connectivity to any type of database from the client application.

Many developers provide not just a simple ODBC driver, but a complete industry standard ODBC database solution for a wide range of operating systems such as Windows, Unix, Linux, MacOS, Sun Solaris, etc.

3.5.3.4 Java Database Connectivity (JDBC)

With two different types of technologies available in the market today viz., the Windows and the Java technologies developed by the Microsoft and the Sun Microsystems respectively, it is essential for any company to ensure proper integration of the two technologies so that the customer support is ensured inspite of the technological divide.

Not just ordinary ODBC tools and drivers, it has become almost essential for the companies to obtain the JDBC drivers as well. With JDBC drivers, it would become possible to connect the Java applications with any type of databases and can query as well as update data from any data source across intranets or the Internet.

3.6 OTHER ASPECTS

There are considerations for an intranet other than just hardware, software and security. They are the protocol support, web based tools and security tools.

3.6.1 Protocol Support tools

Intranet should support the tools meant for providing various services on the Internet through the protocols. In addition to the conventional TCP/IP support, the intranet base should also extend support to a variety of protocols such as the IPX, SPX, NetBIOS, etc. thereby providing a total freedom from the network architecture, machine dependence or topology dependency. The following is the list of protocols supported by intranet:

- ARP
- TCP
- IP
- FTP
- Telnet
- HTTP
- SPX
- IPX
- UDP

- POP
- LDAP
- SMTP
- HTTPS
- CGI
- NetBIOS
- IMAP
- SOCKS

and others.

3.6.2 Web Based Tools

3.6.2.1 HTML, XML, CGI and other open standards

As is well known that the web as well as intranets speak and understand only one language i.e., the HTML. The browser at the client's end after downloading the pages from the server, interprets the language and converts it into human understandable format and the output would be what everyone actually see on their computers. Until recently, HTML was available as an open standard i.e. it was not under control of any vendor. Web application developers intending to release their product had to conform to this standard.

With the increasing competition between certain vendors especially the Microsoft and the Netscape, there has been a number of changes to the open standard. One company introduces interactive components; other adds capability of audio and video. In the meanwhile, another company would add frames and still another would add Java compatibility.

Even the companies or developers themselves have been affected with such modifications to the open standards since they would rely only on their technology and could not get the benefits of other powerful features. On the clients' side, there will be great frustration since they would have to choose only one from all the available technologies. The story does not stop there. A number of features as well as new languages like the ASP, CGI, Perl, XML, DHTML, VRML, etc. have evolved since the HTML open standard was released.

It would be clear from this situation how important standardization is. It has now become essential that all the major developers come together along with the group of customers and include in their products all the features that the customers like to have. This would bring them lot of prosperity as well as total customer satisfaction can be ensured.

More details on standards, protocols and services have been discussed in detail vide Unit 6 under the heading intranet protocols.

3.6.2.2 Web authoring tools

CGI was considered excellent in the beginning since it was also open standard. The only drawback it suffered was that it was slow. Major software developers virtually ignored the CGI and consequently CGI could not survive the competition.

Need arose for addressing various issues related to the web programming. Software were required for establishing connection, ensure security, connectivity to databases, conversion of the results to web format, and lot many more. In response to the rising needs, numerous vendors have come up with numerous products, some of them like the following:

- IntraLaunch
- CodeCharge

- Benefit Profiles Portal Suite
- Servicespace Suite consisting of Enterprise, Customer Portal, Partner Portal
- LiveHelp
- HTML/OS
- WebSiteManager.

This aspect of web authoring and management tools is not being discussed here in detail since it has been covered in Unit 5 under the heading Web authoring and management tools.

3.6.3 Security tools

Securing an intranet is not a simple task. Just as articles in a house are protected by use of various types of security systems such as lock and keys, almirahs, burglar alarms, etc., so also the intranet should be protected using various types of security systems.

A number of security products covering a broad range of methods are available in the market. Most popular of all the security measures are the firewall, the VPN and the SSL. While the firewall is supposed to be easily manageable and configurable as compared to all other security measures, the VPN and SSL are considered the most inexpensive and easy security methods.

3.6.3.1 Firewalls

While getting one firewall for the company's intranet it should be well known that firewalls come in both hardware and software forms, and that even though, all firewalls are programmed, they require proper configuration at the time installation to suit the requirements of the company. While doing so a number of considerations have to be taken into consideration.

The firewall vendors may be giving tall claims about the success of the product in the world, but the purchaser must keep a number of issues ready before actually obtaining one for the company. The customer must be cautious that firewall security can be highly complex and that just simplicity can not be a good measure for the performance, and finally that the firewall after installation requires proper configuration.

While deciding whether to buy a hardware or software firewall, the user must consider important factors such as performance and flexibility. Hardware firewalls can be easy to set up and may also be customized to improve performance, the software firewalls offer the flexibility of use on any hardware platform is available, and the platform can be upgraded much easily and thereafter moved to a different platform altogether.

The Unix-based firewalls are considered most secured as compared to the Windows NT based ones. The firewalls binds the holes of the operating system under which it has been installed by closing all the security holes and by eliminating all possible services that could be used by attackers.

There are proxy servers that act as good firewall protection for the entire intranet system. In some cases, firewall comes as a separate server altogether, whereas in certain cases, firewall themselves can act as a proxy server.

It must be ensured that the firewall is being updated from time to time and the personnel responsible are alert and loyal.

3.6.3.2 Virtual Private Network (VPN)

Even though, many firewalls also include the features of the virtual private network, the functionality and capabilities of VPN capability are different from that of the firewall.

It is important to understand that installing a firewall is only one part of a security strategy. In addition to it, other aspects such as user authentication through username/password combination, VPNs, a public-key cryptographic code and resource management should also be added to the policy of the company's intranet security.

When determining requirements for a VPN, carefully estimate the number of systems to be put behind the VPN, the number of concurrent users, the type of Internet connection in use, etc. It is also essential to study the degree to which internal systems must be protected, the available resources to maintain the VPN, and what security functions are intended from the VPN to perform.

3.6.3.3 Encryption/decryption using by SSL

Once a session is established, the SSL generates a session key using public-key encryption to exchange information between the client and server. This key is used to encrypt the transaction for both request as well as the response. It would be extremely difficult for the attacker to get into the system since each transaction uses a different session key. Hence, even if the attacker succeeds to crack the code of a transaction, he can not use the same key every time for cracking and will have to spend enormous amount of time as he did for decrypting the first key.

Most of the server and browser software developed by various vendors carryout encryption using either a 40-bit or a 128-bit secret key. It is felt that using a 40-bit key could be insecure since any possible combination of 2^{40} can be computed easily using modern day computers. Relatively, use of a 128-bit key eliminates this problem as there would be 2^{128} possible combinations instead of just 2^{40} .

Software are coming up in which the user can select what kind of security measure can be taken for encryption. One such example is the Netscape, in which the user can select from available encryption methods and size of key.

Description of security tools is not being dealt here in detail since it has already been covered in greater detail vide Unit 2 under the heading Intranet's security.

Check Your Progress

- 1) The protocol suite applicable for both intranets and Internet are called _____ and every computer should be compatible to _____.
- 2) There is a separate set of IP address for a company's internal use, more popularly known as _____.
- 3) The NAT router allows receiving of number of _____.
- 4) The latest technology in the line of intranet tools has been the _____, which is an extension to the existing HTTP services.
- 5) _____ is a Web authoring and Management tool.

3.7 SUMMARY

The selection of computing infrastructure should be done on the basis of

- Obsolescence rate
- Cost factor for replacing the old
- Cost difference to replace with new equipment
- Number of major faults during its existence
- Number of upgrades done
- Maintenance overhead
- Availability of spares and service.

These parameters could be considered for both hardware, software and networking environment, as far as applicable. Whenever any one or two of the above parameters becomes extremely high, it stands as an indication for immediate replacement.

Many organizations are using intranets to replace the costly groupware and e-mail applications with simple intranet applications that cost only a few thousand rupees. Organizations initially start their operation with developing one or two applications and attempt to host them on the web thereby making them web-enabled. On success, they develop other application software on the similar lines based on the experience acquired. This kind of approach is also proving to be the cheapest and the best of all strategies. Once all the required applications have been developed, the entire software takes the shape of an enterprise-wide system (may be similar to an enterprise resource planning or ERP type implementation).

The benefits of groupware implementation are

- It allows users to freely exchange, analyze, edit, store and retrieve documents and messages.
- It eliminates barriers of time and space.
- It promotes increased responsiveness and significant improvement in quality of business processes.
- It provides standardized approach to processes.

3.8 MODEL ANSWERS

- 1) Transmission Control Protocol/Internet Protocol, TCP/IP
- 2) Subnet IP address
- 3) Data Streams
- 4) Web based Distributed Authoring and Versioning
- 5) Code Charge

3.9 FURTHER READINGS

- 1) *Practical Guide for implementing secure Intranets and Extranets* by Vinton G.Cerf, Artech House (Publisher).
- 2) *Designing the Total Area Network: Intranets, VPN and Enterprise Networks Explained* by Steve Pretty, John Wiley & Sons.
- 3) *Reality Cold Fusion: Intranets and Content Management* by Ben Forta, Macromedia Press.

Reference Websites

- 1) <http://www.brill.com/intranet/ijx/index.html>
- 2) <http://indiafocus.indiainfo.com/internet/index.html>
- 3) <http://community.marion.ia.us>
- 4) <http://www.planet-intra.com>

UNIT 4 CONFIGURING INTRANET

Structure

- 4.0 Introduction
- 4.1 Objectives
- 4.2 Configuring Intranet
 - 4.2.1 Web Authoring Preview
 - 4.2.2 Web Graphics
 - 4.2.3 Adding Interactivity
- 4.3 Installation
 - 4.3.1 Network installation and administration
 - 4.3.2 User management
 - 4.3.3 Disk Quotas
 - 4.3.4 Security Configuration and Analysis
 - 4.3.5 Account Policies
 - 4.3.6 Permissions and restrictions
 - 4.3.7 Tuning server performance
 - 4.3.8 Configuring network settings
- 4.4 Networks and Security
- 4.5 Tuning applications over Intranet
- 4.6 Summary
- 4.7 Model Answers
- 4.8 Further Readings

4.0 INTRODUCTION

The next step in setting up an intranet is to configure intranet that is to how to create and host the web pages and step to secure the network. There are different types of web page authoring tools for content creation. Managing user and granting permission and restriction is also important part of Intranet administration. Decision like risk level and how much exposure one can stand. Once that is done it is now time to find out where the network is vulnerable.

The next part of this section deals with discovering the vulnerabilities on network. Unfortunately, there are dozens and dozens of ways network can be compromised, and the first step in finding them is by looking around.

4.1 OBJECTIVES

In addition to the basic tools for authoring intranet, various other issues related to intranet such as the user management, hosting on intranet, permission and restriction, network security issues and tuning applications on intranet is discussed in this unit.

4.2 CONFIGURING INTRANET

The first step of setting up intranet is to configure a web server. Many web servers are available some of them are commercial and some are free. One of the popular web server is Apache, the current version of Apache web server is 1.3.3-x. It is available free with Red Hat Linux 5.2, and can also downloaded from <http://www.apache.org>. It set-up and ready to run automatically at boot as soon as the

Linux installation is completed. Apache web server is extremely powerful, and can be configured to handle any kind of environment from a lightly loaded Intranet to a commercial heavily loaded Internet Web server taking more than 100,000 hits a day.

It is very simple to test the working of Apache web server, simply point the browser to the URL `http://localhost`. The Apache's default "It Worked" page starts up. The `index.html` file in the `/home/httpd/html` directory can be changed to start publishing pages on the Intranet. The default configuration file `/etc/httpd/conf/httpd.conf` is suitable for simple configurations, though one might want to edit it if there is an unusually heavy load, or wish to configure a different machine name, port, or address to send error messages.

4.2.1 Web Authoring Preview

All that is needed to author a Web page are a word processor, attention to detail, common sense and a computer to serve the page where others can access it with Web browsers. Web page can be in any word processing or text editing program. Using a word processor requires knowledge of Web page programming language HTML (hypertext markup language). Use of software designed specifically for Web authoring eliminates the need to know HTML language and make creating a Web site as simple as typing on a word processor. Newer word processors (e.g. MS Word) can even export formatted text to HTML.

Many web page editing programs also provide for basic editing and placement of graphics and have built-in file transfer protocols to upload web pages to the server. Web pages consist of text marked with HTML tags that give a web browser guidelines for how to display or align text and how to link text or graphics to another file on the Internet. For example, to emphasize something, enclose the required text in a pair of tags, such as: ``. This is a demo text line!!!! It!``. A Web browser will then show **This is a demo text line!!!!** in boldface type, in this example, to make it stand out visually. Attention to detail counts, because HTML tags are picky, and typographical errors can highly embarrassing on even simple pages.

It is important to see what the web site looks like on many different browsers and computers, and then edit it appropriately. It is also important to name graphics for people with browsers that cannot view them.

4.2.2 Web Graphics

Most of today's web browsers support two graphic formats: GIF and JPEG. Both formats use internal compression routines that make the graphics smaller, thus decreasing download times. When it is decided to put a graphic on the Web, it is important to decide whether to use GIF or JPEG.

GIF Versus JPEG: GIF stands for graphics interchange format. It is the only format that all graphics-savvy browsers can display, so it is the format to use for graphics that is to be seen by everyone. The bad part about GIF graphics is that they are limited to 256 colours and typically do not compress as well as JPEG graphics do. The latest version of the GIF specification (version 89a) supports transparent mode, a nifty option that make one colour in a graphic transparent. GIFs are shaped like rectangles, to make a GIF's background colour transparent, one can end up with a GIF that looks like an irregularly shaped object.

