UNIT 3 INTRANET HARDWARE AND SOFTWARE

Structure **Page Nos.**

3.0 Introduction 38
3.1 Objectives 39
3.2 Selection of Computing Infrastructure 39
3.3 Hardware 40
 3.3.1 Servers
 3.3.2 Clients
 3.3.3 Security Systems
3.4 Network Environment 43
 3.4.1 Local Area Network (LAN)
 3.4.2 Address Translation
 3.4.3 Firewall
3.5 Software 45
 3.5.1 Operating System–Server and Client
 3.5.2 Groupware
 3.5.3 Database Connectivity
3.6 Other Aspects 50
 3.6.1 Protocol Support Tools
 3.6.2 Web Based Tools
 3.6.3 Security Tools
3.7 Summary 54
3.8 Solutions/Answers 54
3.9 Further Readings 54

3.0 INTRODUCTION

Intranets not only provide a secure environment for companies but also provide an excellent working environment that is full of information and resources for the users as well as for 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 the 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 with along with all the graphics until the user actually sees the effect on the computer can be considerable.

Now many organisations 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. These value added services, though seeming costly in the first instance, make for a reduction in recurring expenditure of communication costs while enhancing productivity. Installation of such services requires a one time high budget. The companies are realising 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 off places.

Just a few years back, when analog audio and video conferencing systems were used, the procurement and installation was complex, less reliable as well as costly. With the advancement of technology and reduction in communication costs, it has become possible to send and receive voluminous amounts of information much quicker and at almost negligible cost.

3.1 OBJECTIVES

A number of software tools are available in the market today. Similarly, hardware of various specifications is 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.

After going through this Unit, you will able to:

- understand the hardware requirements for input;
- understand the Network environment and its components;
- understand the software requirement for internet, and
- knew different protocol, web and security tools.

3.2 SELECTION OF COMPUTING INFRASTRUCTURE

The computing equipment on an Intranet must be selected in such a manner that they do not get obsolete very quickly or become too costly for the company. Apart from the specification of such equipments, the following points should also 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. leased lines are the dedicated channels between two network components as shown in *Figure 1*.

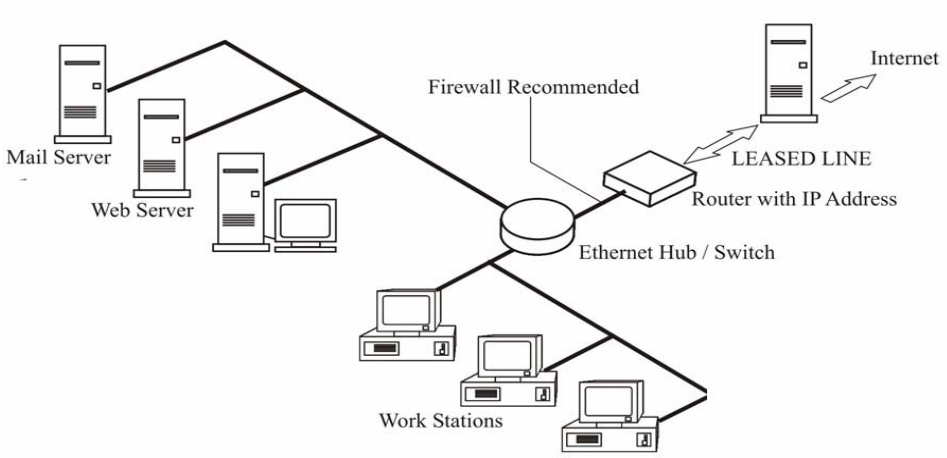


Figure 1: Leased Lines in Intranet

- Network equipment and connectivity should address various networking equipments 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, X.509 Certification, etc., in order to provide security to the Intranet server.

For an Intranet to work smoothly, the following tasks should be properly synchronised:

- 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 if the language used is Hyper Text Markup Language (HTML), everything that is developed for and intended to be hosted on the Intranet must follow HTML invariably.
- The protocol suite applicable for both Intranets and the Internet are called Transmission Control Protocol/ Internet Protocol (TCP/IP) and every computer should be compatible with 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 Intranets and the 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 obsolescence 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 professionals select hardware equipments 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 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

Xeon Processor

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 the following specifications would be sufficient for a medium to large organisation:

A Pentium III Xeon based server (dual processor recommended)
2×40 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 the number of nodes within an Intranet. Limits exist only on use of licenced software or on user restrictions on the network environment.

