UNIT 1 WINDOWS 2000 NETWORKING

Structure **Page Nos.**

1.0 INTRODUCTION

Windows 2000 is a network operating system with built-in support for peer-to-peer and client-server networking. The focus of a network operating system (NOS) is on use of remote services and resources existing in a networked computer system. In distributed operating system, the focus is on effective utilisation of resources in distributed computing environment.

Windows 2000 consists of 4 separate products.

- ***Windows 2000* Professional**
- ***Windows 2000* Server**
- ***Windows 2000* Advanced Server**
- ***Windows 2000* Data Center Server**

Following is a list of features for *Windows 2000* network support:

- It has an integrated **support for network protocol** like TCP/IP and IPX/SPX.
- It **supports dial up networking** (that facilitates mobile users to connect to a computer that is running on *Windows 2000* platform).
- *Windows 2000* server incorporates **Microsoft's Internet Information Server (IIS)** that is a secure web server to host Internet.
- It supports a set of security features which were not there in earlier versions of windows.

In this unit we will explore the issues related to networking support in Windows 2000-operating system.

1.1 OBJECTIVES

After going through this unit you should be able to:

- describe Windows 2000 operating system architecture;
- describe peer-to-peer networking support in Windows 2000;
- describe Windows 2000 domains;

- identify protocols supported by Windows 2000;
- distinguish between FAT16 and FAT 32 file systems;
- how to share folders in Windows 2000;
- describe Distributed File System, and
- describe support of network printing in Windows 2000 environment.

1.2 WINDOWS 2000 OPERATING SYSTEM ARCHITECTURE

CISC (Complex Instruction Set Computer) is a computer with a large number of instructions (complex) and constructs. Most of the NOS are based on CISC whereas early 80s designers recommended RISC (Reduced Instruction Set Computers) with simple instructions.

Windows 2000 is a portable operating system that is meant for CISC based machines (Complex Instruction Set Computing). CISC is a processor technology which is represented by a large set of instructions with variable formats. Major processor families used in the design of modern computer system are RISC, superscalar VLIW (Very Large Instruction Word), superpipelined, vector and symbolic processors. *Windows 2000* is always pre-emptive, which means that the high priority process gets executed first then compared to the low priority process. A complete Windows architecture is given in *Figure 1*.

Windows 2000 system is made of layers: It works in two modes:

- User Mode
- Kernel Mode.

User Mode is responsible for providing insulation of end users from kernel mode. *Windows 2000* user mode API subsystems are responsible for execution for different supporting system applications like win32 and POSIX. These subsystems have their own API's (Application Programming Interface) System data and hardware is accessible to kernel mode layer of *Windows2000.* Operating system itself runs in the kernel mode. Environment subsystems run in user mode. The lowest two layers nearest to the hardware use the kernel and Hardware Abstraction Layer (HAL) that is written in C and assembly language. Upper layers are written in C and are machine independent layers. Most of the drivers in Windows2000 are written in C or C++.

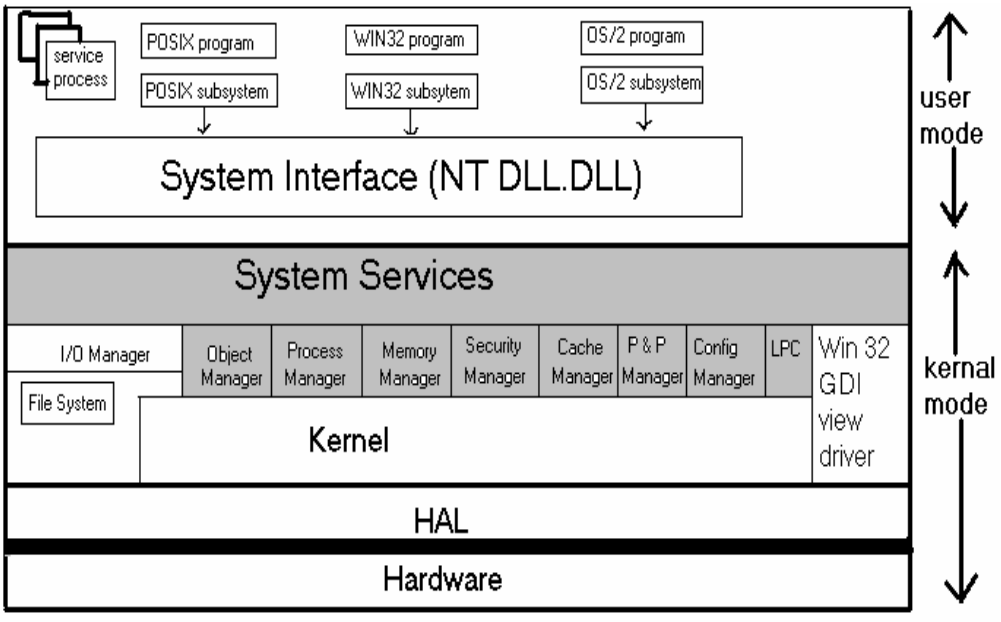

Figure 1: Windows 2000 layered architecture

HAL (Hardware Abstractor Layer)

The aim of HAL is to present the rest of the Operating System with an abstract view of hardware devices. It isolates the OS from platform specific H/W differences. The HAL makes each components such as bus system. DMA controller, computer, interrupt controller, system timer & memory module look the same to the kernel.