GIF

GIFs also can be interlaced, meaning the image is saved in alternating horizontal bands. Looking at the first half of an interlaced GIF, one would see a low-resolution, striped image, with blank horizontal stripes representing the second half of the image. Some browsers display interlaced GIFs as they read them, first they display every eighth line, then every fourth line, then every second line and then

every line. This display method makes it so people waiting for the image to load can quickly figure out what the final image will look like. Other browsers bring in a rough version of the graphic and gradually refine it. GIFs also support animation. It is possible to piece together numerous GIFs and create a simple movie.

JPEG

JPEG stands for joint photographic experts group. It is a graphics compression format that works best for digitized photographs, particularly if they depict photos of natural scenes such as forests or sunsets. JPEG was designed to lose details that the human eye often will not notice, particularly details that would not be noticed from an image with gradual changes in shading and colour. JPEG is most likely to lose too much detail with images that have sudden transitions from one colour to another, so JPEG tends to be a poor format for graphics containing text, line drawings and navigational icons. JPEG images can have millions of colours instead of a just 256. They have better compression, but many older browsers cannot display them without the assistance of a helper application (where the picture displays in a different programs window).

The bottom line: Use GIF unless one has a photograph that looks much nicer or compresses significantly tighter as a JPEG.

4.2.3 Adding Interactivity

Once the construction of basics like text, hyper text links and graphics are over, interactive additions such as image maps, sound, video, search capability, database retrieval, forms and even encryption security is desirable depending on the type of requirement. These advanced functionalities require the help of technologies such as Java programming, common gateway interface (CGI) scripting or the addition of plug-ins. They usually require additions to and modifications of the server software. Such a discussion is beyond the scope of this topic.

Hosting Web Pages on the Internet

Organizations that will host the web pages, can be asked from the Internet service provider (ISP) or system administrator. Another option to serve the web pages is dedicating a computer to run Web server software. The advantage of a dedicated computer is personal control of Web server software. This option requires a dedicated Internet connection. Some ISPs also provide a option to keep web server computer at their site for a direct Internet connection. This usually requires remote control software or many trips to the ISP. Personal server software is becoming popular for small-scale Web sites on office computers with a dedicated Internet connection.

After finding an organization that will serve the web pages or choosing own Web server software, some question can be asked:

1. What kind of file name extensions are used? The Web is very particular about file names, the file names must end with an extension that indicates the file type. For example, a Web page coded in HTML needs a .htm or .html extension. The specific extension and the length of the file names depend on the server that serves the files. The beginning Web page may need to be called homepage.html, default.html or index.html depending on the server software.
2. How to updates pages? This is usually accomplished by using file transfer protocol (ftp) to transport all the html documents and graphics files to a specific directory on the server. FTP access to the server along with a password is required for this.

HTML code is easily downloaded for review. It is also possible that if some web site technique that is of interest, can be simply saved as HTML from its code. This will provide special techniques that are used in developing own web pages. Web site graphics are also easily downloaded as HTML files but there is need to consider infringement of copyright laws, if any, before incorporating them into own Web site.

4.3 INSTALLATION

4.3.1 Network installation and administration

In order to connect to the Internet or setting up an Intranet, one should plan and layout the physical network, which include the following steps:

- Designing topography
- Planning the connectivity or wiring
- Installing routers and hubs
- Setting up servers
- Establishing security measures such as implementation of firewalls
- Selection and connecting to an ISP.

4.3.2 User management

Authentication

Authentication is a process that is performed by the system automatically to ensure that the user is genuine (i.e. really who they claim to be). Authentication may be done at and for a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- **Kerberos V5** : An Internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain.
- **Windows NT LAN Manager (NTLM)** : Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** : Requires certificate servers and is used to authenticate users that are logging onto secure web sites.
- **Smart card** : Contains a chip with information about the user along with the user's private key. A personal identification number (PIN) is normally required for authenticating using a smart card. Requires Extensible Authentication Protocol (EAP) to be enabled for the server to allow smart card authentication. Also some certificate authority must provide keys.

Authentication uses X.509 standard and kerberos.

Process of Logging On

1. As the first step the Ctrl+Alt+Del key combination has been pressed, name and password entered, and local or domain logon is indicated.
2. If the logon is local, the name and password are checked against the local database. If the logon is a domain logon, the name and password are encrypted into a key, and timestamp information is encrypted. This information is sent to the Windows 2000 domain controller with an authentication request.
3. The domain controller decrypts the information and checks for a valid timestamp. If the timestamp is valid, two Kerberos tickets are made and encrypted with the password. The tickets are sent back to the client computer. The tickets are:
 - User session key - Used to log on.
 - User ticket - Used to get other Kerberos tickets for accessing other domain resources.
4. The client decrypts the tickets and uses the session key to log on.

Shares used for logon

NETLOGON/SYSVOL - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

Accounts:

Built in Accounts

The below accounts are created when any Windows 2000 system is installed. These accounts are also created on domain controllers automatically when Active Directory is installed.

Administrator - Cannot be deleted or disabled and should be renamed.

Guest - Disabled by default. A password is not required. This account can't be deleted but can be renamed, and should be disabled.

Account Types

- Local - For local computer access.
- Domain - For access to network resources in the domain.

Administrators and power users can create and modify accounts in the domain. Administrators on local computers can create and modify accounts locally. The Windows Scripting Host (WSH) assists administrators in creating many users and groups quickly.

User Properties

In addition to the usage, it is essential to note the following for smooth operation:

- Username - A unique name up to 20 characters excluding:
“\ [] ; | , + * ? < > \
- The username may be changed after it is created. Choose a naming convention for large organizations.
- Password - Case sensitive and up to 14 characters.
- User must change password at next logon
- User accounts can be renamed.

Account Creation and Modification

- Local account: - Use the “Local Users and Groups” tool.
 1. Right click “My Computer”, select “Manage”.
 2. Click the + next to “Local Users and Groups” in the “Computer Management” box.
 3. Enter user information into the “New User” dialog box.

To modify the user properties, right click on the user and select “Properties”. User Property tabs include:

- General - Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.
- Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. The profile includes desktop settings.
- Member Of - Set up local groups the user is a member of.

- Dial-in (Only on Server computers) - Set remote access permission, callback policy, and IP address and routing information.
- Remote account: - Use the "Active Directory Users and Computers" tool.
 1. From the Active Directory Users and Computers tool click + next to the domain name.
 2. Highlight the "Users" folder and select "Action", "New", and "User".
 3. Enter user information into the "New User" dialog box.

To modify the user properties, right click on the user and select "Properties". User Property tabs include:

- General - Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.
- Address - Set mail address or physical address information.
- Account - Set hours that the user can logon during and restrict computers the user can use. The following operations are possible:
 - User must change password at next login
 - User cannot change password
 - Password never expires
 - Store password using reversible encryption.
 - Account is disabled
 - Smart card is required for interactive logon
 - Account is trusted for delegation - The user can delegate authority for their privileges or rights to other users.
 - Account is sensitive and cannot be delegated.
 - Use DES encryption types for this account.
 - Do not require Kerberos preauthentication - For systems supporting Kerberos but not preauthorization.
 - Indication of account lockout is here.
 - Can set when account expires.
- Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. A logon script file can be set. Domain user logon scripts are in the NETLOGON share on the domain controller in the SystemRoot\SYSTEM32\sysvol\domainname\SCRIPTS folder. The profile includes desktop settings. Default profile file location is C:\Documents and Settings\username on the computer that the user logged on to.
- Other aspects such as Telephones, mobile, fax phone numbers, etc. and about the organization consisting of the user title, department, manager, and company could be entered.
- Member Of - Used to assign users to groups and remove users from groups.
- Dial-in - Dial-in privileges can be granted or denied and callback options are set here.
- Published Certificates - Can add or remove user internet certificates.
- Object - View information about the user account object such as when the account was modified last.

- Security - Can set users and groups that can modify this domain user account properties.

The "NET USER" command line tool may be used to create users when used with a batch file.

Permissions

The permissions on Windows 2000 systems are all selectable with two boxes, which are:

- Allow - Grant the permission.
- Deny - Any denied permission for a group or user will override any allow permission, even if the user is in a group that is granted that permission.

If neither box is checked, the permission is not granted for the user or group, but if the user is in another group that has the permission, it will not be denied. Normally, if a user is a member of several groups that have different levels of permissions to an object, the least restrictive permissions apply unless the user, or one of their groups have the no access box checked for that permission.

Standard File and Folder Permissions

- Read(R) - View attributes, contents, and permissions. Can synchronize.
- Write(W) - Can change attributes, and file contents. Can create files or folders. Can synchronize.
- Read(R) and Execute(E) - Can change sub folders, perform read operations, and execute a file.
- List Folder Contents - Can perform read and execute permissions on folders. Can view folder contents, attributes, and permissions. Can synchronize and change to subfolders.
- Modify - Perform Read, Execute, and Write permissions along with ability to delete.
- Full Control - Can perform Modify functions (above), take ownership, and modify permissions.

Permissions assigned to directories are inherited (default) by all files and subdirectories that are contained in the directory. The inheritance option, selected by default, may be deselected. Each file or directory has an Access Control List (ACL). To set permissions for additional users or groups, they are added to the ACL of the file or directory. Windows Explorer can be used to set permissions.

NTFS File and Share Permissions

When these permissions are different, the most restrictive permissions are applied. The share and NTFS file permissions must overlap in order for the user to have the permission. That means to read a file, the user must have both read share and read NTFS permission.

When a user has full control permission for a folder, the permissions will apply to the files in the folder even though permission for an individual file in the folder may be set to NO ACCESS for that user. When a file or folder is moved, it retains its current permissions, but when it is copied, it inherits the permission of the parent folder or partition it is being copied to.

Ownership

If the owner's user is a member of the administrators group, the owner is the administrators group. Administrators do not have access to all resources, but they may take ownership of any resource. Once ownership is taken, it cannot be given back. Also taking ownership of resources changes all existing permissions for that resource.

Delegated Permissions

Permissions that can be delegated include:

- Create, delete, and manage user groups.
- Create, delete, and manage user accounts.
- Manage group policy links - Group policies assigned by organizational unit may be modified.
- Modify group membership.
- Read all user information.
- Read user account passwords.

Setting Permissions

1. Right click on the file or folder.
2. Select properties
3. Select the security tab on the properties sheet.
4. Click on the permissions button.
5. If the file selected is a subdirectory there are the following check box choices:
 - Replace permissions on subdirectories - Permission changes are applied to all sub folders.
 - Replace permissions on existing files - Permissions are applied to all files in the folder. If both are selected, permissions are applied to all sub folders and files in all files in the folder and its sub folders.
6. Click on OK to exit the permissions box and OK to exit the properties box.

4.3.3 Disk Quotas

Disk quotas are used to track the use of disk space for each user. They are normally disabled and are only supported on NTFS file systems. Quotas are tracked per partition and per user using ownership information to account for resource use. Compressed file sizes are measured according to the uncompressed file size.

Disk quotas may be viewed and administered by using the "Disk Management" tool to select the properties dialog box of the disk or volume. The "Quota" tab contains quota information and management functions. Quota management must be enabled. Warning levels may be set and hard limits may also be set. Disk space may be denied to users who exceed their quota limit. The events may be logged when the user exceeds their warning and/or quota limit.

Windows Explorer can be used to setup and monitor disk quotas. Windows Explorer local disk properties tabs:

- General
- Tools
- Hardware
- Sharing
- Security
- Quota - Used to enable quota management, deny disk space if the quota is exceeded, limit the disk space and set where the disk quota warning is given.

The user can also log when the warning level or quota level has been exceeded. The "Quota Entries" selection box is used to view quota utilization for the volume. To modify the quota levels for any given user, double click the user's entry.

- Web Sharing

User Rights

User rights are different from access permissions, which allow access to resources such as, read, write or execute access. User rights allow system control, which includes the ability to format, a hard drive or shut the system down.

Local Users created at installation time

1. Administrators - Used to administer the system. Making a backup of the administrator user would be highly useful during critical situations.
2. Guests - Have minimal privileges. It can be renamed, but cannot be deleted. On NT workstation, disable the guest account or give it a password, since it is enabled upon installation.
3. Initial User - Member of administrators group.

Two levels of security

- Logon
- User Rights

Adding Accounts

The "Local Users and Groups" tool is used to create user and group accounts locally and the "Active Directory Users and Computers" tool is used to create users remotely. They are also used to with managed functional user rights, security auditing, and account policies. Functional user rights determine what programs the user can run or what system capabilities they have. Passwords are case sensitive, but user names are not. Both can contain spaces.

Two methods of adding user accounts:

- Creation
- Make a copy of an existing account.

When an account is copied from a template the following fields are left blank:

- Username.
- Full Name
- Password and confirm password
- User cannot change password
- Account disabled.

User accounts should not be made local on various workstations when using domain user accounts. If a user account is deleted, when it is recreated, even though it may have the same name, it will have a different user ID number and resource access for that account must be set up again.

Passwords are case sensitive and can be up to 14 characters. User names are not case sensitive and can be up to 20 characters. The user's home directory can be specified when the user is created or set later. The home directory is where data from an application is saved by default and where the command prompt will be when a command line session is begun.

User rights are divided into:

- Logon rights
- User privileges

Setting User Rights

- Organizational Units - In Administrative Tools, select "Active Directory Users and Computers".
- Domain - In Administrative Tools, select "Domain Security Policy". The ADMINPAK must be installed on the computer.
- Domain controllers - In Administrative Tools, select "Domain Controller Security Policy". The ADMINPAK must be installed on the computer.
- Local computers - From the Control Panel, "Administrative Tools" applet, double click "Local Security Policy".

Domain controllers do not have a power users group. On the Domain Controllers, Server Operators are similar to the Administrator group on the Workstation with all rights.

