# UNIT 4 NETWORK SOFTWARE

**Structure**

## 4.0 OBJECTIVES

After studying this unit you will be able to :

- understand the different types of network software;
- know network management and their basic functions; and
- get yourself acquainted with various types of commands used to test the network.

## 4.1 INTRODUCTION

There has been an explosive growth in computer networks during the 1980s. In fact, networking has revolutionized our use of the computer. As companies realized the cost benefits and productivity gains created by network technology, they began to add networks and expand existing networks almost as rapidly as new network technologies and products were introduced. Computer networks came into the picture with the realization that computers and their users need to share information and resources. Networks exist for applications. That is, users install networks to get a job done. Users can have computers, cables, interface cards, file servers, and protocols, but without applications software users can't do much but copy files from disk to disk. Network application software is what people use. The network is just the substrate upon which they use it. Many computer manufacturers now package networking software as a part of the operating system. A network operating system (NOS) causes a collection of independent computers to act as one system. A network operating system is analogous to a desktop operating system like DOS or OS/2, except it operates over more than one computer. Like DOS, a network operating system works behind the scenes to provide services for users and application programmes. But instead of controlling the pieces of a single computer, a network operating system controls the operation of the network system, including who uses it, when they can use it, what they have access to, and which network resources are available. There are three types of applications - network-ignorant, network-aware, and network-intrinsic.

### 4.1.1 Network-ignorant Applications

Network-ignorant applications are written for use on one computer by one person. These programmes can run on a network in the sense that they may be stored on a file server and network users may run them at their workstations. Most of the time there are severe limitations on what these applications can do. Moreover, if two people try to use the programmes at the same time, data can be lost or corrupted.

For example, if two people try to work on the same 1-2-3 spreadsheet, the person making the last change to the spreadsheet will write over all the changes made by the user who first saved his work. The programmme has no way of keeping the users from destroying each other's work. It lacks concurrency control. On the other hand, 1-2-3 can be used safely by several people at the same time, as long as they are using different spreadsheets (and if they have a license to do so). But the standalone version of 1-2-3 does not provide functions to take advantage of the network.

### 4.1.2 Network-aware Applications

Network-aware applications are a step above network-ignorant applications. Usually, they are network-ignorant programmes modified to run on a network. These programmes recognize they will be used by several users at a time. They have concurrency control features such as file and record locking to coordinate usage by multiple users. For example, when a Paradox user begins to modify an address in a mailing list database, other users who are also looking at the same database table are prevented from changing that particular address record. This is called record locking. When the change is complete, the change is displayed on the screen of every other user looking at the table.

Another network-aware feature is file locking. This is a less sophisticated and less used form of concurrency control. Instead of keeping users out of a particular record, they are kept out of the entire file altogether while another user has it open. Word processing programmes are the primary users of this type of concurrency control. Communications software and electronic mail are also network-aware applications. They use the network to extend the abilities of a PC and share network resources.

At the same time, even these network-aware applications use the network as little more than a peripheral sharing device. The file server holds the data and the programmme but does not do any processing. Users access the programme as if it were local, but all the work is being done by their PC, including all concurrency control. This is changing.

Network-aware programmes make up the vast majority of programmes written for networks. They are a big improvement over network-ignorant applications and have gone a long way to spur the growth of networking. As they become more sophisticated, the distinction between network-aware and network-intrinsic is blurring.

### 4.1.3 Network-intrinsic

By implication, network-intrinsic applications have the ability to distribute data over the entire network. Network-intrinsic applications actually share the processing power of several computers. Usually, although not always, this is done by dividing the application programme into pieces. One piece is the server, which does data processing; the other piece is the client, which talks to the user. In the client-server computing environment, conversely, developers separate their applications into two components, a “front end” and a “back end,” with the elements sharing the processing demands according to which is best suited for the task. This separation of responsibilities allows client-server systems to more efficiently use an organization’s computing power and network bandwidth.

Servers may run on different network operating systems across different hardware platforms and use different database servers. The Network File System (NFS) is a facility for sharing files in a heterogeneous environment of processors, operating systems, and networks by mounting a remote file system or a directory on a local system and then reading or writing the files as though they were local. The client application invokes these services without considering the technology of the various servers.

## 4.2 CLIENT – SERVER (TWO TIER) ARCHITECTURE

In the early days of computing there was no communication among the computers as the computers were operated independently or as standalone entities. This led to the development of multiprogramming, time sharing systems such as in mainframe architectures followed by the development of standard protocols and open systems for network operations.