Kernel

The aim of the kernel is to make the rest of the Operating System machine independent, hiding all the low-level details. Accessing the hardware using HAL Kernel is responsible for generating higher-level abstractions.

Kernel also includes the code for thread scheduling. It also provides low-level support to two internal objects – control objects and dispatcher objects. The shaded area is the executive. The entire executive area is written in C language and is architecturally independent and can be easily ported to machine.

It consists of the following objects:

- Object Manager
- I/O Manager
- Process Manager
- Memory Manager
- Security Manager
- Cache Manager
- Windows/graphics manager
- Local Procedure Call Manager.

1. **Object Manager:** Creates, manages, and deletes W2K Executive objects and abstract data types that are used to represent resources such as processes, threads, and synchronisation objects. It enforces uniform rules for retaining, naming, and setting the security of objects. The object manager also creates object handles, which consist of access control information and a pointer to the object. W2K objects are discussed later in this section.

2. **I/O Manager:** Provides a framework through which I/O devices are accessible to applications, and is responsible for dispatching to the appropriate device drivers for further processing. The I/O manager implements all the W2K I/O APIs and enforces security and naming for devices and file systems (using the object manager).

3. **Process Manager:** Creates and deletes objects and tracks process and thread objects.

4. **Memory Manager:** Maps virtual addresses in the process's address space to physical pages in the computer's memory.

5. **Security Manager:** Enforces access-validation and audit-generation rules. The W2K object-oriented model allows for a consistent and uniform view of security, right down to the fundamental entities that make up the Executive. Thus, W2K uses the same routines for access validation and for audit checks for all protected objects, including files, processes, address spaces and I/O devices.

6. **Cache Manager:** Improves the performance of file-based I/O by causing recently referenced disk data to reside in main memory for quick access, and by deferring disk writes by holding the updates in memory for a short time before sending them to the disk.

7. **Windows/graphic manager:** Creates window oriented screen interface and manages the graphic device.

8. **Local Procedure Call Manager:** Enforces a client/server relationship within a subsystem in a manner similar to remote procedure call facility used for distributed application.

Minimum hardware requirements for W*indows 2000* are 32-bit Pentium 133 MHz processor, 128 MB RAM, 500 MB or more of disk space to set up Windows 2000.

1.2.1 Peer-To-Peer Network

MS Windows 2000 is an ideal Operating System for peer-to-peer networking. In a peer-to-peer network, computers work independently, providing various services like:

- Each computer can have its own separate user accounts.
- Sharing of resources (folders, printers etc.) is possible.
- Each computer is responsible for managing its security.
- Easy set up for the network.

On a peer-to-peer network, workstations communicate with one another through their own operating systems. Files, folders, printers, and the contents of entire disk drives can be made available on one computer for others to access.

Here is a simple peer-to-peer network (*Figure 2*)

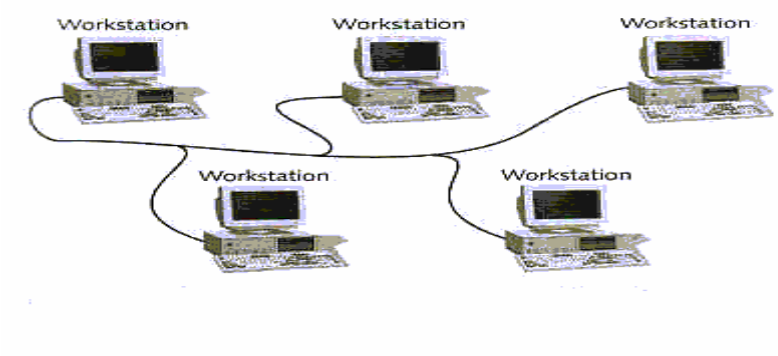

Figure 2: Peer-to-peer Network

1.2.2 Domains

A domain is a collection of accounts representing network computer uses, and group of users all maintained in a control security database for care of administration.