4.3.4 Security Configuration and Analysis

The "Security Configuration and Analysis" tool is used to analyze a computer security configuration. To get ready to use this tool, do the following:

- The MMC "Security Templates" snap-in must be previously installed. Once installed, it is the administrative tool called "Security Console".
- The MMC "Security Configuration and Analysis" snap-in must be installed to the "Security Console" by starting it from "Administrative Tools", selecting "Console" and "Add/Remove snap-in".
- A database in the snap-in must be created by selecting "Administrative Tools", "Security Console", select "Action", and "Open database".
- To perform the analysis against a template, open a database, and then select "Action", and "Analyze Computer Now".
- To apply settings from a template, open a database that has the settings user intend to apply to the computer, then select "Action", and "Configure Computer Now".

User Profiles

The user's profile allows the user's environment to be configured. The User Manager administration tool allows user profiles to be modified when "user properties", then "profile" are selected. The user profile contains:

- Desktop settings - screen colours, wallpaper, screen saver
- Persistent network and printer connections
- Mouse settings and cursor settings
- Recently edited documents.
- Start-up programs, shortcuts, and personal groups
- Settings for Windows applications - Notepad, Paint, Windows Explorer, Calculator, Clock, and more.
- Start menu settings - Programs that can be selected from the start menu.

The user profile settings are saved on disk. They are loaded when the user logs on. There are two profile types:

- **Local profile** : Stored in the C:\Documents and Settings\username folder. The profiles file is NTUSER.DAT in the directory called by the user's name. A mandatory profile which discards any changes the user makes to their profile at logoff time, can be implemented by modifying the name of the user profile file from NTUSER.DAT to NTUSER.MAN. The ntuser.ini file is used to set up the user roaming profile components that are not copied to the server. The ntuser.dat, LOG file is used for NTUSER.DAT file recovery in the case of an error. Additional folders in the C:\Documents and Settings\username folder are:
 - **Application Data**: Refers to data used by application programs that the user may modify when they change a setting in the application.
 - **Cookies**
 - **Desktop** - Refers to desktop and briefcase shortcuts.
 - **Favourites** - Application favourites such as web site favourites on IE and favourite programs.
 - **FrontPageTempdir** - Only on Windows 2000 Servers for files made by Microsoft FrontPage.
 - **Local Settings** - Settings used by applications such as IE.
 - **My Documents**.
 - **NetHood** - Network servers or shared network folder shortcuts.
 - **PrintHood** - Network printers.
 - **Recent** - Shortcuts to documents recently used.
 - **SendTo** - Shortcuts to places where files are copied.
 - **Start Menu** - The user's start menu and shortcuts.
 - **Templates** - Application templates.
 - **Roaming** - Stored on an NT server and downloaded to the computer that the user logs onto. This way the same user's profile can be available on any machine.

Profile Creation

- **For local users** : If no user profile exists when the user logs on, the contents of the Default User profile folder are copied to the C:\Documents and Settings\username folder.
- **For domain users** : The NETLOGON share on the domain controller is checked for a default user profile. If one does not exist, it copies the contents of the local Default User profile folder to the local computer NETLOGON\username directory.

The default user settings are used to create a new user's profile when the new user logs on the first time. The administrator may modify the contents of the Default User profile directory to change the settings for first time users of the system. The Control Panel, System applet is used to copy user profiles. The "User Profiles" tab is used. The System applet is also used to delete user profiles. Shortcuts may be added to the Default User profile directory using Windows Explorer.

All Users Profile

Administrators may install applications and place shortcuts in the All Users Profile directory. All users will have access to these shortcuts and applications. These applications appear on users' desktops. The All Users Profile is not available on a main wide basis.

1. Using a text editor, open the start file, which is located in `server_root/https-server_identifier`.
2. In the 10th line counting from the top of the script, insert the following: `echo "SSL-enabled_server_password"`

For example, the edited line might look like this:

```
echo "MBi12!mo"}.${PRODUCT_BIN} -d $PRODUCT_SUBDIR/config $@
```

Restarting with inittab

To restart the server using inittab, put the following text on one line in the `/etc/inittab` file:

The `-i` option prevents the server from putting itself in a background process.
`http:2:respawn:server_root/type-identifier/start -i`

Replace `server_root` with the directory where the server has been installed, and replace `type-identifier` with the server's directory.

It is required to remove this line before stopping the server.

4.3.7 Tuning server performance

Server's technical options can be configured, including the number of maximum simultaneous requests, listen-queue size, and DNS usage.

Configuring maximum simultaneous requests

Number of maximum simultaneous requests can be set, which is the number of active requests allowed for the server at one time. However, for general purpose internet or intranet use, one probably will not need to change the default value (128 requests).

To get the number of simultaneous requests, the server counts the number of active requests, adding 1 to the number when a new request arrives, subtracting 1 when it finishes the request. When a new request arrives, the server checks to see if it is already processing the maximum number of requests. If it has reached the limit, it defers processing new requests until the number of active request drops below the maximum amount.

In theory, one could set the maximum simultaneous requests to 1 and still have a functional server. Setting this value to 1 would mean that the server could only handle one request at a time, but since HTTP requests generally have a very short duration (response time can be as low as 5 milliseconds), processing one request at a time would still allow to process up to 200 requests per second.

If it is required to change the number of maximum simultaneous requests, set the number before starting the server. To reset the number:

1. Choose Server Preferences|Performance Tuning.
2. Type the number of requests.
3. Click OK.
4. Click Save and Apply.

Enabling Domain Name System lookups.

The server can be configured to use Domain Name System (DNS) lookups during normal operation. By default, DNS is not enabled, if DNS is enabled, the server looks up the host name for a system's IP address. Although DNS lookups can be useful for server administrators when looking at logs, they can impact performance. When the server receives a request from a client, the client's IP address is included in the request. If DNS is enabled, the server must look up the hostname for the IP address for every client making a request.

Configuring listen-queue size

The listen-queue size is a socket-level parameter that specifies the number of incoming connections the system will accept for that socket. The default setting is 128 incoming connections.

To manage a heavily used web site, one should make sure that system's listen-queue size is large enough to accommodate the listen-queue size setting from the Server Manager form. Before changing the listen-queue size, make sure that system supports the new size. The listen-queue size set from the Server Manager form changes the listen-queue size requested by the server.

Configuring the HTTP persistent connection timeout

With HTTP 1.1, a connection can be set to be persistent (similar to keep alive in HTTP 1.0). However, even if a connection is persistent, it still needs to have a timeout setting, otherwise it may consume system resources.

If it is needed to change the setting:

1. From the Server Manager, choose Server Preferences|Performance Tuning.
2. Enter a number in seconds in the HTTP Persistent Connection Timeout field.
3. Click OK and finally, save and apply the changes made.

Configuring MIME types

MIME (Multi-purpose Internet Mail Extension) types control what types of multimedia files the mail system supports. One can also use MIME types to specify what file extensions belong to certain server file types, for example to designate what files are CGI programs.

1. Choose Server Preferences|Mime Types.
2. Select the category and enter the content type and file suffix.
3. Click New Type.

To edit a MIME type:

1. Click Edit next to the type user want to edit.
2. Change the category, content type, and file suffix as needed.
3. Click Change MIME Type to update.

To remove a MIME type, click Remove next to the type to removed.

4.3.8 Configuring network settings

Server's network settings can be changed using the Server Manager.

Changing the server's location: To change the server's location

1. Choose Server Preferences|Network Settings.
2. Type the pathname of the server's new location.
3. Click OK and finally, click Save and Apply for changes to take effect.

Changing the server's user account

The server user specifies a Unix user account that the server uses. All the server's processes run as this user. There is no need to specify a server user if one chose a port number greater than 1024 and are not running as the root user (in this case, one don't need to be logged on as root to start the server). If user account is not specified here, the server runs with the user account that starts it with. Make sure that when server starts, the correct user account is used.

To change the server's user account:

1. Choose Server Preferences|Network Preferences.
2. Type the new server user account.
3. Click OK and finally, click Save and Apply for changes to take effect.

Changing the server name

The server name is the full hostname of the server machine. When clients access the server, they use this name. The format for the server name is `machinename.yourdomain.domain`. For example, if the full domain name is `netscape.com`, a server with the name `www.netscape.com` can be installed.

If the system administrator has set up a DNS alias for the server, use that alias on the Network Preferences form. If not, use the machine's name combined with the domain name to construct the full hostname.

Changing the server port number

On the Network Preferences form, the Server Port Number specifies the TCP port that the server listens. The port number chosen can affect the users—if a nonstandard port is used, then anyone accessing the server must specify a server name and port number in the URL. For example, if port 8090 is used, the user would specify something like this URL:

`http://mydomain.com/:8090/abc/xyz.htm`

If it is not sure that if the port number to use is available, look at the `/etc/services` file on the server machine. Port numbers for the most commonly used network-accessible services are maintained in the file `/etc/services`.

The standard unsecured web server port number is 80; the standard secure web server port number is 443. Technically, the port number can be any port from 1 to 65535.

Changing the server binding address

At times it is required that the server machine to answer to two URLs. For example, to answer both `http://www.netscape.com/` and `http://www.mozilla.com/` from one machine.

If the system is set up to listening to multiple IP addresses and want to use this feature, on the Network Preferences form use the Bind To Address field to tell the server which IP address is associated with this hostname.

Changing the server's MTA host

To change the MTA (Message Transfer Agent) host, use the MTA Host field on the Network Preferences form to change the name of the SMTP mail server. One must enter a valid MTA host to use the agent email function.

Changing the server's NNTP host

To change the NNTP (Network News Transfer Protocol) host, use the NNTP Host field to change the name of the news server. A valid NNTP host must be entered to use agents with the capability to post to news.

Customizing error responses

To specify a custom error response that sends a detailed message to clients when they encounter errors from the server. One can specify a file to send or a CGI program to run.

Instead of sending back the default response file on encountering error, one might want to send a custom error response instead.

What are the errors?

Response to several different kinds of errors can be customised:

- **Unauthorized** : This error occurs when users without access permissions try to access a document on the server that is protected by access control. One might send information on how they can get access.
- **Forbidden** : This error occurs when the server does not have file system permissions to read something, or if the server is not permitted to follow symbolic links.
- **Not Found** : This error occurs when the server can't find a document or when it has been instructed to deny the existence of a document.
- **Server Error** : This error occurs when the server is not configured properly or when a catastrophic error occurs, such as the system running out of memory or producing a core dump.

Setting up the response

Before setting up the response, one need to write the HTML file to send or create the CGI program to run. After this, set the response by doing the following:

1. From the Server Manager, choose Server Preferences|Error Responses.
2. From the Resource Picker, choose the server resource intended to be configured.
3. Select the error response wanted to be customized.
4. Type the absolute pathname to the file or CGI script that will return for that error code. Check the CGI box if the file is a CGI program that is intended to run. Repeat this process for each of the error responses to be customized.
5. Click OK and finally, click Save and Apply to confirm changes.

To remove a customization, return to the form and delete the filename from the text box next to the error code.

4.4 NETWORKS AND SECURITY

A network, whether it is a small home office network or a 5000 node LAN/WAN, securing it should be a top priority. From the smallest to the largest network steps should be taken to make sure that it is secure from attack or theft. How to protect the integrity of network information can be handled aggressively or casually depending upon what one have and how much one need to protect. For doing a good job there are specific steps that one should take and in a specific order. Bear in mind that not all steps are necessary for all network situations. Like any major project to be undertaken, one should start with a plan, and a good plan starts with an outline. Below is a sample outline of the process of securing the network.

- Risk Assessment
- Vulnerability
- Budget Analysis
- Security Policy
- Implementation
- Auditing

SQLBase 7 offers five connectivity interfaces for linking client applications with SQLBase databases. One can choose the connectivity interface that best suits the needs based on the development tool/language users are using and application requirements:

- SQL/API is a low level, high performance interface suited for use with C and languages that support external functions in DLLs. It provides complete access to the SQLBase feature set, including "administrative" operations.
- SAL is the 4GL scripting language used in Gupta's development environments for coding business logic.
- SQLBase++ is an object oriented "wrapper" around the SQL/API for use with C++ Applications.
- The SQLBase JDBC driver provides a native interface for Java applications and applets.
- The SQLBase ODBC driver provides a simple and portable interface via ODBC. SQLBase 7 fully supports multi-threaded ODBC applications. It is also fully compatible with the older ODBC 2.0 API.

4.5 TUNING APPLICATIONS OVER INTRANET

SQL/API

"The Structured Query Language/Application Programming Interface (SQL/API) is a function library designed for use with the C programming language, and development environments that support C-style external function calling conventions. SQL/API is a call level interface (CLI) analogous to SQL*Net in Oracle environments and CT-LIB in Sybase environments.

One can make calls to SQL/API functions throughout the application to interact with SQLBase. Typical function calls include connecting and disconnecting to a database, passing SQL statements to the server for compilation and execution, providing bind variable data, and retrieving result sets.

Additionally, the SQL/API provides functions to perform administrative tasks such as performing database backups and restorations.

ODBC

Not just an ODBC driver, Recital ODBC Developer provides a complete industry standard ODBC database solution for Unix, Linux, or OpenVMS. Consisting of an ODBC driver, and an Application Server, which has a complete SQL-92 database engine, Recital ODBC Developer can create, query and update Recital databases from Windows applications. If Recital applications are running on Unix, Linux, or OpenVMS, one can provide full read and update access to the databases from Microsoft Windows clients with Recital ODBC Developer. Using Recital ODBC Developer one can use industry standard management reporting tools such as Crystal Reports to generate high quality reports against live data in a Recital based application.