The limitations of Mainframe architecture, viz., having centralized intelligence, lack of graphical user interface support and no access to multiple database, led to the emergence of two-tier (Client-Server) architecture in the 1980s as shown in figure 1.

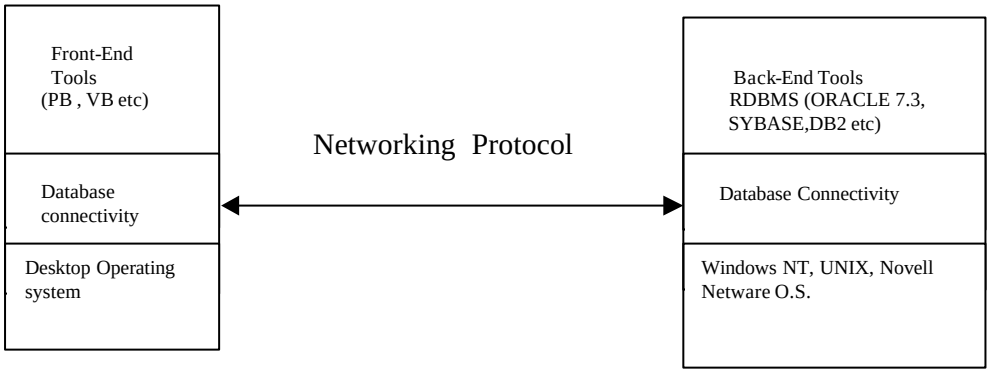



**Figure 1 : Client/Server Architecture**

The front end, or client-based part of the application, provides the end-user interface-that is, the onscreen images the user follows while interacting with the application-as well as processing capabilities. As in the traditional network client-server model, the back end delivers server-based functions such as data lookup and retrieval.

In the client-server computing architecture, however, only the front end of the applications - not the entire application - is loaded into users' PCs when they start the programme. Now, when a user's front-end application queries a database for a particular record, the back-end server-based software searches for the specific record and sends it-not entire masses of data - to the user.

This significantly reduces the volume of data moving across the network because entire databases are not continually being sent back and forth between server and client. This offers secondary benefits in that reduced traffic can also lower the risk of electrical or mechanical malfunctions compromising the integrity of data.

Another benefit of client-server computing: Because the server rather than the client handles much of the manipulation of data, it eliminates the need to give each employee who accesses the database a high-performance PC. Only the database server needs a large, fast hard disk, high-performance controller hardware, or multiple high-powered processor chips.

## 4.3 THREE TIER ARCHITECTURE

The client-server applications are written using proprietary front-end tools (Power Builder, Visual Basic, Developer 2000). This is a big risk because proprietary

languages have no guarantee of performance and they are not equally supported across different platforms. The two-tier client/server architecture is a good solution for distributed computing, where work groups are defined as dozen to 100 people interacting over a LAN simultaneously. It has, however, limitation when the number of user exceeds 1000 as the performance begins to deteriorate.

It is also very difficult to modify the code on both sides as the rules change often. All clients that connect to the database must be modified to reflect the new rules. Programmers know that it is annoying to maintain different pieces of software that basically access the same data. The code of one programme may barely import into another programme even when developed with the same programming language and tools. Approaches such as standard in-house developed libraries address the problem but too often do not totally solve it.

The idea of three-tier architecture as shown in Figure 2 emerged to overcome the limitations of two tier architecture by moving most of the codes that access and process data into the third tier/middle tier. In the three tier architecture, a client is split into two parts, i.e., Browser (User-interface) and logic. Thus two tier Client-Server becomes three tier architecture. Nothing much changes on the database side. It still maintains the data and holds the most important stored procedures on the server that consume the most CPU cycles. It keeps the role of providing concurrent accesses, integrity, recovery and helps in data administration. Browser (thin client) no longer holds any byte code of the programme for the access of the data using SQL. It will neither see rows of data nor map rows of data to load variables or object data module.