If anyone intends to have a higher configuration such as installation of four processors in place of the 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 lakhs to Rs. Rs. 2 lakhs, thereby taking the cost of server straight up between Rs. 12 lakhs and Rs. 15 lakhs.

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

- Reliability and Recovery
- Service Support
- 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 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 a 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., the 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 cannot 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 high 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 to the power of 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. In 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. is made.

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 for a variety of OS such as UNIX, Windows NT, Mac OS, etc.

3.3.2 Clients

The most interesting thing is that almost every computer can be connected as a 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
- 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 the Intranet open to various attacks from outside.

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

All the Units entering the Intranet must be scrutinised 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.

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 unauthorised 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 sent from authorised 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 anybody outside the organisation. It is useful for every communication within the organisation.

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, viz., 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 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 Fiber optic Cable

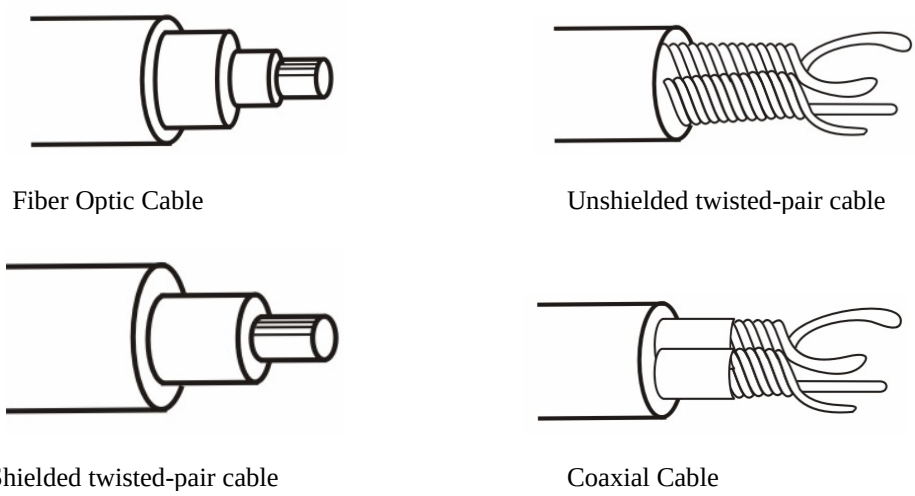


Figure 2: Communication Cables

In Figure 2 you can see different cables like Twisted pairs cables (Shielded and Unshielded), Coaxial cable and Fiber optic 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
- 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.

3.4.1 Local Area Network (LAN)

LAN is an interconnection of computers and associated peripherals as well as to the communications system as shown in *Figure 3* 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.

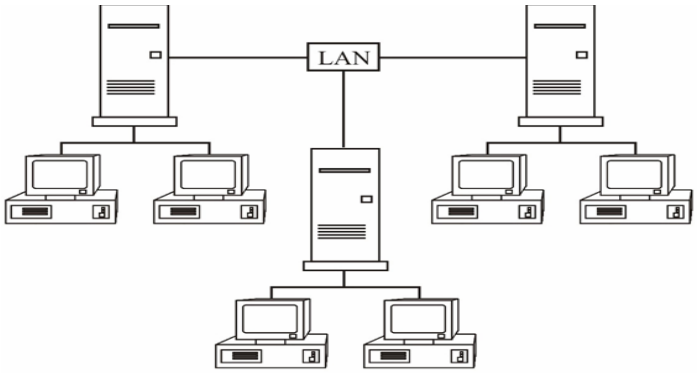


Figure 3: Local Area Network

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.

A detailed study of 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 to.

3.4.2 Address Translation

When a Web site address or URL is typed in the Web browser, as www.startv.com and not as a 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 computer 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 a data streams. If it receives a transmission in the form of 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, a brief description of the operating system, groupware and databases has been made. 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:

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

These 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 a 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 the Intranet, e.g., a Lotus Notes application can cost over Rs. 8 crore for a big group whereas for the same group corporate Intranet could be easily served with about Rs. 8 lakh.