JDBC

Not just a JDBC driver, Recital JDBC Developer provides a complete industry standard JDBC database solution, consisting of an all-Java type 3 driver, and an Application Server that implements a complete SQL-92 database engine. With JDBC Developer, Java applications can query and update data from any data source across Intranets or the Internet.

Check Your Progress

- 1) The first step of setting up intranet is to configure a _____
- 2) An Internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain is _____
- 3) SQLBase 7 fully supports _____ ODBC.
- 4) SQL/API is a call level interface (CLI) analogous to _____ in Sybase environments.
- 5) _____ types control what types of multimedia files the mail system supports.

4.6 SUMMARY

In the world where communication is key to business process, every one wants to make use of Intranet technology for business success. While setting up intranet are should be taken to prevent undesired flow of secret business information the competitors.

It is to be always remembered that foundation of network depends on the technology that is used to set up the intranet and the security features that are available with it. The role of a network administrator/intranet administrator is thus very important. One should judiciously decide who should and should not be allowed certain privileges, which can pose threat to the network.

Finally, it is desirable for the company to have proper security policy to curb network security lapses.

4.7 MODEL ANSWERS

- 1) Web server
- 2) Kerberos V5
- 3) Multi-threaded
- 4) CT-LIB
- 5) Multi-Purpose Internet Mail Extension

4.8 FURTHER READINGS

- 1) *Empowering Intranets to implement Strategy. Build Teamwork and Manage Change* by D.Keith Denton, Praeger Publishers.
- 2) *Intranet's Decisions : Creating your organization's internal network* by Lisa Kimball, Miles River Press.
- 3) *Internet and Intranet Security Management : Risks and Solutions* by Lech Janczewski, Idea Group Publishing.

Reference Websites

- 1) <http://petra.austinc.edu/>
- 2) <http://javacorporate.com/>
- 3) <http://www.tech-noel.com/>
- 4) <http://www.netscape.com/>

UNIT 5 INTRANET AUTHORIZING AND MANAGEMENT TOOLS

Structure

- 5.0 Introduction
- 5.1 Objectives
- 5.2 Intranet Authoring Tools
 - 5.2.1 Editors
 - 5.2.2 Supporting applications for services like FTP, Telnet, etc.
 - 5.2.3 Graphical tools for creating, animating, etc.
- 5.3 Intranet Management Tools
 - 5.3.1 Databases - basic, ODBC, distributed
 - 5.3.2 Web Servers
 - 5.3.3 Other tools
- 5.4 Summary
- 5.5 Model Answers
- 5.6 Further Readings

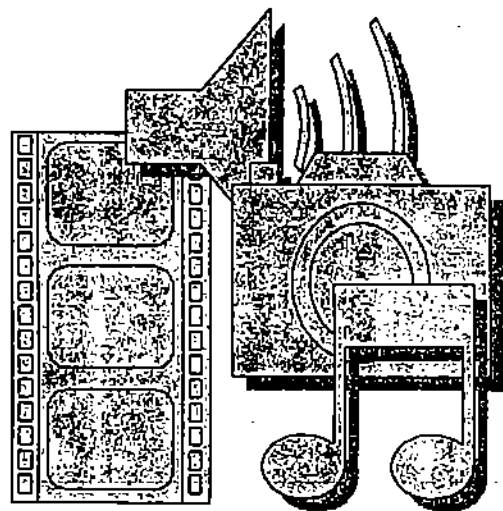
5.0 INTRODUCTION

The success behind the intranet or Internet is the authoring and management tools. On one side, they provide opportunity for higher productivity and on the other hand, the tools give tremendous manageability. It is needless to mention that good powerful tools improve the management of tasks as well as make the processes fast and organized. Another hidden aspect is that use of tools make the processes more and more computer processing intensive thereby leaving the users to put their else for other tasks.

An activity as simple as web page designing could be many times more complex and tedious than preparing similar output using a general word processor. Many software developers have extended the features of general application software used in day-to-day activities by adding up a number of features. Many have properly analyzed the requirements of the developers and tried to give a proper organized shape to them.

With the advancement in the object oriented technologies and the software engineering concepts, the software developers are seeing all application software as tools for achieving higher goals. Earlier this was not the concept and every piece of software developed was considered a masterpiece in themselves. But as the time passed, it was found that adoption of advanced concepts such as OO techniques and OO based software engineering, it had become possible to visualize and realize essential features required in different software (thereby making them complete).

There were days when designing and management of just 10 web pages for a corporate was viewed as a major project and a task such as changing the reference to a web page in all web pages could consume almost half a day.



Whereas these days life of designers and developers has become very easy due to the sophisticated and elegant tools, more than 20000 pages can be handled with few mouse clicks and tasks such as changing web page reference can be as easy as a child's play.

The impact of the tools has been so strong on the computing line that a number of new employment opportunities evolved in no time. There has been great demand for graphic designers, animators, publishers, creative artists, information or content specialists, and many more. Needless to mention that due to the impact, an era of dotcom companies came for about a decade before the dotcom culture burst off. The use is still functioning due to certain major players in the industry such as companies running search engines, newspaper, massive portals, etc.

5.1 OBJECTIVES

This unit contains information on various authoring as well as management tools available in the market for intranet. These are the tools that help in improving the look and feel of the information to be hosted on the Intranet and can be used for Internet also. Tools with lots of features are available which can improve the productivity of the professionals as well.

Details about web page editors, general services tools, graphical tools, etc. as well as database connectivity and higher tools have been discussed in this unit.

The details of each tool has been given wherever possible, however, it is expected that as an exercise, the students should endeavour to identify various features that should be provided by the developer in the given categories of tools. This is very important in view of standardization of the tools as well as study of tools in academic interest.

5.2 INTRANET AUTHORIZING TOOLS

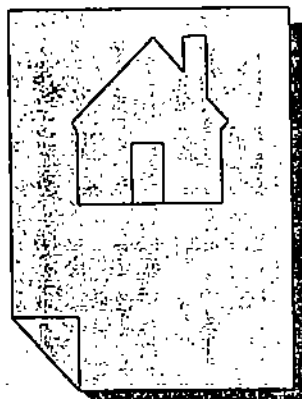
With the active involvement of major developers such as Microsoft, Netscape, Macromedia, Adobe, Trellix, Sun, etc., there are a number of tools ranging from small applications such as image animation up to powerful email response handling applications available to everyone. Most of them are even free on the web and those available commercially can be obtained at reasonably low cost.

5.2.1 Editors

In the yesteryears, not very far but just about 5 years ago, the web page developers used a standard text editor or basic Word Processor, such as notepad, to create HTML file. This involved very laborious activities such as coding everything by hand and then saving the HTML pages as text files. Then finally test the output offline using browsers like the Netscape or Internet Explorer. Not many tools were available for carrying out petty activities such as animation, placement or presentation of material, elegant user interface, etc.

It was essential to know almost all the HTML tags and take care of every tag and parameter of the HTML syntax. This need has led to invention or development of appropriate tools to take care of relevant activities. These tools are being updated very quickly to suit to the requirements of various newly added features, integration with other tools as well as to allow cross-platform functionality.

Today, there is no need to remember all the HTML tags and their parameters. Interestingly, there are a number of versions and variations of HTML



available that makes it much more complicated to remember the features and variations.

All that is needed is to obtain the tool, install it, practice a little and then straightaway start working on it. Many better and convenient ways are now available with the availability of software tools for web authoring such as the following:

- Adobe Page Mill
- Microsoft FrontPage
- Netscape Web Tools
- Macromedia Dreamweaver Ultradev
- Trellix Authoring Tool
- Chili! ASP (Active Server Pages from Sun for UNIX)
- Claris Homepage
- GlobalX CORE System
- Revize
- SmartTable (converts spreadsheets into Java applets)
- Web Wizards (create and edit MS Office documents through a web browser).

While the above tools are very popular, this is not the end. Though there a number of editors are available, it is felt worthful to make a little note on these tools that they offer flexibility and manageability that are very new and highly creative.

All efforts have been made to bring out most of the features that are both essential as well as desirable for all editor tools to offer.

Features editor tools should provide for

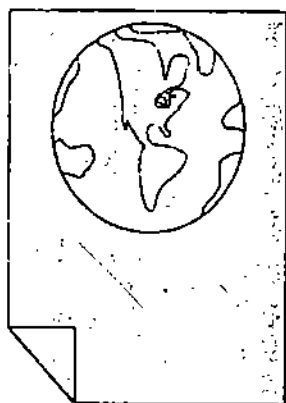
1. **Autocoding:** The tool should provide for automatic coding in the background when the developer assembles the objects on the web page, thereby relieving the developer of remembering the HTML code. When the editor itself inserts the basic framework of actual code on which the developer can add the required features, it becomes quite obvious that the time and efforts of developers reduce by many times. Moreover, the chances of committing errors also reduce substantially.
2. **Modifying the code:** The developer should be free to change or modify a portion of the code or change certain setting through HTML coding, but the corresponding output has to be properly affected by the editor.
3. **Object library:** There are many editors that are more than just editors as they perform the tasks of debugger as well as code generator by use of concepts like the object libraries. Such software tools are considered intelligent and are highly reliable. They also guide the developer on-line during any syntax mistakes.
4. **WYSIWYG kind of output:** The software tool should generate output exactly as designed and laid out by the developers. If the developer designs the page in a particular format, it is essential for the editor to prove coding in a manner to generate the same output.
5. **Compatibility with other server architectures:** The editor should support powerful web server such as Apache, iPlanet or Zeus web servers.
6. **Compatibility with other platforms:** The editors should produce output acceptable to all platforms such as Unix, Solaris, Windows, Linux, HP-UX, AIX, Sun Cobalt, etc.

7. **Less memory usage:** The tools should not consume all the memory space and swap area for want of enormous amount of memory for storing images, texts, links and other parameters.
8. **Preview of the output:** This feature proves to be of great use to the developers since the need to switch over to other browsers to the affect of every small change would consume memory space, time and efforts. Almost all editors are providing this feature.
9. **ActiveX Data Object Support:** New properties and methods to provide a tighter integration with the editor tools should be provided. Popular Web authoring tools (e.g., Macromedia's Dreamweaver UltraDev, Adobe GoLive!) give this support.
10. **Java support:** The editor tool should provide for support to use of Java technologies such as JavaScript, Java Beans, Applets, etc.
11. **Acceptability of variants:** Though this aspect purely depends on the changing market trends, it is desirable that the editor should be able to accept coding specific to variants of the HTML such as DHTML, XML, SGML, VRML, WML, etc. and be capable to generate output in these formats whenever felt necessary.
12. **Site map:** A proper view or estimate of how the web site is organized and how massive it is makes the web site more attractive. Editors should provide a broad view of the web in the form of an GIF or JPG image whereas some even provide this as a web page.
13. **Simple and elegant user interface:** The use of various objects such as colours, background, textures, buttons, banners, etc. make the web pages look more beautiful. The editors should support such things and the product would be readily accepted if it contains features related to handling of graphical representations nearer to photo-realistic nature.
14. **Compatibility to popular word processing, spreadsheet and presentation software:** It has become common now-a-days that most features of a web page editor are integrated directly into the word processors since the features of both are not much different. In addition to this, it should also be possible to publish the work done using spreadsheet or presentation software on to the web site as well as use the existing pages to load and accordingly process using these software.
15. **Clipart support:** Most editors come with a huge gallery of clipart and some even provide a collection of sounds, music and multimedia clips. Though, this is optional, it is desirable to provide one such library to enable the developers to use ready available objects.
16. **Audio support:** The editors should provide for playback of audio files of various formats.
17. **Multimedia capabilities:** The editors should also give the option of playing multimedia files so that the web site gives a much better look and feel.
18. **Extension of support to various file formats:** As it is known that there are hundreds of file formats available, the editors must give the support of a majority of the file formats. There are different sets of formats for images, audio, video, multimedia, text, support files, fonts, compressed files and many more.
19. **Powerful search and replace facility:** The editors should be smart enough to locate for a particular word or phrase in the entire web site on click of the mouse button.

20. **Managing different peripheral devices:** Devices such as web camera, scanner, light pen, etc. can be handled directly through the editor for better flexibility.

5.2.2 Supporting applications for services like FTP, Telnet, etc.

There are a number of tasks identified for hosting applications on the web. After the designing tasks are over, the next important activity would be to host on the server, and to carry out this task, it is essential that the developer is aware of the developments in this line. There is a huge range of software available for communication and file transfers between the developers/computers and the web servers.



This issue could be as simple as clicking the mouse to transfer thousands of files and it could be as difficult as using a set of programs to execute and test the developed software. It may also be possible that the developer may have to use character user interface (CUI) many times.

The developer must also know what are all the possible activities that can be performed and what objective would be achieved by use of particular service. In addition, it must also be known what additional features would be covered under that particular service and what software are available to carry out this task easily.

Take for instance, a service like the file transfer. It is possible to carry out using software designed for Unix, DOS, Windows and other platforms. They are offered to work through different user interfaces such as CUI, GUI, etc. Those offered through the GUI technology are much popular and provide the easiest way to transfer files across the intranets and Internet connecting to an FTP site in seconds, even if the user is a beginner. Whether publishing a Web page, downloading the images, software and music or transferring high-capacity files between branch offices, such software provides the flexibility users need to make the tasks more enjoyable and productive.

It may be noted that there are a variety of tasks such as FTP, Telnet, Gopher, etc. that the users want to use without knowing much about the software tool they would be using and the underlying technologies. Users as well as the developers would like to look out for better user interface while hiding the supporting details and technologies.