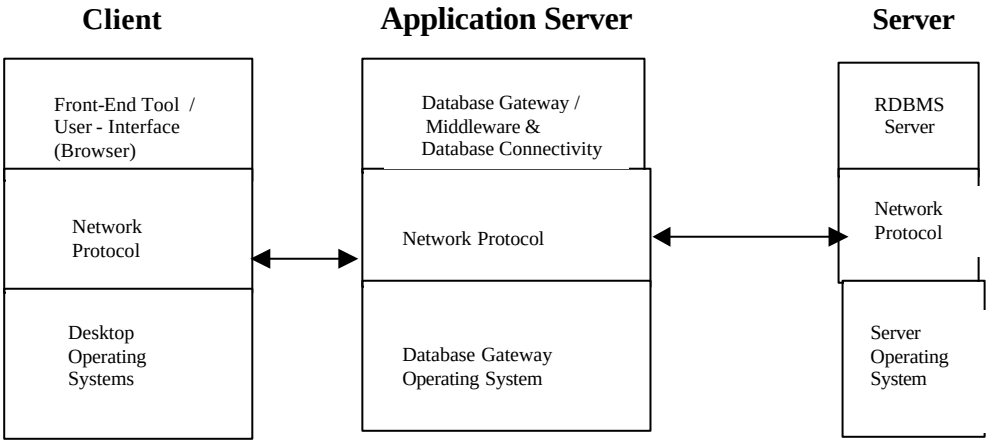



**Figure 2 : Three-Tier Architecture**

The logic, which describes how to access and process data is moved to a new server. The application server which is also called Middleware is a client of the database server and in a sense a server for the thin client application. The client can deliver its request to the middle tier and disengage because the middle tier will access the data and return the answer to thin client.

The middleware software sits on top of the web server. When an user requests a page through browser, specifying an Uniform Resource Locator (URL), the HTTP / web server translates this URL into a pathname for a file on the server host machine. If the file is an .html, .gif, .jpeg the web server sends the file directly to the browser.

However, when a browser requests an URL for the middleware, the web server passes the requests to a middleware programme.

Middleware helps the programmers to create networked applications. Data access in terms of OSI reference model takes place at the application (seventh) layer. Programmer has defined Middleware products by their Application Programme Interface (API). Depending upon the difference between the API of the Middleware products, they can be classified as under.

### 4.3.1 RPC - Based Middleware Products

RPCs allow a programme running one computer to call a procedure (similar to a function or subroutine) that executes on a remote machine and performs a single, discrete task. RPCs allow point-to-point communication. Some of the products are: OSF/DCE/RPC, Sun ONC TIRPC (Transport Independent RPC),Net Wise RPC, Trans Access, HP NCS RPC, Digital DCE Runtime Services, Gradient Technology DCE.

### 4.3.2 Message-Oriented Middleware Products

Message-oriented middleware uses a different approach from RPCs. Messages are sent asynchronously to a distribution, that is they are sent there; but the sending programme does not require a reply before continuing operations. This approach generally is implemented using one of two mechanisms. Publish and subscribe or message queuing. Some of the products are : Peer logic Pipes, Momentum software's IPC, BM MQ series, Sunsoft Tool talk Message, Decmessage Q.

### 4.3.3 Distributed Transaction Processing (DTP) Monitor Middleware Products

DTP Middleware - the category of software that includes transaction server - ensure transaction integrity, balance application work loads across multiple servers, and enforces appropriate secure access at the application and transaction levels. Some of the popular products are as under : Tuxedo,Encina,Web.Sql, Net.Data, MS Intendev, Jacquar CTS

### 4.3.4 Object Request Broker(ORB) Middleware Products

The Common Object Request Broker architecture (CORBA) specification was developed by the Object Management Group (OMG) to allow communication between applications no matter where they are located and on which operating system. For example, a CORBA could allow a thin client written in Java running on a PC to seamlessly invoke a procedure written in C which executes on a Unix server setting in a different city. The client might then invoke a procedure that is part of a legacy application written in COBOL which executes on a mainframe in a different country. With CORBA software component there is no need to know which software or hardware platform it is running on or where that hardware is located on the network.

## 4.4 NETWORK OPERATING SYSTEMS (NOS)

A network operating system (NOS) is a collection of software and associated protocols that allows a set of autonomous computers, which are interconnected by a computer network, to be used together in a convenient and cost-effective manner.

At a basic level, the NOS allows network users to share files and peripherals such as disks and printers. Most NOSs do much more. They provide data integrity and security by keeping people out of certain resources and files. They have administrative tools to add, change, and remove users, computers, and peripherals from the network. They have troubleshooting tools to tell network managers what is happening on the network. They have internetworking support to tie multiple networks together.

Network Operating Systems offer many capabilities including:

— Allowing users to access the various resources of the network hosts.

— Controlling this access so that only users with proper authorization are allowed to access particular resources,.

— Making the network and the eccentricities of the host computers transparent to the users.

— Making the use of remote resources appear to be identical to the use of local resources.

— Providing uniform accounting procedures throughout to the network.