These applications are many but not limited to the following:

- Communication tools
  - Voice mail
  - Email
  - Fax
  - Video conferencing applications as shown in *Figure 4.*

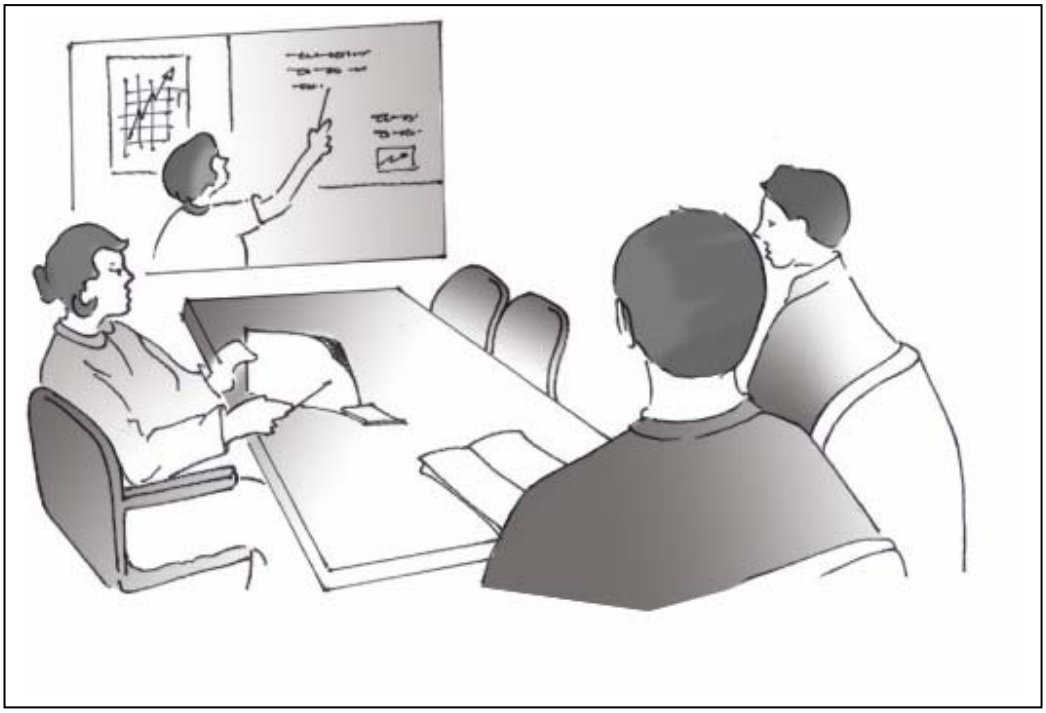


Figure 4: Video conference

- 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 for example excel 5 spreadsheet is shown in Figure 5.
  - Word processors
  - Graphical editors

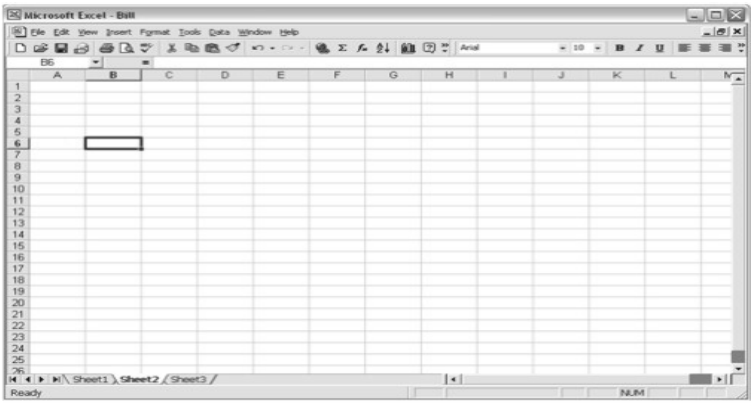


Figure 5: Excel Spreadsheet

- Web tools
  - Authoring
  - Publishing
  - Content management
  - Other graphical tools
- Simple security tools