The actual details of the protocol services would be dealt with in the next unit, but for now it is sufficient to remember that telnet clients are part of the larger category of terminal based applications such as FTP, Gopher, etc., and are programs designed to allow one computer to emulate another type of computer. It gives a feel as if the user is actually working as a part of a big network group situated geographically distant from his place and that too may be on a separate platform. Some of the popular software for telnet are as follows:

- **NetTerm:** One of the best telnet clients available — features remote host file editing.
- **HyperTerminal:** A must-have free upgrade for the standard Windows HyperTerminal client.
- **CRT - Combined Rlogin and Telnet:** one of the best terminal apps on the net.
- **SecureCRT:** CRT with SSH2 (Secure Shell) support and RSA authentication.
- **CommNet :** One of the better telnet clients available — features Zmodem support.
- **QVT/Term:** The standalone terminal client found in the QVT/Net Internet suite.

- **Anzio Lite:** A solid terminal emulator with extensive connectivity options.
- **EWAN:** A good Emulator Without A good Name.
- **Kermit:** Kermit and a whole lot more for Windows 95/98/NT/2000 users.

The features considered essential and relate to most of the services that the supporting software tools should provide are given as follows:

Features common to all

1. **Simple Drag 'n' Drop based Instructions:** The tools developed in recent times offer this feature and it will here to stay. One should look for this service if easy transfer of files, less command based interface, etc. are desired.
2. **Extensive host type support:** The software should offer full support for various host types that the user can choose from, which may include VMS, MVS, NT, OS2, AS400, Novell, Chameleon, and VM/ESA.
3. **Quick connect URL:** Some software have icons and simple text entry boxes for easy connectivity so that FTP URLs, usernames and passwords, etc. can be entered and directly connected into the server just like a browser.
4. **Macro record/playback scripting:** Automation has never been so easy with software offering recording of macro scripts. Clicking the record button, performing the tasks required and then storing the performed actions as a macro can record a group of activities or commands. These macros can be used time and again so that the entire group of actions need not be repeated again and again.
5. **Dial-up networking support:** The ISP should be automatically dialed as soon as attempt is made to connect to a remote site and still further the ISP should also be automatically reconnected after if the connection with ISP is lost due to certain reasons.
6. **Right-click shell integration:** Should allow performing a range of activities by just right-clicking anywhere and selecting from the choices given. The intention is that the users have to know little about the complexities of the program and gives the minimum input to the process. If required, it should also lead to the shell execution of the platform.
7. **Record sessions log:** The details of the logging should preferably be recorded at some place to a file so that the details can be updated daily, weekly or monthly.
8. **Force upper/lower/preserve file case:** Most software can be forced to transact with files in lower, upper or preserved case.
9. **Auto-renaming of file extensions:** Though most of the platforms do not support this, it is desirable that the users should be relieved of the job of knowing the file extensions and types. Renaming of a file extension should be done automatically during upload or download or any other process.
10. **Change file attributes (such as chmod):** Bringing up a GUI for easy manipulation of file attributes would be highly useful for every user.
11. **Wildcard macro support:** Transacting activities through macro scripts that are masked with wildcards.
12. **URL parsing/pasting:** The laborious task of parsing URLs should be automatic whereas pasting/copying URLs from the clipboard to the software for automatic connection to a site could be boon to the users.
13. **Support for relevant international standard:** It is essential that the software should function based on the established international standard in order to provide proper compatibility to all other platforms, formats and architectures.

14. **Book-marking of remote directories and sites:** Ability to store the addresses of sites and location of directories of remote sites should be essential so that the user do not have to remember hundreds of sites for information. Once selected, the software should automatically lead the user to a specified directory when connected through FTP or telnet or otherwise.

Exclusive for FTP service

15. **Simple Drag 'n' Drop file transfers:** The tools developed in recent times offer this feature and it will here to stay. One should look for this service if easy transfer of files is desired. Note that it is an essential feature for all the FTP software.
16. **Transfer queue and file transfer scheduling:** Selection of multiple files from various folders or directories as well as sites, and queuing them for transferring later sometime should be possible. Queued transactions should be open for being edited, saved, and scheduled for later recurring file transfers.
17. **Caching of directories on remote servers:** During a FTP session, one of the most time consuming task is updating the directory display after almost every process. This could be simplified by means of proper caching or storing and processing at the users' end.
18. **Resume upload and download:** If the files could not be downloaded due to any reason, the software should be smart enough to resume downloading or uploading immediately once the connectivity has been established. This could save tremendous efforts and precious time.
19. **File finder feature:** When it is required to search a massive site for simple information, the software should be capable to search the site for files using multiple search engines or similar strategy.
20. **Site to site transfers:** Sometimes it becomes essential to transfer files from remote server to another remote server very quickly. During such a situation, the software should be intelligent enough to keep minimal processing at its end and ensure success.
21. **Directory Comparison:** Local and remote directory contents can be compared based on case, name, date, or size. Files that are different from each other can be highlighted and selected for directory wide changes.
22. **Directory upload and download:** Some software allows the user to upload and download entire directory tree structures to and from the remote server.

Exclusive for security

23. **Site security:** The software should allow the developer or user to protect the entire site using combination of username and password pairs or any other security method. Whenever required, it should be able to generate reports about the type of user logged into and other details such as the users address, platform used, date and time of logging, files or information requested, etc.
24. **Extensive firewall support:** It is the responsibility of the software to handle proper firewall security to keep the site secure. It is desirable that the depth of firewall implementation should be considerable. The software should be easily configurable and manageable.

Exclusive for Telnet

25. **File filters:** The file filters allows the users to specify the type of files in the local window. In short, the software should ensure that the commands are easily provided through single interface and provides excellent manageability. For example, if the user specifies that only .doc files are needed to be displayed, then other unwanted types are suppressed allowing easy operation on those files.

5.2.3 Graphical tools for creating, animating, etc.

There are a variety of tools available on the web such as Adobe Photoshop, Corel Draw, GIF Animator, etc. to name a few for performing various tasks related to web authoring. The tools could be used for a large range of tasks such as but not limited to—



- Animating, enhancing the images
- Modifying images, text, contents
- Converting file formats
- Touching and finishing images
- Dealing with audio/sound
- Dealing with multimedia effects
- Graphically representing text
- Mapping images and text
- Compression and decompression
- Designing better user interface
- Preparing allied objects for use in the presentation
- Enhancing the content presentation

While some tools offer a combination of above activities, most tools offer these separately. These tools in integrated form can prove to be wonderful use and the applications could be as prestigious as graphic rendering for movies such as Star Wars, Jurassic Park, Matrix, etc.

The cyberspace is as powerful as the print media. Just as the presentation is key mantra in the print media, so also is it in the cyber media. Most of these tools help in enhancing the ultimate design and finally the look and feel of the web pages. With the advent of GUI based tools, the productivity as well as the beauty of presentation have grown manifold, but even then it may take some more time to bring-in a proper synchronization in the cyber media and print media.

The technology and its tools start its function initially from education. With due acknowledgements to the Institute offering a course on use of graphic tools and technology, following methodology of learning has been given; note the extent of tasks that can be accomplished using these tools:

Through the study of technology applications foundations, including technology-related terms, concepts, and data input strategies, students learn to make informed decisions about technologies and their applications. The efficient acquisition of information includes the identification of task requirements; the plan for using search strategies; and the use of technology to access, analyze, and evaluate the acquired information. By using technology as a tool that supports the work of individuals and groups in solving problems, students will select the technology appropriate for the task, synthesize knowledge, create a solution, and evaluate the results. Students communicate information in different formats and to diverse audiences. A variety of technologies will be used.

The student demonstrates knowledge and appropriate use of hardware components, software programs, and their connections. The student is expected to:

- a) demonstrate knowledge and appropriate use of operating systems, software applications, and communication and networking components;
- b) compare, contrast, and appropriately use the various input, processing, output, and primary/secondary storage devices;

- c) make decisions regarding the selection, acquisition, and use of software taking under consideration its quality, appropriateness, effectiveness, and efficiency;
- d) delineate and make necessary adjustments regarding compatibility issues including, but not limited to, digital file formats and cross platform connectivity;
- e) use the vocabulary as it relates to digital graphics and animation software;
- f) distinguish between and correctly use process colour (RGB and CYMK), spot color, and black/white;
- g) identify colour mixing theories and apply these theories to the creation of new colors in the digital format;
- h) compare, contrast, and integrate the basic sound editing principles including the addition of effects and manipulation of wave forms;
- i) distinguish between and use the components of animation software programs including cast, score, stage, and the animation control panel;
- j) select and connect task-appropriate peripherals such as a printer, CD-ROM, digital camera, scanner, or graphics tablet; and
- k) distinguish and use the different animation techniques of path and cell animation.

The student evaluates the acquired electronic information and is expected to evaluate the fundamental concepts of a graphic design including composition and lighting.

The student uses appropriate computer-based productivity tools to create and modify solutions to problems. The student is expected to:

- combine graphics, images, and sound for foundation or enrichment projects;
- integrate the productivity tools including, but not limited to, word processor, database, spreadsheet, telecommunications, draw, paint, and utility programs into the digital graphics;
- use perspective including backgrounds, light, shades/shadows, and scale to capture a focal point and create depth;
- use the basic principles of proportion, balance, variety, emphasis, harmony, symmetry, and unity in type, colour, size, line thickness, shape, and space;
- use repetition of colour, shape, texture, spatial relationships, line thickness, and size to develop organization and strengthen the unity of a product;
- create three-dimensional effects using foreground, middle distance, and background images;
- apply a variety of colour schemes to digital designs including monochromatic, analogous, complementary, primary/secondary triads, cool/warm colors, and split complements;
- use the basic concepts of colour and design theory to work in a bitmapped mode, creating backgrounds, characters, and other case members as needed for the animation;
- use the appropriate scripting language to create an animation or movie;
- read, use, and develop technical documentation;
- edit files using appropriate digital editing tools and established design principles including consistency, repetition, alignment, proximity, ratio of text to white space, image file size, colour muse, font size, type, and style; and
- use a variety of techniques to edit, manipulate, and change sound.

5.3 INTRANET MANAGEMENT TOOLS

Tools other than web or intranet authoring tools fall under the category of web or intranet management tools. They include tools ranging from simple solutions to massive deployment tools.

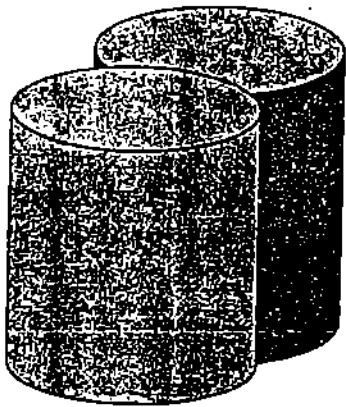
Groupware can be considered as one good solution but not the only suitable solution or tool. Databases, application servers and other software tools for controlling the operations such as tools for discussion forum, emailing, chatting, etc. come under this category.

These tools are sophisticated and require higher expertise to tackle with.

5.3.1 Databases - basic, ODBC, distributed

It has been said that every software that finds proper application must be supported with a database to store the source in the form of raw data. In view of this every programming language has been redesigned to provide connectivity to every other database product available in the market. Embedded coding for use of records has been introduced to operate upon the data through programming languages.

The scope of databases is growing every day. Today, there are hierarchical, relational, network, object-oriented and federated databases available in the market, but very large databases (VLDBs) are yet to make entry. Databases could be installed at one place or can be distributed based on the nature of application. The field of the database world cannot wait any longer for introduction of knowledge bases.



All programming languages either have proper drivers in-built to connect to the databases or need driver software to do so, if the feature has not been provided by the developer.

While purchasing the database or programming language software, do not forget to notice a separate CD-ROM or floppy diskette in the package consisting the required database connectivity driver. It is essential that all the databases should support one another with respect to the method of storage, retrieval, and many other aspects. Even if they differ at every stage,

it is utmost important that all the databases provide method of connecting and converting between different formats or else there is tremendous risk of non-connectivity and isolation from rest of the information world plus in addition there will be huge unnecessary expenditure for installation, maintenance and conversion.

Databases - basic

Almost all the programming languages support databases. Most popular databases are the Oracle, Sybase, DB2, etc. for massive implementations whereas Microsoft Access, SQL Server, etc. are highly popular for standalone personal computers.

Visual Basic or Visual C++ provides different ways to work with databases. The user can directly call database API functions from the DAO or ODBC Software Development Kits (SDKs). Or the user can choose to use the Microsoft Foundation Class Library (MFC), and let the MFC DAO classes and MFC ODBC classes simplify working with either database API.

Remember that while using the DAO classes through any language, Microsoft Jet (.MDB) databases are used. It is also possible to use DAO to work with external databases, such as ODBC data sources. When not using the Jet databases, the user is free to work with ODBC API for complete data-source independence.

Databases - ODBC

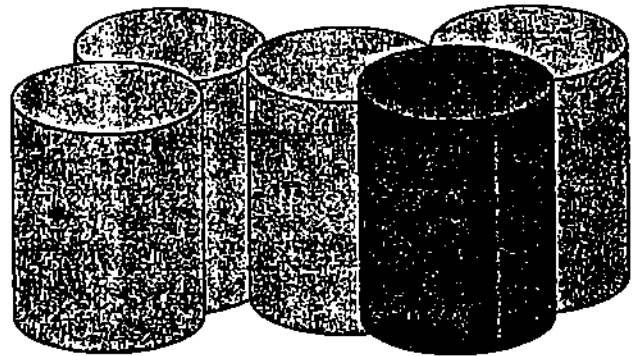
Since it is essential that many web based applications would connect to respective databases for querying and appropriately responding to users requests, the driver

software enable the applications to have connectivity to databases. There are different drivers for different platforms and databases. Of all of them, the ODBC drivers play most important role since they are used to connect to any kind of databases. They provide significant performance improvements in data access and also help shorten deployment time.

Open Database Connectivity (ODBC) is a widely accepted application programming interface (API) for database access. It is based on the Call-Level Interface (CLI) specifications from X/Open and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language.