— They can also distribute processes. This makes for distributed databases, compile servers, compute servers, multitasking communications servers, and many other applications in which programmes cooperate across the network to get a job done.

Network operating system software, such as NetWare, LAN Manager, and Solaris, provide some applications. Because most modern network operating systems support TCP/IP protocols, heterogeneous computers ( Windows NT Operating System, IBM mainframe, Unix systems, Open VMS System) can be interconnected easily.

TCP/IP supports a suite of protocols each of which provides a different service. The protocols allow networking communications to be independent of network hardware. The TCP/IP protocol suite is organized in the following groups:

- Application-Level Protocols, such as DOMAIN, Exterior Gateway Protocol (EGP), File Transfer Protocol (FTP), FINGER, TELNET, Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol.

- Transport –Level Protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)

- Network-Level Protocols, such as Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Protocol.

  In addition to the TCP/IP, most of the applications people use with the Internet also have their own protocols and are used for different purposes such as :

- Simple Mail Transfer Protocol (SMTP) defines a straight forward way to move E-Mail between hosts.

- Hyper Text Transfer Protocol (HTTP) is a standard method for transmitting information through the Internet. HTTP and its sibling standards, the document mark-up language known as Hyper Text Markup Language (HTML) have

done more than anything to make information exchange accessible to the masses and have been the principal contributing factor in the explosive growth of the Internet. HTTP is known as a "stateless" protocol. That is, HTTP can't "re*member" the st*ate that it was last in. What really happens is that when a Web browser connects to a site, it sends a request for a particular file on the server. The Web browser returns the file and then totally forgets about it. When the next file is needed because the viewer clicked a link, the entire process is repeated.

## 4.5 DOMAIN NAME SYSTEM (DNS)

On a TCP/P network, computers know each other by their IP addresses. But for human beings, remembering numbers is not the easiest thing to do. Remembering names is much easier. Similarly, a way was devised to associate IP addresses with names that can be easily remembered.

In the early days of the Internet "hosts" files were used to associate machines with names. The hosts file is simply a table of IP addresses and corresponding names like a phone directory. Any name lookup (the process of identifying the IP address associated with a name) will first check the hosts file (if present) on the machine making the query to see whether the name can be resolved.

But with the number of hosts on the Internet increasing rapidly to an unmanageable level, that soon became impossible. The way out was the DNS : The Domain Name System. In 1984 DNS started to get over the problem of remembering routes and the network numbers.

The DNS is a distributed, scalable database of IP addresses and their associated names. It is distributed in the sense that unlike the hosts file, no single computer contains all the DNS information in the world. The DNS data is distributed across many Name Servers. It is scalable i.e the volume of total DNS data and requests from machines for the same data, without significantly increasing the querying time. Otherwise the World Wide Web would really have become the World Wide Wait.

To understand the DNS and the way it is used, we need to understand the Internet naming structure. Let us take for example the address http://www.inflibnet.ac.in or http://inflibnet.inflibnet.ac.in

**www** **:** indicates that the machine is part of the world.

**in** **:** indicates the top level domain (TLD) that the machine is part of. Top level domain include .com, .edu, .gov, .in, etc.