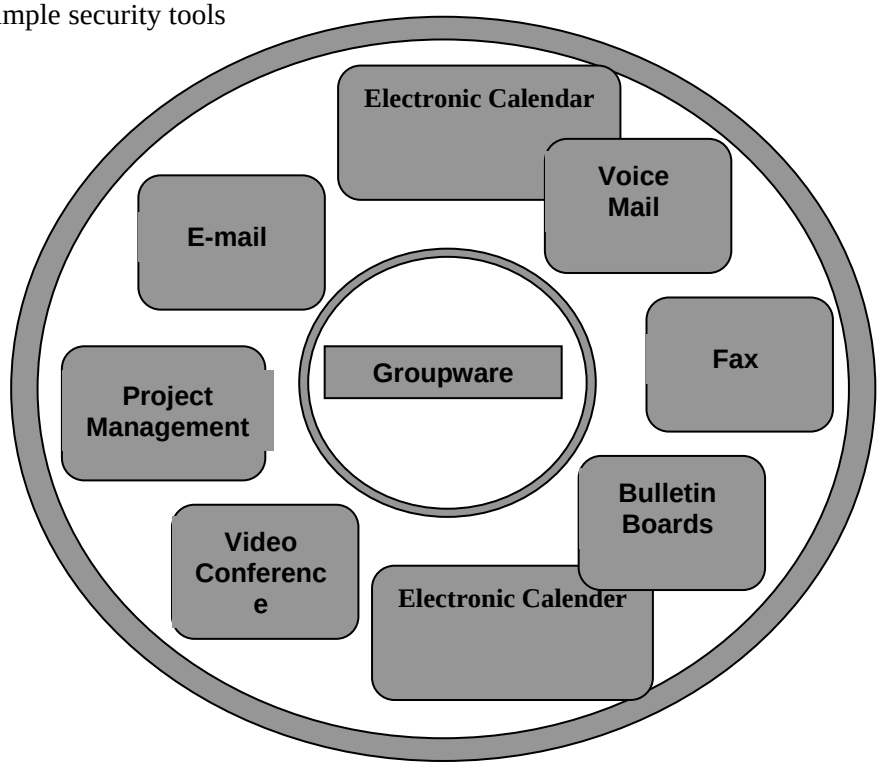


Figure 6: Contents of a groupware

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, analyse, 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 organisation on the whole contents of group are also shown in the *Figure 6*.

The downside of groupware is that they are very costly and with the increase in complexity or additional features, the cost 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 time the groupware proves to be cheaper, but such implementations are rare.

As long as the 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 the Intranet, users were free to use any platform they liked on any computer architecture. In order to eliminate every kind of barrier, all they need to have is an 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 explicit 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 the huge amount of day-to-day documents still remains a problematic issue. Not just storage but context based search also has been troubling the groupware developers.

Many developers have found a solution to this problem through a specialised tool, called the content management tool. These tools were initially developed for use of Web site management, but found suitable place readily on the Intranets as well.

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 likely 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 into 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 the Intranet.

3.5.3 Database Connectivity

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 the 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.

Middleware support

All the connectivity interface 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 even though 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.

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 an 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 as shown in *Figure 7*.

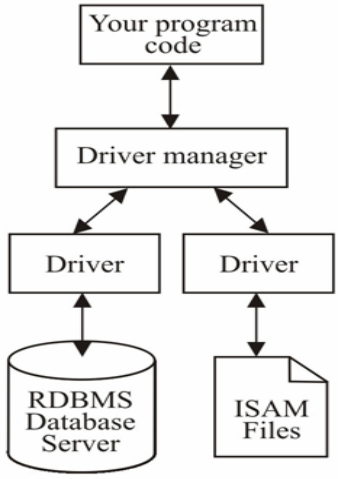


Figure 7: ODBC

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.

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 in spite of the technological divide.

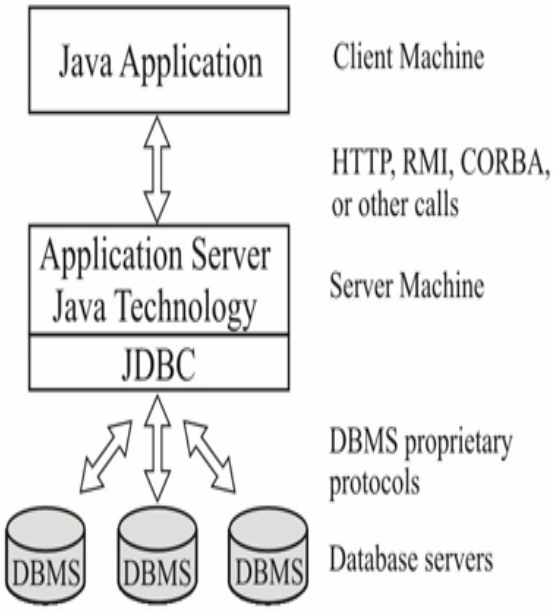


Figure 8: JDBC

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 as shown in *Figure 8.*

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

The 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 total freedom from the network architecture, machine dependence or topology dependency. The following is the list of protocols supported by the Intranet:

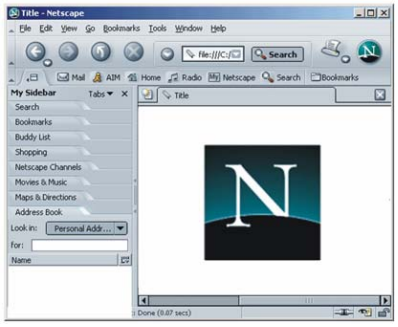
- **ARP:** Address resolution Protocol is used to resolve the hardware address of a card to package the Ethernet data. It works at the data link layer.
- **TCP:** Transmission Control protocol is a connection oriented reliable protocol working at the transport layer.
- **IP:** Internet Protocol. The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.
- **FTP:** File Transmission Protocol is a TCP/IP protocol running at the application layer.
- **TELNET:** An Internet communications protocol that enables a computer to function as a terminal working from a remote available at the application layer. (According to web reference TELNET derived from *TELephone NETwork).*
- **HTTP:** Hypertext Transmission Protocol is the protocol used to communicate between web servers and web browser software clients.
- **SPX:** Sequenced Packet Exchange operates at the transport layer providing connection-oriented communication on top of IPX.
- **IPX:** Inter-network Packet Exchange supports the transport and network layers of the OSI network model. It provides fast, unreliable, communication with network nodes using a connection less datagram service.

- **UDP:** User Datagram Protocol is a connection less unreliable protocol working at the transport layer.
- **POP:** Post Office Protocol is a used by mail clients to download messages from a mail server on the Internet.
- **LDAP:** Lightweight Directory Access Protocol is online directory service protocol defined by the Internet Engineering Task Force (IETF).
- **SMTP:** Simple Mail Transfer Protocol is a server-to-server protocol for delivering electronic mail.
- **SSL:** Secure Sockets Layer is a protocol designed to provide secure communications on the Internet.
- **HTTPS:** Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL Protocol enabling the secured transmission of Web pages.
- **CGI:** Common Gateway Interface is a way of interfacing computer programs with HTTP or WWW servers, so that a server can offer interactive sites instead of just static text and images.
- **NetBIOS:** Network Basic Input Output System is an API (applications programming interface) used with other programs to transmit messages between applications running on a network.
- **IMAP:** Internet Message Access Protocol is a protocol that allows a user to perform certain electronic mail functions on a remote server rather than on a local computer.
- **SOCKS:** The SOCKS Protocol is an Internet protocol that allows client-server applications to transparently use the services of a network firewall.

3.6.2 Web Based Tools

HTML, XML, CGI and other open standards

As is well known, 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 sees 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.



Netscape Browser

With the increasing competition between certain vendors especially the Microsoft and the Netscape, there have been a number of changes to the open standard. One company introduces interactive components; other adds capability of audio and video. 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 is standardization. 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 a lot of prosperity as well as total customer satisfaction can be ensured.

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

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.

The need arose for addressing various issues related to Web programming. Software were required for establishing connection to ensure security, connectivity to databases, conversion of the results to Web format, and a lot more. In response to the rising needs, numerous vendors have come up with numerous products. Some of them are listed below.

- 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., the Intranet should also be protected in a similar way 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.

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 of installation to suit the requirements of the company. While doing so a number of facts have to be taken into consideration.

The firewall vendors may be making 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 cannot 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 customised to improve performance. The software firewalls offer the flexibility of use on any hardware platform.

The Unix-based firewalls are considered most secured as compared to the Windows NT based ones. The firewalls bind 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 firewalls themselves can act as a proxy server.

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

Virtual Private Network (VPN)

Even though, many firewalls also include the features of the virtual private network, the functionality and capabilities of VPN are different from those 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 for the VPN to perform.

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 in cracking the code of a transaction, he cannot use the same key every time for cracking and will have to spend an enormous amount of time as he did for decrypting the first key.

Most of the server and browser software developed by various vendors carry out 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. Compared to this, the 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 the kind of security measure required to be taken for encryption. One such example is the Netscape, in which the user can select from available encryption methods and size of key.

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

☞ Check Your Progress 1

1) The protocol suite applicable for both Intranets and the 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 a 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 overheads
- 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 become extremely high, it stands as an indication for immediate replacement.

Many organisations are using Intranets to replace the costly groupware and e-mail applications with simple Intranet applications that cost only a few thousand rupees. Organisations 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 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 a 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, analyse, 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 standardised approach to processes.

3.8 SOLUTIONS/ANSWERS

Check Your Progress 1

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/internet/ijx/index.html.
2) http://indiafocus.indiainfor.com/internet/index.html
3) http://commUnity.marion.ia.us
4) http://www.planet-intra.com