ODBC drivers for the following databases must be available:

- Microsoft SQL Server
- Microsoft Access
- Microsoft FoxPro
- Microsoft Excel
- dBASE
- Paradox
- Oracle
- Unix based databases
- Text files



In addition, most of the databases also accept spreadsheets as well as tables in word processors as input and offers easy and fast conversion to their internal representation. This feature of conversion from and to (called importing and exporting respectively) proves to be extremely useful and is slowly becoming an essential feature of the databases. Some databases also offer a feature wherein the data stored in external format can be processed locally without disturbing the format of the actual database (called linking databases). It is most likely that the term convertibility would lose its importance in due course of time.

Databases - Distributed

Organizations select distributed databases for either or both of two following reasons:

- That there is a difficulty of communicating massive data and applications across the network on-line. In such a scenario, the organization plans to implement distributed database and connects them into an integrated network. For instance, look at the railways or airline ticketing which cannot be easily communicated over the expensive network lines for hours. Usually all processing is done at local level and are connected to the central server only when there is a need.
- That the organization may like to keep the information centralized but applications remain distributed in order to attain greater reliability, availability, safety or performance, or all of the above.

The following could be some of the strong points for implementation of distributed databases:

- **More fault-tolerance** : Such databases can work even if one or more databases or systems fail to work. In such an event, other centers can keep communicating and updating themselves thereby ensuring continuity of work.
- **More flexibility** : Distributed databases are easy to work with and they offer extremely high flexibility through various aspects ranging from installation, interface to manageability.

- **Easier to extend** : It is possible to have more processing and storage capability by increasing the number of relevant components.
- **Easier to upgrade** : It is not necessary to dismantle and install a new system or upgrade all the components at a time. The concept is that whenever a single large computer system or database becomes obsolete, usually it has to be replaced resulting in huge cost and disruption of all operations whereas in systems under distributed architecture, they may be upgraded in parts without major disruptions.

While there a number of good things happening due to distributed databases, there are few major problems too. They introduce several problems that are normally not found in centralized systems.

- Distributed databases and their implementation are highly complex due to complex synchronization between processes, systems and databases. They introduce lot of problems due to maintaining consistency of data.
- Generally speaking, since the central control and management is lost, it becomes difficult to change any part of the database or structure or any other aspect of data.

Keeping the above information in view, the planning for implementation of distributed systems or databases should be carefully dealt with.

Databases - Object Oriented Models

These days a number of programming languages as well as object oriented tools have come up due to rapid development in IT discipline. Consequently, databases also have taken the shape of object oriented database management systems or "OODBMS", which function purely on object orientation. They also offer connectivity to a broad category of other tools and programming languages to manipulate with objects. The concepts of data and schema have become old, but OODBMS with strong capabilities of managing objects are yet to hit the market.

Just as people deal with the entities/objects around them, the object-oriented models also attempt to implement the concepts of objects on the computer. The concepts, ideas, processes, or data, or combinations of these, are grouped together into one capsule-like entity called an object. An object supports a number of interfaces with which it communicates with other objects. It is much easy to operate with objects as compared to day-to-day issues since they provide much better manageability and organization.

Objects provide with an effective way of encapsulating things so that they can be used in other parts of the model. The interface describes exactly how to use the object. In a true object model everything is an object; however, going too far down this road enables to describe anything recursively and thus ending up explaining nothing. The object concept is used to build up a model of a distributed system, the model will then show what types of object interaction will be needed to support.

The re-usability of objects, and refinement through inheritance, makes systems more open, since they can support diversity, but permit comprehension of diverse systems into one.

5.3.2 Web Servers

Web servers allow serving information about the organization, its services and products over the intranet or Internet. At the most fundamental level, it uses the Hyper Text Markup Language (HTML) for presentation of the content.

The job of web servers does not end there; they accept requests from browsers like Netscape and Internet Explorer generated by users at the client end and then returns the appropriate HTML documents.

With the advancement of technologies, thousands of new features are being added day-in and day-out. A combination of many server-side computing techniques and technologies can be used to enhance the power of server beyond its ordinary capabilities; which may include implementation of CGI scripts, server-side includes, SSL security, and Active Server Pages (ASPs).

Note that the software are described separately as web servers and application servers. There is a little difference between the two. While the web servers perform functions encompassing those of application servers and other services like security, multithreading, communication, and many more. Some application servers available are as following:

- Allaire Cold Fusion
- Bluestone
- CreDO
- Cyberprise
- FastTrack
- Infoscape
- Intertop - I-Xpresso
- NetDynamics
- NetObject Fusion
- Netscape Application Server
- Netscape Enterprise
- NeXT WebObjects
- Persistence
- Perspecta (XML Based)
- Progress/Apptivity (Java Only)
- RadNet WebShare
- WebStar Pro

Primary Web Servers

The primary web servers apply all that have been discussed just now (as above) as the most fundamental services. Products such as AOLserver, Apache, WNServer, IIS, PWS, etc. are very well known and are easily configurable and manageable.

At the first instance, all the servers offer similar services; however, all of them differ in terms of certain additional value added features, better manageability, etc.

There is absolutely no shortage of free web servers on the market, especially those based on Unix. Apache is the most popular of all the available web servers and it is a freeware. Apache is a Unix-based software package that rules on about 60 percent of the web server market in the world as estimated by a survey.

The situation is different in the web server world other than Unix based. There are few freeware available and requires lot of searching for one such server. It is a well-known fact that most Windows-based servers are either costly or integrated into the operating system thereby making the process more complicated.

As a professional, the purchaser must ensure that the web servers provide support for two major standards, i.e. the HTTP 1.1 and CGI 1.1, both of which have become the most popular and widely used.

Most web servers are based on the content of a file and consequently are purely based upon the file extension. For instance, if a file of HTML format has been named "html.txt", then it would be served as a text file only.

AOLserver

AOLpress and AOLserver were formerly known as GNNPress and GNNServer (and much before they were popularly known as NaviPress and NaviServer) respectively. America Online combined or bundled the features of web authoring tools and web server into one.

The basis of AOL's complete web development service is known as PrimeHost, which combines the fineness of the HTML editor and web server. Joining the PrimeHost service, as a member will allow the user to have own domain name, a web site space of 20 MBs or more, counter programs, SSL support, and CGI capabilities.

Using PrimeHost user accounts can be easily set up with appropriate and moderate inexpensive monthly rates. Also offered are membership categories such as an individual, commercial, or dedicated user. Using the AOLserver software, whenever any a page is saved through AOLpress, it gets automatically hosted on the site. This cuts out the time and efforts required for saving files locally, transferring them to the remote server using FTP, and then making additional changes for maintenance thereafter.

In addition to seamless integration with the AOLpress client, the AOLserver offers the following services:

- Secure Sockets Layer (SSL) support (40-bit encryption);
- Multithreading and multi-homing capabilities with the ability to configure hundreds of virtual servers in a single process;
- An integrated search engine;
- Hierarchical access control (for restricting access to parts of the web site);
- Built-in TCL scripting language capabilities (for quickly building custom Web applications);
- Internal image map support;
- SQL database services;
- A complete C API for writing custom functions, drivers, and applications;
- Support for AOLserver Dynamic Pages (ADPs) which make it easier to create dynamic content;
- An integrated nsftp module (a fully-functioning FTP server that uses the AOLserver's permission system);
- Support for server-parsed HTML;
- HTML caching (allows pages to be served more efficiently);
- An nsyhost module for virtual hosting (non-SSL only);
- And many more.

AOLserver also offers native support for server-side includes, CGI, HTML-forms based configuration, remote site and page administration, custom error responses, page trailers, and more.

There are certain drawbacks of this server application as well. Most important being its support for the Windows NT platform only, the server also ignored the famous 128-bit SSL security technology support responding to the export regulations of US.

Overall, it stands as a good solution for serving anything from personal home pages to right up to corporate web sites. The presence of the AOLpress and the PrimeHost web-hosting service makes the duo-combination even much better.

iServer

iServer was developed by Servetec, written entirely in Java for any Java-enabled operating system, has the dual purpose of serving both web pages and Java servlets. In other words, it can be said that this is a special kind of product that offers the functionality of both a web server as well as an application server.

As a web server, iServer provides support as a simple multithreaded web engine generating threads for multiserver type environment and managing them. The iServer offers the following features:

The server supports HTTP 1.1

Uses minimal resources as the basic installation takes up to only 85K and the full package occupies space less than 125K.

Since it can manage Java servlets, it supports the more advanced protocols like IIOP and CORBA as well as fundamental protocols like ODBC, JDBC, SSI and CGI

It is a unique combine of BASIC and Java, permitting users to create BASIC-like scripts for Java environment. Also supports TCL and Perl.

The administration is done very easily through web while detailed log files help tracking usage levels and problems with the site.

As an application server, iServer has some attractive features, including:

- Load balancing (which allows management of incoming requests to a cluster in the most efficient manner and could include redirection to a less busy server);
- Fault tolerance;
- Database-connection pooling;
- Since it can run on a server with Java, it can be easily installed on the smallest PC based machine to the largest mainframe computer.

These features are usually found in enterprise-level application servers but not in web servers and hence offer flexibility for a scaleable web-server installation. However, there are some downsides in iServer:

- There is no provisioning for any other third-party authentication;
- Users, access rights, resources, and access control lists must be set up manually i.e. it is not even possible to import any user lists even from a Windows database or from the outside;
- Separate Perl support is not available (one could implement through CGI);
- No support provided for the Microsoft FrontPage extensions.

WN Web Server

WN is a free web server that runs on a number of variants of UNIX platforms. It provides support for both the major standards, HTTP 1.1 and CGI 1.1.

In the WN server the method of operation is unique and easy. The server is not based on the file extensions but a separate database called `oindexo` is maintained in which the filename, extension, type, security information, etc. are entered. All requests or references are checked with the entries in the index. A file is loaded only when there is a reference and permission for execution or service. The WN does not serve files unless specifically instructed by the index.

Obviously, the database called index makes the process of searching the website very easy. This is in line with the basic objective of WN to create an easy-to-search website. It becomes possible for the end users to search for desired data in many different ways and in different portions of the files.

Most important and notable point is that the security is implemented by the process of minimization rather than by authorization. The concept is as clear as that if the malicious users cannot see it, they would not know what to hack.

WN was one of the original web servers developed in this line. It is not just one of the nicest web servers available, but combine the features of stability with decent security features.

Sambar Server

Sambar is excellent web server software and had taken a lead further by being functional, reliable, and free. Sambar 5.0 is the latest version and provides the following:

- It is functional that means Sambar not only works like the server but also works very well in a wide variety of applications. At any time, if it is found that the server does not work according to the desired pattern, the system administrator can program APIs using languages like C and C++;
- A web-based step-by-step guidelines for configuration of Sambar;
- Supports ASP Web pages via the Sambar Server CScript language so that the system administrators can create dynamic and database-driven web pages;
- Sambar uses the HTTPS protocol in both 40- and 128-bit versions. Also, the OpenSSL libraries are supported;
- Sambar is reliable. When matched with a Windows-NT-based system, Sambar's reliability can come very close to that of a Unix/Apache-based system, so long as the supporting, custom APIs are programmed properly;
- Sambar can run as a Windows NT System Service by executing a file named ntserver.exe binary in the "bin" directory;
- Provides features similar to Unix daemons, i.e., the use of a system program without the need to log on to a machine and keep it connected;
- Provides a module called the Watcher Daemon that will try to restart the Web server and build up the system status automatically, and also arrange to send e-mail the administrator if server crashes.

It would be interesting to note that the basic Sambar Production Server is available free. The professional version of Sambar (that is priced at few thousand rupees) features such as DNS, mail, telnet, and proxy capabilities are offered.

Microsoft's initiative

The Microsoft Corporation has taken a lead over other software developers due to the fact that it has provided the most popular operating systems and other applications. This has led to seamless interchange of information and proper standardized approach for all the users.

The wave of Microsoft products continued and had followed the pattern in web servers as well. Most notable contribution of Microsoft has been the Internet Information Server (the latest being version 5.0) and the Personal Web Server (popularly known as PWS for the benefit of personal computer users).

Internet Information Server

Microsoft's IIS 5.0 is a great improvement over the existing versions of web servers and now bundled with the Windows 2000 Server operating system. This

version contains many new features along with enhanced performance and reliability. Notable improvements include

- Better and clearly documented security policies;
- Support for the new WebDAV publishing standards;
- Faster restarts of both Web and FTP services;
- Support of clustering, Microsoft has significantly improved the configuration and setup to enable multiple machines to share the load and deliver more reliable web services.

Microsoft has also added a few new wizards to perform common tasks much easily. Three important wizards are

- The Permissions Wizard (to synchronize and align Web and NTFS security settings);
- The Web Server Certificate Wizard (to obtain and install server certificates);
- The CTL Wizard (to create and modify certificate trust lists).

There is a strong support of a number of standards in IIS 5.0 including:

- Fortezza (a new U.S. government security standard);
- Transport Layer security using SSL 3.0;
- Digest Authentication (a method of hashing authentication information introduced in IE 5.0);
- Replacing NT LAN Manager authentication with the stronger Kerberos 5.0 authentication protocols used in Windows 2000.

The greatest improvement in IIS 5.0 is supposed to be the web-based distributed authoring and versioning or in short WebDAV. It is a newly developed standard designed to make the construction of intranets simpler. It also helps many simultaneous users to publish and host documents on a common web server. A step ahead, this protocol allows the users to use the web directories through Office 2000 and IE 5 tools running on Windows 98, NT and Windows 2000 as if they were shared over Windows file system.