**ac** **:** shows that the computer we are looking for is in a network called ac

**inflibnet** **:** indicates a sub network (a group of computer with a common function or at a common location).

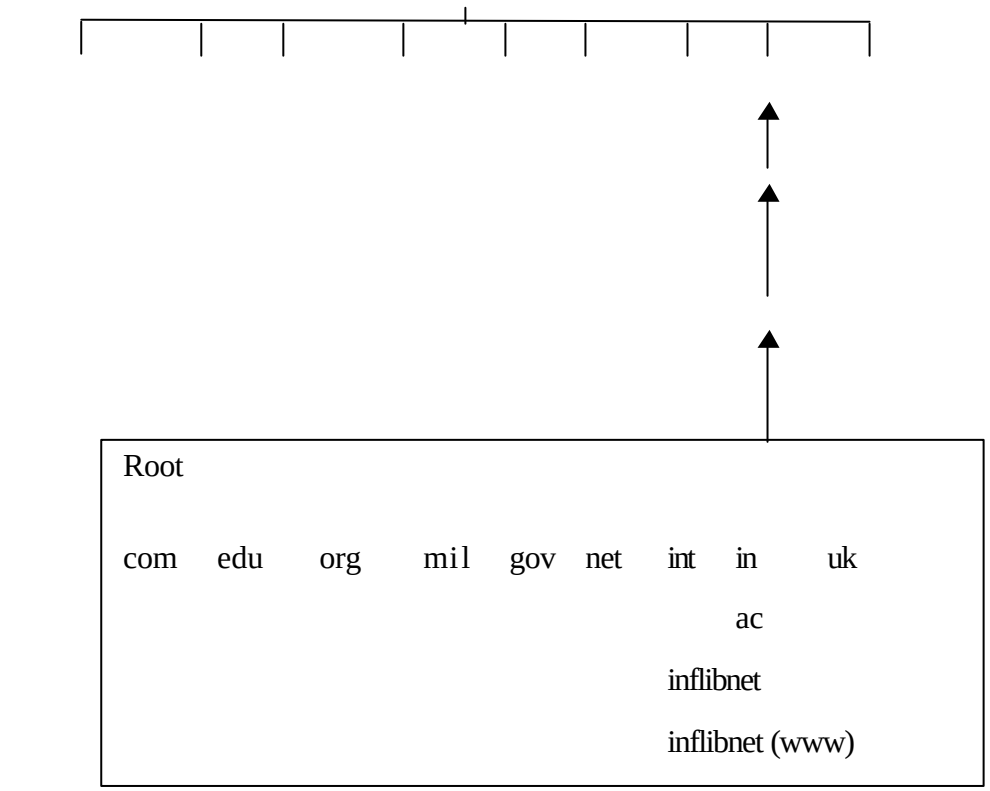
**inflibnet** **:** is that name of the machine that we are interested in and the name is changed to www.

| TOP LEVEL INTERNET DOMAINS | | |
|---|---|---|
| Domain | Indicates | Examples |
| com | Commercial organisations | yahoo.com |
| ac | Academic Institutions | iiml.ac |
| mil | A (US) military set up | nic.mil |
| gov | A (US) government set up | nasa.gov |
| org | Other organisations | www.bjp.org |
| net | Other networks | vsnl.net |
| int | An international organisation | tpc.int |
| in, uk | Which country the network | ac.in is for India. |
| etc | is in | bbb.co.uk |

Let's see how the DNS aids in identifying the machine's IP address, given its name. At the top level of DNS structure are the nine root name servers of the world, which contains pointers to the master name servers of each of the top level domain. To find the IP address of http://www.inflibnet.ac.in, the DNS server (the one that services the host making the request) will have to ask one of the root name servers for the address of the master name server for the .com domain. This master name server will have the addresses of the nameservers for all the .in domains.

From here you get the address of the name server for the inflibnet.ac.in domain. You move on to this nameserver, which will give you the IP address of the machine www.inflibnet.ac.in or inflibnet.inflibnet.ac.in .

**The Structure of the Internet**



## 4.6 ELECTRONIC MAIL (E-MAIL)

Electronic Mail is the most widely used TCP/IP application which has abolished the notion of distance and engages the largest number of people. E-Mail is a convenient way to reach people and normally is easy to use. The message is sent to an electronic mail box with a specified destination address. A typical address look like hasansk@yahoo.com in which hasan specifies local part giving the name of mail box on a destination computer and yahoo.com domain name.

The transmission of an e-mail message through the Internet relies on the Simple Mail Transfer Protocol (SMTP ). The SMTP defines a straight forward way to move mail between hosts. There are two roles of the SMTP Protocol, i.e., Sender and Receiver.

The sender establishes a TCP connection with the receiver. The well known port used for a receiver is 25. First they identify their host domain names. Then the sender executes a mail transaction by : Identifying the mail originator, Identifying the mail recipients, Transmitting the mail data, Transmitting a code that indicates that the item is complete. At the end of a transaction, the sender can start another transaction, reverse roles so it becomes the receiver, quit and close the connection.

SMTP is fast and efficient, and does a great job, but has one drawback. It expects both end nodes to be on-line simultaneously. That is where POP comes in.

### 4.6.1 Post Office Protocol (POP)

The Post Office Protocol (POP) can be used to transfer mail between desktop stations and a mail server. Like SMTP, it is simple to implement, as it uses plain ASCII text , which assure it of platform and operating system independence, a factor of crucial importance for the Internet. POP is an idea , but it is fast beginning to show its limitations.

### 4.6.2 Internet Mail Access Protocol (IMAP)

IMAP unlike POP, allows hierarchical storage of mail and a message retrieval system that allows selective access to the mail box. While POP is used for simply retrieving and deleting the message, using IMAP the mail can be organised so that it can be read on the server itself.

For a user getting connected over a slow dial up line, IMAP provides ways to download only the header or the body of the message that contains a large attachment. In addition, IMAP allows one user to access multiple mail servers and multiple users to share a single mail box.

IMAP can work on any of three modes of communication: on-line, off-line, or disconnected operation. In the Online mode, the mail is processed in an interactive fashion, that is the client can ask the server for a reply to the message headers and then request only specific messages, or can even retrieve just parts of certain messages.

IMAP also allows one user to access multiple mail servers and multiple users to share a single mail box. Similar to POP, IMAP also depends on SMTP for sending the mails.

There are many e-mail software available such as MS Exchange 5.5 , Lotus Notes, Pine etc. Pine (Pine Is Not Elm) software , a sophisticated e-mail utility that can

send not only text files but also binary files such as images and sounds by using MIME (Multipurpose Internet Mail Exchange) which comes bundled free of cost with Linux operating system.

## 4.7 USEFUL TCP/IP COMMANDS

### 4.7.1 FTP (File Transfer Protocol)

File transfer between machines running TCP/IP; these machines may or may not be running the same operating system. Many FTP Servers allow one to download files without having an account on the machine by having anonymous or FTP for a user name and the e-mail address for the password. This is a major means of distributing software and information on the Internet.

FTP ip address, i.e., FTP 202.141.130.67
FTP>PUT "filename"
FTP>GET "filename"
FTP>BYE

### 4.7.2 TELNET

Remote login on a machine running TCP/IP ; these machines may or may not be running the same operating system.

TELNET ip address i.e TELNET 202.141.130.67

### 4.7.3 FINGER

A standard utility that is a part of the TCP/IP protocol stack that helps in finding a valid user logged into a system you have access to. It's used in Unix based systems.

FINGER xyz@inflibnet.ernet.in

### 4.7.4 Packet Internet Grouper (PING)

Internet Control Message Protocol (ICMP) is an important maintenance protocol. It allows two systems on an IP network to share status and error information. This information can be used by higher-level protocols to recover from transmission problems or by a network administrator to detect network trouble. Although ICMP packets are encapsulated within IP packets, they are not considered to be a higher-level protocol. The PING utility uses the ICMP echo request and echo reply packet and allows one to query another IP device on the network to determine if the IP device is "alive" and how long it takes a packet to reach the device. Following is the syntax to launch the PING utility.

PING [-t] [-a] [-n count] -[-l size] [-f] [-i TTL] [-v TOS] [-r count] [-j host-list]|

[-k host-list] [-w timeout] destination-list

example

C> PING 202.54.4.114

If a device is having communication problems on the network, enter the following command at the DOS prompt.

PING 127.0.0.1

The address 127.0.0.1 is the loopback address. If you enter this command, the device pings its own TCP/IP stack. If the device can't see its own TCP/IP stack, the device can't communicate on the network.

### 4.7.5 TRACERT

The TRACERT utility allows one to determine the route that a packet may take to get from one device to another (if a route exists). This utility can be used to determine the time that it takes the packet to reach routes and to identify sluggish spots on the route.

Following is the syntax to launch the TRACERT utility :

tracert [-d] [-maximum hops] [-j host-list] [-w timeout] target-name.

C> tracert 202.54.4.114

### 4.7.6 Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is one of the maintenance protocols that support the TCP/IP suite and is usually invisible to the users and applications. For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address.

After receiving a MAC-layer address, IP devices create an ARP cache to store the recently acquired IP-to-MAC address mapping, thus avoiding having to broadcast ARPS when they want to recontact a device. If the device does not respond within a specified time frame, the cache entry is flushed. Following syntax can be used to launch the ARP utility :

ARP -a[inet_addr] [-N if_addr]

ARP -s inet_addr eth_addr [if_addr]

ARP -d inet_addr [if_addr]

### 4.7.7 ROUTE

When considering how to route packets to a remote destination, a device first checks its local routing tables. The ROUTE utility can be used to manually add entries to the routing table; however, devices usually learn routes dynamically from the network.

Following syntax can be used to launch the ROUTE utility :

ROUTE [-f] [command] [destination] [MASK netmask] [gateway]

## 4.8 NETWORK MANAGEMENT SYSTEM (NMS)

The network delivers a reliable communication service. The computers and applications deliver critical information, analysis, access control and security. Increasingly, computer and applications depend on the network for access to distributed databases, user authentication and communication with other computers and applications. The network is becoming more highly utilized and more critical to the process of doing business. The network has become business critical.