The minimum specification required for running IIS is a 200 MHz Pentium based computer with 128 MB of RAM. Another product from Microsoft that acts as complementary to the IIS i.e. the Advanced Server that is meant for clustering purpose. Companies planning for running the Advanced Server clustering should double the RAM and CPU speed. Similar step is required even if it has been planned to run MS-SQL or Transaction services on the same machine as the web server. It should be remembered that for setting up clusters through Windows 2000, it is essential to think of Advanced Server that works fine with IIS.

Personal Web Server

Microsoft's Personal Web Server (PWS) also functions on the lines similar to the IIS or in other words, it can be that PWS is a lowered version of the IIS introduced and bundled along with the Server edition of Windows NT. Even though, it has been designed for Windows 95 and Windows NT Workstation users, the PWS has made greatest impact on the design, development and publishing of web documents by bring them to the personal computer range. It proved to be boon for small web sites and intranets.

While it is extremely easy to install and use PWS in terms of the clients, there are wizards that help the developers to quickly publish, share and administer the documents. The Explorer interface or the Personal Web Manager of the PWS can be used to share folders, start or stop the server services and do other similar tasks.

The documents intended to be published on the web site can be tested before hand for dead or invalid links, scripting errors and many other possible loopholes.

Once the site is ready to go live you can either continue using PWS to serve your Web site or you can use Microsoft Front Page to copy the Web site developed on PWS over to IIS. PWS and IIS are packaged together as part of the freely downloadable Windows NT 4.0 Option Pack; Microsoft Frontpage is a commercial Web design client that must be purchased separately.

Certain advanced features such the Index Server, Certificate Server, and Site Server Express found in IIS are not present in PWS. Further, the server does support the famous Active Server Pages (ASP), script debugging, and many other important features. PWS offers the ability to develop web applications using the Microsoft Transaction Server.

In general, it can be said that though large organizations may prefer other high-end web servers such as the IIS, the PWS remains a best option for smaller companies and personal computer users.

5.3.3 Other tools

There are tools available on certain web sites that can automatically check for various features of the submitted web site and give a detailed report about missing and dead links, compatibility to Netscape and Internet Explorer, download speed, size of images, etc. Such tools can prove to be very useful for error detection and better updation of the web pages. This kind of feature is also available in software like Macromedia Dreamweaver Ultradev.

In addition to all the tools available for web authoring and management, there a number of tools available separately in the market for carrying out the desired tasks in a much professional manner. A partial list of popular tools has been given below categorized under the kind of application:

- Agents
 - ✓ UMBC Agent Web
 - ✓ MIT Software Agents Group
- Discovery Agents (Content)
 - ✓ Web Robots Database
 - ✓ Aliweb
 - ✓ Harvest
 - ✓ Kinetoscope Via Agent Developer (Java Based)
 - ✓ Merzcom
- Discovery Agents (Network)
 - ✓ Advent Network Management (Java Based)
 - ✓ Concord
 - ✓ Kaspia Network Device
 - ✓ Network General
- Push Agents
 - ✓ SkyTel Web Paging Service
- Search Agents
 - ✓ AltaVista
 - ✓ Autonomy (Pattern Matching based)
 - ✓ Excalibur RetrievalWare (Pattern Matching based)

- ✓ Fulcrum
- ✓ Livelink Pinstripe
- ✓ Merzcom
- ✓ NewSurfer.com (multi-lingual)
- ✓ PicoSearch
- ✓ Semio (Pattern Matching based)
- ✓ Tacit
- ✓ Ultraseek
- ✓ Verity
- ✓ Web Browser Intelligence (IBM)
- ✓ WebSeeker
- **Subscription Agents**
 - ✓ BackWeb
 - ✓ DataChannel (XML Based)
 - ✓ Incisa
 - ✓ Majordomo
 - ✓ Marimba (Java Based)
 - ✓ NewsFlash
 - ✓ PointCast
 - ✓ Smart Delivery
 - ✓ Tibco (Rendezvous)
- **Tracking Agents**
 - ✓ eClips (Wireless Services)
 - ✓ Karnak
 - ✓ NetMind
 - ✓ Tympani NetAttche Pro
 - ✓ Tympani NetAttache Server (Group Services)
 - ✓ WebSeeker
- **Collaboration**
 - ✓ Bantu (web-based service)
- **Calendaring - Scheduling**
 - ✓ Amplitude Reserve
 - ✓ CrossWind
 - ✓ CyberScheduler
 - ✓ Netscape Calendar Server
- **Discussion (audio-video)**
 - ✓ CU-SeeMe
 - ✓ White Pine Reflector

- ✓ netPodium (Java Based)
- ✓ VXTREME video streaming
- Discussion (text)
 - ✓ ForeFront Roundtable
 - ✓ Forum
 - ✓ News Gateway
 - ✓ HyperMail
 - ✓ Internet TalkShow
 - ✓ Majordomo
 - ✓ Mastermind Forum Master
 - ✓ MIT Conferencing Gateway
 - ✓ Netscape Collabra Server
 - ✓ Xpound
- Document Sharing (create and edit MS Office documents through a web browser)
 - ✓ DataChannel (XML Based)
 - ✓ Net-It Central
 - ✓ Transit Central
 - ✓ Tympani Atlas Server
 - ✓ Web Wizards
- Email Response Management
 - ✓ Brightware
 - ✓ eGain
 - ✓ Genius Server
 - ✓ MailQueue.

Check Your Progress

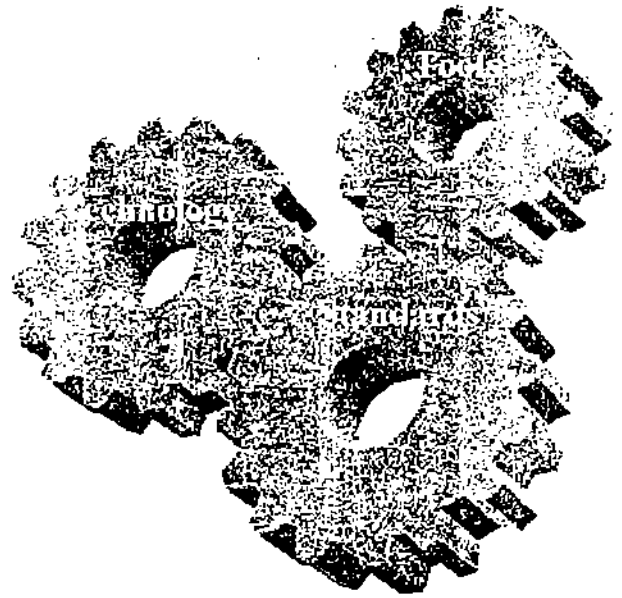
- 1) The Modeling Language that can be used in Virtual Reality Environments is _____
- 2) CommNet is one of the _____ clients available , features Zmodem support
- 3) _____ is a solid terminal emulator with extensive connectivity options
- 4) Distributed databases and their implementation are highly complex due to complex synchronization between _____
- 5) ASP stands for _____

5.4 SUMMARY

The adoption of higher concepts and systematic techniques such as object orientation and software engineering principles has also provided for proper interaction amidst tools. Clearly, the output of one tool can not be given as input to

another, for instance, the output of vernier caliper can not be taken as input to temperature controller, whereas it has become possible for computer based tools to interact with one another.

There is a specific need to stress on the importance of such tools with respect to intranet and Internet. As the technologies grew in number, so also the type of tools increased day-by-day. Today, there are hundreds of tools available right from the browser to request handling and much higher levels of request management and thread management, covering a number of platforms such as DOS, Windows, Unix, Mac, Solaris, Linux, HP-UX, AIX, Sun Cobalt and what not.



It is the law of nature, by default, that whenever there is a variety of tasks, tools, objects, entities or otherwise available, the immediate next step is standardization. This also follows standardization of various web authoring and management tools. The process of standardization should not stop just by identification but also extend to the minimum features they should contain and the functionality to perform. From the figure, it should be clear that the technology, tools and standards work hand in hand to attain the objective.

5.5 MODEL ANSWERS

- 1) VRML
- 2) Telnet
- 3) Anzio Lite
- 4) Processes, Systems and Databases
- 5) Active Server Pages

5.6 FURTHER READINGS

- 1) *Professional Active Server Pages* by Brian Francis.
- 2) *Building and Managing Virtual Private Networks* by David Kosiur, John Wiley & Sons.
- 3) *Designing Microsoft ASP.Net Applications* by Douglas J.Reilly Microsoft Press.

Reference Websites

1. <http://www.citrix.com/>
2. <http://www.novell.com/>
3. <http://www.developer.com>
4. <http://www.epicentric.com>

UNIT 6 INTRANET PROTOCOLS

Structure

- 6.0 Introduction
- 6.1 Objectives
- 6.2 Basic Intranet Protocols
 - 6.2.1 Communication cum Mail Protocols
 - 6.2.1 Service Protocols
- 6.3 Web Server Specific Protocols
 - 6.3.1 Common Gateway Interface (CGI)
 - 6.3.2 Internet Server Application Program Interface (ISAPI)
 - 6.3.3 Netscape Server Application Programming Interface (NSAPI)
 - 6.3.4 Distributed Mail System Protocol (DMSP)
- 6.4 Latest Protocols
 - 6.4.1 Code Division Multiple Access (CDMA)
 - 6.4.2 Wireless Application Protocol (WAP)
 - 6.4.3 General Packet Radio Service (GPRS)
 - 6.4.4 Protocols for E-Commerce
- 6.5 Model Answers
- 6.6 Further Readings

6.0 INTRODUCTION

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

This is just 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.

Take it for granted that without ensuring proper customer protection, the e-commerce and trade over the Internet can not function at all. Hence, methods should be evolved to protect the consumer/customer interest first and business next.

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, 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, HOP, etc.

6.1 OBJECTIVES

Almost all the protocols that can be used for Internet can be used for 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.

In addition, certain information on the latest protocols and communication methods through CDMA, WAP, etc., which enable mobile communication has also been incorporated in this unit. Little information about protocols useful for e-commerce applications has also been provided at the end.

6.2 BASIC INTRANET PROTOCOLS

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

6.2.1 Communication cum Mail Protocols

Address Resolution Protocol (ARP)

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

The Address Resolution Protocol (ARP) 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:

0	8	15	16	31
Hardware Type		Protocol Type		
HLEN	PLEN	Operation		
Sender HA (octets 0-3)				
Sender HA (octets 4-5)		Sender IP (octets 0-1)		
Sender IP (octets 2-3)		Target HA (octets 0-1)		
Target HA (octets 0-1)				
Target IP (octets 0-3)				

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

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 also such as Netscape or Eudora that have 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 uuencode 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 uudecode.

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, 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 timeout. 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 connection.

Post Office Protocol (POP)

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

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	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 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 the 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 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.

6.2.2 Service Protocols

Many Internet users are familiar with the protocols such as TCP/IP to connect to the Internet. These include those protocols that permits 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)

As 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 view, 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 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 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 it reaches the nearest machine or the immediate neighbourhood or server and then 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 appropriate range of IP numbers to different organizations. Thereafter, it becomes the job of the organizations to assign IP numbers to its departments and uses.

For an organization, there are two sets of IP addresses. This is where the difference between the Internet and intranet comes into 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 organization 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 organization. The organization 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 utilized 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 address are divided into four classes since networks vary in size, which the organizations 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 organizations;
- Class C addresses are for small networks (fewer than 256 devices) or may be for those at the level of organization, and
- Class D addresses are also called multicast addresses, normally for representing devices and computers on the network.

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 1 : Four classes of the IP addressing

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 organization or a service provider (in this case it is VSNL), 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 × 256 × 256 × 256 computers or devices or networks on the Internet, in short this amounts to 232. 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 addressing 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 when working on a Windows NT based computer, it is preferable to connect to a computer that actually runs on Sun Solaris or SCO Unix and run all the commands on that while viewing the output at this Windows 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 an impression that the user can access someone else's computer (also called a host computer) and that all the required permission 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 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 them when they arrive. The standard web browser installed at the clients' computers generate requests that are handled at the server by this HTTPd. Users demand to see the web pages by typing in the Uniform Resource Locator or URL of the organization 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 version 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 protocol version on 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 the future applications. The details of usage of HTTP methods are not being dealt here as they are beyond the scope of this context and relevant HTML programming reference should be referred for further information. The built-in methods of HTTP are given below:

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 resource (e.g., a Web page)
DELETE	Remove the Web page
LINK	Connects two existing resources
UNLINK	Breaks an existing connection 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 clients computers to servers.

The FTP service is widely popular amidst the 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 to do the activities in a much easier manner; even the commands need not be remembered at all. 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, or UDP as it is known, 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 a 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.

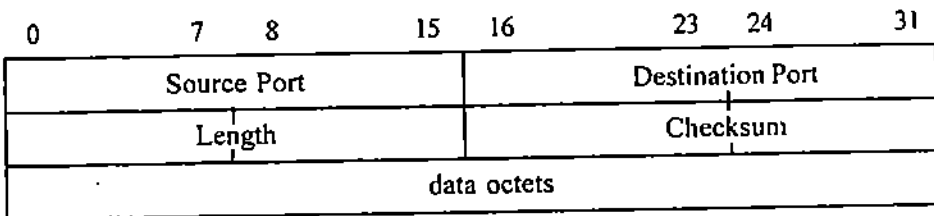


Figure 2 : User Datagram Header Format

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 lot of processing time spent on breaking and reassembling them.

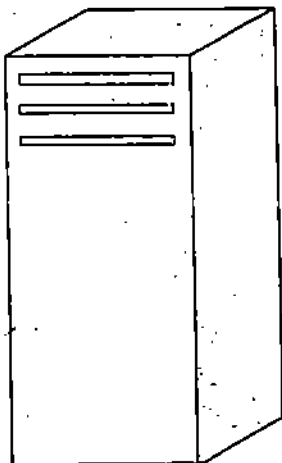
It may be remembered that a specific protocol called the Trivial File Transfer Protocol (TFTP) is based on UDP support rather than the conventional TCP. UDP can also be employed for Internet name server applications and usage. UDP offers two services not provided by the IP layer. First, it provides the port numbers where the request has actually 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.