This increasing utilization creates higher requirements for resilience. Should the network fail, business-critical applications would fail with it. The network carries traffic of varying priorities; order entry / tracking, accounting audits, engineering design, e-mail file transfer, and World Wide Web access. The higher utilization of the network makes it necessary to treat this traffic in different ways in order to allow the business-critical traffic to flow without congestion. Congestion on the network causes business-critical applications to process fewer transactions each day, costing the business untold amounts of money.

The network connects all the business critical resources in a company. This makes it the doorway into the business that is vulnerable to attack. In order to prevent these attack, network must distribute security to the very edge of the network. In this way, the network refuses access to unauthorized users and unauthorized traffic.

Network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks. Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with an outdated protocol analyzer. In other cases, network management involves a distributed database, autopolling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. Well-known network management protocols include the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP).

## 4.8.1 ISO Network Management Model

The ISO has contributed a great deal to network standardization. Its network management model is the primary means for understanding the major functions of network management systems. This model consists of five conceptual areas.

### 4.8.1.1 Performance Management

The goal of performance management is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization. Network congestion affects the performance of the VPN and other mission critical applications. To provide reliable and quality service, traffic management policies require to be defined to allocate bandwidth for inbound and outbound traffic, based on, relative merit or importance, the performance of mission critical and other high priority applications without “starving out” lower priority applications. **:** Rate control and queuing are two primary means of traffic control. Rate control was designed to smoothen typically bursty TCP traffic between connections, providing a method of bi-directional traffic control. The purpose of rate control is to reduce the transmission rate during periods of congestion.

Rate control identifies traffic flows according to such variables as source address, and port number. Based on this information, the rate control mechanism tweaks such variables as the TCP window, which determines how much a data system can send at a given point of time.

The receiving device initially establishes the TCP window size to tell the sending device how much room is available in its buffer. This information is included in each TCP acknowledgement. Rate control mitigates the problem of buffer overflow, which can be induced by excessive retransmissions.

Ensuring proper window size can be tricky. If the window size is too small, latency will ensue. If the window is too large, packets may be dropped and repeatedly retransmitted, inducing buffer overflow.

#### 4.8.1.2 Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on the network operation of various versions of hardware and software elements can be tracked and managed.

#### 4.8.1.3 Accounting Management

The goal of accounting management is to measure network utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of network access across all users.

As with performance management, the first step towards appropriate accounting management is to measure the utilization of all important network resources. An analysis of the results provides an insight into current usage patterns, and usage quotas can be set at this point. Some correction, of course, will be required to reach optimal access practices. From this point, ongoing measurement of resource use can yield billing information as well as information used to assess continued fair and optimal resource utilization.

#### 4.8.1.4 Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

Fault management involves first determining symptoms and isolating the problem. Then the problem is fixed and the solution is tested on all-important subsystems. Finally, the detection and resolution of the problem is recorded.

#### 4.8.1.5 Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem, for example, can monitor users logging on to a network resource and can refuse access to those who enter inappropriate access codes.

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to any network resource is inappropriate, mostly because such users are usually company outsiders. For other (internal) network users, access to information originating from a particular department is inappropriate. Access to Human Resource files, for example, is inappropriate for most users outside the Human Resources department.

Security management subsystems perform several functions. They identify sensitive network resources (including systems, files, and other entities) and determine

mappings between sensitive network resources and user sets. They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources.

#### 4.8.1.5.1 Firewall

The Internet, like any other society is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's wall with spray paint, tearing their mail boxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. The only way to completely protect the network from attacks via the Internet is not to provide access. Since this is not a practical reality, firewall is installed to keep the jerks out of the network while still letting one get the job done. A firewall is a system or group of systems that enforces an access control policy between two networks, i.e., Internal network (Intranet) and the external network such as Internet. The firewall can be thought of as a pair of mechanisms one of which exists to block traffic, and the other exists to permit traffic. Firewall can act as " ambassador " to the Internet. Firewalls are configured to protect against unauthorised interactive login from the "outside" world.

The firewall controls access between the internal network and the Internet by performing the following functions.

The firewall does not allow any direct connection between the internal network, and the external network. It directs all traffic to application gateways which give hosts reliable access to a wide variety of services on the Internet. The grant or denial of access to these services depends on the security policy specified in the system. By also installing a proxy server software on the Firewall server, it is possible to locally cache Web pages accessed frequently to facilitate speedy access

The firewall allows one to limit access to authenticated users from the internal network or from the external network or from both the directions.

The firewall acts as an external access point for mail and other services such as the Domain Name Services (DNS).

The firewall logs all connections, whether successful or not. It also logs all other significant events and produces a report based on these logs.

The firewall alerts one to any suspicious activity by using predefined alarms to detect and give warning of unusual or hostile activity.

#### 4.8.1.5.1.1 DHCP

DHCP is a method of automatically assigning a TCP/IP address from a pool of addresses to a requesting client. DHCP eliminates the need to manually assign static IP addresses. Implementing DHCP client and server features in the firewall significantly eases deployment into cable and digital subscriber line (DSL) broadband environments, where static IP addresses can be costly and cumbersome to maintain.

***4.8.1.5.1.1.1 DHCP Client:*** Support for DHCP client allows the firewall to dynamically acquire an untrusted interface's IP address, netmask, and optionally the default route from a DSL or cable Internet service provider (ISP). This feature is required when a firewall is directly connected to a DSL or cable modem/router.

***4.8.1.5.1.1.2 DHCP Server:*** The firewall can provide DHCP services for hosts located on the trusted network, allowing it to automatically assign IP addresses to machines that are configured for dynamic addressing.

## 4.9 INTRANET

The Internet has introduced a new level of security risk, it is now much harder to protect proprietary information and sensitive data from unauthorised access. Once connected to the Internet, an organisation data may be subject to theft, corruption or loss. This has led to the evolution of INTRANET. An Intranet can be defined as a protected internal network using Internet technology to provide cheap and effective access to information within an organisation. Geography becomes immaterial, and Intranets spans continents and; links global corporations together with the information needed to compete in today's economy. Intranet can be wholly internal with no outside links at all, or with links to the outside world through a protective barrier known as Firewall.

The Intranet working is about information individuals with information democracy in an organisation empowering individuals so that the job can be done better and effectively.

**Self Check Exercise**

1) What is the Network Operating System?
2) What are the goals of configuration management?
3) What are the goals of fault management?
4) What are the goals of security management?

.....

.....

.....

.....

.....

.....

## 4.10 SUMMARY

A network operating system (NOS) is a collection of software and associated protocols that allows a set of autonomous computers, which are interconnected by a computer network, to be used together in a convenient and cost-effective manner. Most modern network operating systems support TCP/IP protocols. So heterogeneous computers/operating systems (Windows NT Operating System, IBM mainframe, Unix systems, Open VMS System) can be interconnected easily. A variety of universities, Government agencies and computer firms are connected to an Internet-work, i.e., Internet which follows the TCP/IP (Transmission Control Protocol/ Internet Protocol). In addition to the TCP/IP, most of the applications

people use with the Internet also have their own protocols and are used for different purposes such as:

- Simple Mail Transfer Protocol (SMTP) defines a straight forward way to move E-Mail between hosts.
- Network File System (NFS) allows a computer to use disk space and files on another computer over a TCP/IP connection.
- Hyper Text Transfer Protocol (HTTP) is a standard method for transmitting information through the Internet. HTTP and its sibling standards, the document mark-up language known as Hyper Text Markup Language (HTML) have done more than anything to make information exchange accessible to the masses and have been the principal contributing factor in the explosive growth of the Internet.

Network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

## 4.11 ANSWERS TO SELF CHECK EXERCISES

1) A network operating system (NOS) is a collection of software and associated protocols that allows a set of autonomous computers, which are interconnected by a computer network, to be used together in a convenient and cost-effective manner.

2) To monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

3) To detect, log, and notify users of network problems and automatically fix then problems to keep the network running effectively.

4) To control access to network resources according to local guidelines so that the network cannot be sabotaged and so that sensitive information cannot be accessed by those without appropriate authorization.

## 4.12 KEYWORDS

**UDP (User Datagram Protocol)** **:** If reliability is not essential, UDP, a TCP complement, offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like IP).

**Datagram** **:** A method of sending data in which parts of the message are sent in random order. The recipient machine has the task of reassembling the parts in the correct sequence. The datagram is a connectionless, single packet message or item of data that can traverse a network

at OS I Level Three, the Network Layer. It typically does not involve end-to-end session establishment or delivery-confirmation acknowledgment. In addition to the information within the datagram, there is a destination network address and usually a source network address.

## 4.13 REFERENCES AND FURTHER READING

Optimizing Web Performance, Express Computer, December 9, 1996

Rupley Sebastian, The XML Infusion, PC Magazine, December 5, 1998

A business guide to web publishing, Information Communications World, July, 1996.

Dr. Alok R Chaturvedi, Dr Hemant K Jain, Putting Client/Server computing to work, Tata Consultancy Services.

Network Security: Private Communication in a Public World, by Charlie Kaufman, Radia.