6.3 WEB SERVER SPECIFIC PROTOCOLS

Even though there are a number of protocols available for communicating over Internet, there are certain protocols available specific to usage 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 embedded in the server side scripting. Many of them also provide thread management capabilities that are essential for handling multiple requests simultaneously.

6.3.1 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 organization or a product or a concept. The repository could be further included with massive database based applications. The Common Gateway Interface or CGI provides mutual agreement between various HTTP servers on integrating information exchange through gateway scripts and programs. The CGI scripts are used in conjunction with HTML forms to build database applications and query processing.



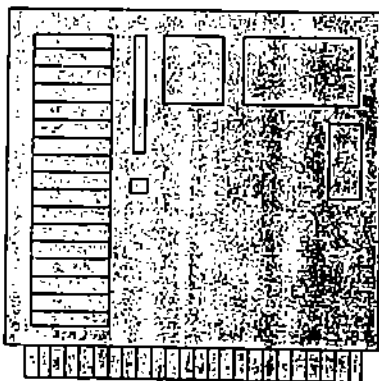
Following two are the most noticeable disadvantages of CGI based applications:

- 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.

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

6.3.2 Internet Server Application Program Interface (ISAPI)

The Internet Server Application Program Interface or ISAPI is purely based on 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 its counterpart - a CGI based application.



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 thereby increasing the processing speed many times more.

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 accommodate 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 and quite naturally, it offers far more flexibility than the 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 provides 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 customized logging, encryption, and authentication or path-mapping support. Filters allow users to alter the behavior 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 other 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

6.3.3 Netscape Server Application Programming Interface (NSAPI)

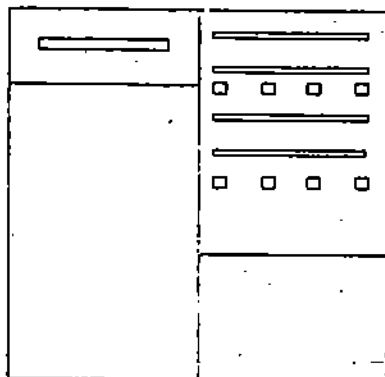
Just as ISAPI is specific to the Microsoft technology, another arch-rival in the market i.e. Netscape developed the Netscape Server Application Programming Interface or in short, NSAPI. It was created as a more efficient and robust replacement for the CGI. It can also be used to develop applications involving customized authorization, 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 the 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 and 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's functions called the built-in server application functions (SAF). Once initialized, the server waits for a 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 (authorization 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 authorization 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 of 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 the 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).

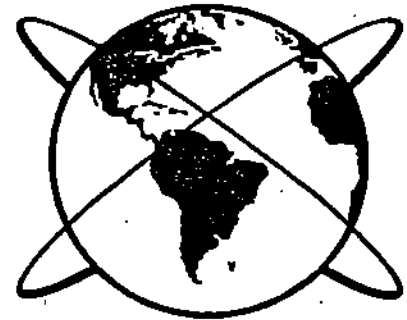
6.3.4 Distributed Mail System Protocol (DMSP)

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 the case with POP3 and IMAP.

It also offers the facility of multi-session connection for message delivery. At the first instance, it permits the users to download all the email messages from the server to a work station, 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, sessions is established, emails are transferred and the system is automatically resynchronized.

6.4 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 as 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 ushered into an era of electronic trading and mobile computing. This section bring out information about such technologies and protocols that guide these latest trends.

6.4.1 Code Division Multiple Access (CDMA)

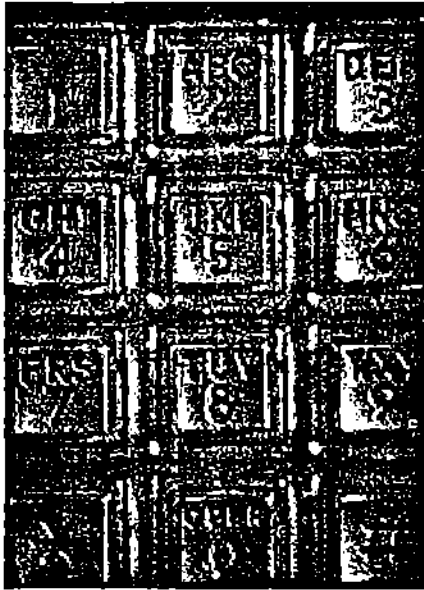
The CDMA technology spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal. This technology offers a number of benefits to the cellular operators as well as to the subscribers. To name a few, the following are the benefits of CDMA:

- Capacity increases of 8 to 10 times that of an analog system
- Improved call quality, with better and more consistent sound as compared to system or near-wireline quality voice service
- 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 that has been derived from military applications viz.,

- that the enemy efforts to jam communications system should be prevented by use of anti-jam or AJ techniques
- that the enemy should not even know that communication was even taking place, by use of concept sometimes called low probability of intercept (LPI).



The history of CDMA traces back to the days of 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 the telephone traffic capacity also called the Erlang capacity
- Greatly enhanced the voice quality and eliminating the audible effects of multipath fading
- Minimized incidence of dropped calls due to handoff failures
- Providing reliable transport mechanism for data communications, such as facsimile and internet traffic
- Reduced the number of sites needed to support any given amount of traffic
- Simplifying site selection
- Minimized deployment and operating costs because fewer cell sites are needed
- Greatly reduced average transmission power
- Reducing interference to other electronic devices
- Reducing potential health risks.

Availability of low cost, powerful digital integrated circuits, that reduced the size, weight, and cost of the exchanges or subscriber stations to minimal level. The two major break-throughs 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.

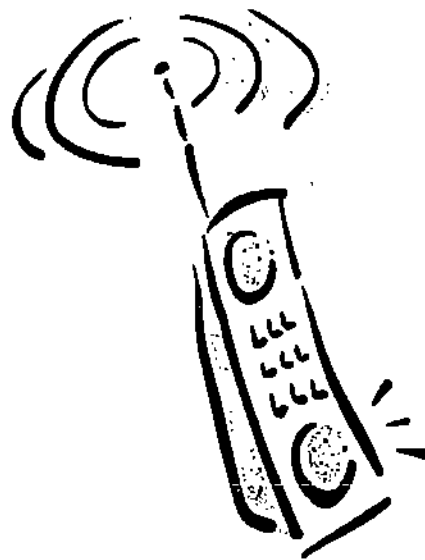
Since CDMA supports the digital technology, it changes the method the subscriber station operate. Programming the features has become extremely easy. Core technology has changed from extreme analog system to extreme digital system. CDMA receivers do not eliminate analog processing totally, but communication channels are separated by means of certain kind of modulation techniques that is

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 use throughout the North American continent 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 in 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 the 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.

6.4.2 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 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 result of

examination, amount balance in the bank account, temperature and humidity of the day, simple message service, etc. can be easily provided on the phones. Day-by-day, new services are being added to the features.

The WAP is the talk of the town due to the wide hype in the telecom industry as well as outside it. WAP is a standardized 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 forced all telecom and IT companies to open up departments for producing WAP based technologies in less than a year's time. WAP is in the news for the reason that it provides a standardized way of linking the Internet and mobile phones, thereby linking two of the largest and dynamic industries anywhere. The forum that founded the protocol includes major wireless corporates such as Nokia, Ericsson and Motorola, and Phone.com.

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

Initially, it was expected that mobile information services supposed to be the most important application for wireless based applications 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 limitations such as the following:

- WAP phones are very difficult to configure for new WAP services, with about 18-20 different parameters must 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 is not yet complete, even with the latest WAP version (i.e. ver 1.2) that came in 1999.

New protocols such as SIM Application Toolkit and Mobile Station Application Execution Environment (MexE) have already evolved before the proper standardization 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 the WAP could not attain great success due to the launch of technology much before actually being properly standardized 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 utilize fewest resources possible on the handheld terminals and to utilize 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 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 feature of WAP lies as under:

• 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 the diagram below:

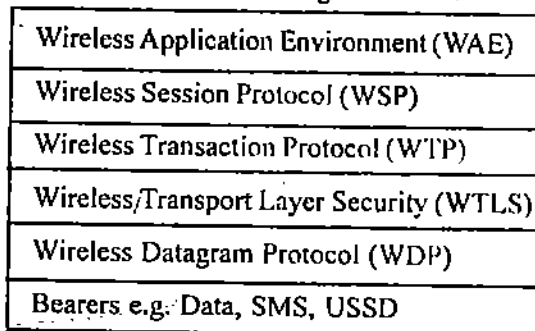


Figure 3 : WAP Protocol Stack

Wireless Application Environment (WAE): The WAE defines the user interface on the phone through the use of the Wireless Markup Language (WML), WMLScript - a scripting language similar to JavaScript and the Wireless 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 as 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 the wireless communication techniques.

The SMS, CSD and the USSD are three most important of the WAP/Es 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 other 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 the WAP would be used to control the 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 to home. Similarly, it would be possible to program the washing machines remotely.

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 77.2 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 enough 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 he intends to use.

In any means, it should be remembered that WAP will play an important role for the development of GPRS-based applications since 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, organized and standardized way to use the same application on different bearers.

4.4 Protocols for E-Commerce

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

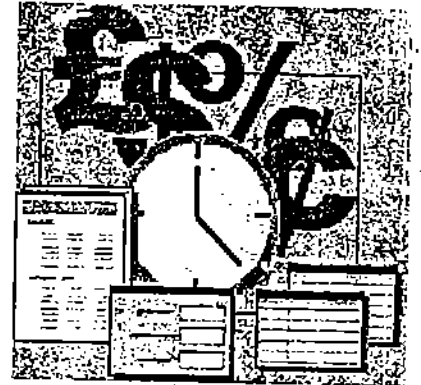
The world is fast moving towards Information Age wherein almost all the activities would be performed in the cyber space. This cyber era is poised to change the life style of every individual including day-to-day activities, the way people think and live. The age-old definitions of various entities as well as sentiments related to numerous issues are likely to get effected.

Electronic commerce is one of the foremost field that would be straightaway be redefined to suit the needs of the world. This field is relatively very new and 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 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 there arise a number of disputes in trade and commerce. With this property, an on-line arbitrator can settle certain customer/merchant disputes.



The MilliCent Protocol

Just as Agora, the 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 decentralized 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 the brokers for taking care of operations during scrip fluctuations. This helps the brokers to check frauds including forgery and double spending. 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 more than \$1 to over 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 cards as well as telephone users have account with the concerned offices that maintain proper account of usage, authenticity of user as well as transactions, provision of additional value added features, and many more. The customers are billed according the usage monthly or any other method that suits them well. But the concept of a protocol in lines with the Millicent is yet to make opening in India.

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

- Communication costs are greatly reduced by verifying the scrip locally at the vendor's site since there are almost no MilliCent-specific communication costs for a normal transaction. Moreover, no centralized 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 the account-based schemes, the vendor maintains the account whereas in MilliCent, the customer himself maintains the account.

MilliCent assumes a triangular trust relationships among the three entities of the system consisting of customers, brokers and vendors. In trustworthiness, brokers are assumed to be on the top followed by vendors and finally the customers. The only time customers need to be trusted is when they lodge complaint about services 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 with little effort use the change of scrip value. From the vendors' side there is absolutely no risk since a digital signature prevents the customer from changing and manipulating with the scrip value.

The following three activities make fraud from brokers' side unprofitable:

- 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.
- Usually customers do not keep large scrips at any one time thereby 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 quite obviously be at stake. A good broker would attract 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.

Most of the vendor fraud consists of not providing desired goods for valid scrip. The customers will lodge complaint to their broker, and in turn the brokers may drop vendors against whom a number of complaints has been lodged. This kind of third party evaluation also helps in policing on one hand and good vendor rating on the other hand.

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 private 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 be straightaway 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-selling of general items and essential commodities of use in day-to-day life.

Secure Electronic Transactions (SET) Protocol

The SET 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 human. 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 the 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 multi-million dollars.

Since the customer/consumer as well as the traders interest has to be protected, methods such as privacy, authentication, encryption, etc. 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 1970's with 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 56 bit key is that it can be easily cracked in few hours and with an investment of less than a million dollars, which is in reach of big companies. And this is possible for almost all security and military organizations 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 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 do not carryout any financial dealing but their 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 customers' bank account and immediately crediting into the vendors' account. Any failures 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. The _____ is situated at the bottom half of the Network layer
2. Media Access Control Layer uses a _____ whereas the Ethernet uses 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 _____

6.5 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 and with this trend, the technology too is following the suit. If it is intended to transfer any information directly to a mobile, it should be possible in few more 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 its 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 one hand and increase the business manifold on the other hand.

Though, the Govt. of India has permitted the trading over the Internet, lot of work is to be done in this line to slowly make a shift from the physical world to cyber world.

The success of the commerce over 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 the trade and commerce ethics, the protocols should be robust enough to handle every kind of eventualities that can come in due to intentional or unintentional manipulations.

6.6 MODEL ANSWERS

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

6.7 FURTHER READINGS

- 1) *David Linthicum's Guide to Client/Server and Intranet Development* by David S. Linthicum, John Wiley & Sons.
- 2) *Intranet's Decisions : Creating your organization's internal network* by Lisa Kimball, Miles River Press.
- 3) *Designing the Total Area Network: Intranets, VPN and Enterprise Networks Explained* by Steve Pretty, John Wiley & Sons.

Reference Websites

- 1) <http://www.semio.com>
- 2) <http://www.persoft.com/>
- 3) <http://www.iora.com/>
- 4) <http://www.vandyke.com/products/crt/index.html>

NOTES

NOTES