In Windows 2000, *domain* is a collection of computers where a server computer referred to as a *Domain controller* is responsible for the management of security for the entire network. This type of logical grouping is desirable for corporate application. Computers of a domain network have local user accounts, but are dependent on a centralised information store called as Active Directory Service. Thus Active Directory in Windows 2000 provides a centralised control.

Domains add several interesting features to Windows 2000 functionality.

- Centralised storage of user information.
- Each domain has domain controller associated with it. In Windows NT, domain controllers are either BDC or primary domain controller. In Windows 2000 there is only one type of domain controller.
- Extension of the existing network becomes easy.

- In Windows 2000 Active Directory unites namespace of internet with window NT directory services since Windows 2000 domain naming uses DNS (Domain Name System).

What is DNS, conceptually, the internet is divided into several domains (e.g., gov, edu, com, net, etc.), where each domain covers many hosts. Each domain is partitioned into several domains and these are further partitioned. The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing the naming scheme. It is primarily used for mapping host names and e-mail destinations to IP addresses.

While creating a Windows 2000 domain, the DNS should be executing and properly configured on the corresponding machine. If in case, DNS is not running, on creation of a domain controller, it is automatically installed later. Thus domain provides Windows 2000 with a grouping mechanism where not only accounts but also network resources are grouped under a single domain name.

Joining a Domain

Windows 2000 has **"Join A Computer To The Domain"** permission for those computers that wish to be a part of Domain. By obtaining this permission, an account is created for that computer. It is like a class of objects, where all the objects of that class are of the same type. The objects type may vary from users to computers. Active Directory Service provides a hierarchy to various resources stored in domain. A Domain has information about the objects it contains. It provides the network with a secure boundary.

1.2.3 Network Protocols

Protocol refers to a set of rules that facilitate communication across a network. A network application does not directly interact with the underlying network hardware; rather it interacts with protocol software that follows the rules of a protocol.

Windows 2000 include support for following different protocols through various layers:

1. TCP/IP
2. IPX/SPX
3. Net BIOS Enhanced user Interface (NETBEUI)
4. Data link control (DLC)
5. ATM (Asynchronous Transfer Mode)
6. AppleTalk
7. Infrared Data Association (IrDA).

Default protocol in Windows 2000 is TCP/IP. Since TCP/IP is the universal protocol of the Internet, thus enabling access to Internet resources. TCP/IP facilitates communication over a network that is otherwise a collection of computers with different architecture and operating systems. Two commonly used Windows 2000 troubleshooting utilities for TCP/IP are Ping and IpConfig.

The **advantages** of TCP/IP are:

- Designed for routing. (IP) and end-to-end data delivery (TCP)
- Is the most used protocol of Internet.
- Compatible with standard networking tools.
- Facilitates communication among diverse networks and network operating systems.
- Enables the use of DHCP and WINS.
- Compatible with Microsoft Windows Sockets.

ATM is a protocol that is able to provide voice, data and video services across wide area networks.

NWLink is MS equivalent of Novell Netware.

IPX / SPX (Internet packet exchange / sequenced packet exchange)

Only TCP/IP is accessible to Windows 2000 networking running Active Directory Services, not NWlink or NetBEUI.

NetBEUI is a kind of legacy protocol that is used to provide accessibility with existing network (small network) that is already using NT.

Appletalk: Apple Computer Corporation developed this protocol suite and is included in Windows 2000 so as to provide compatibility with Apple Machinist clients. In addition because of Appletalk Windows 2000 can function as a router and a dial up server.

DLC (Data Link Control) protocol originally developed for IBM mainframes is required for printers and other peripheral devices installed on a network.

Ir DA is a collection of bi-directional wireless infrared based protocols (that spans a short range). It facilitates communication among multiple device types like camera, printers and PCs.

IP Addressing

The IP address format is called the **dotted decimal notation** address.
It is 32 bits long and contains four fields, consisting of decimal values representing 8-bit binary octets. For example, an IP address might be 198.60.204.2.

A unicast transmission is one in which one packet is sent from a server to each client that requests a file or an application.

A multicast means that the server is able to treat all the clients as a group and send one packet per transmission that reaches all the clients. It saves the bandwidth of a channel.

A **subnet mask** is used to divide a network into subnetworks to meet addressing requirements with limited availability of address.

Static and Dynamic Addressing

Each server and workstation needs a unique IP address, either specified at the computer or obtained from a server that assigns temporary IP addresses.

Static addressing involves assigning a dotted decimal address that is each workstation's permanent, unique IP address.

Dynamic addressing automatically assigns an IP address to a computer each time it is logged on.

Dynamic addressing method uses the **Dynamic Host Configuration Protocol (DHCP)**, which is supported by Windows 2000 Server for dynamic addressing. It provides an enhancement to TCP/IP. DHCP in addition to permanent addresses assigned to computers that run a server it automatically allocates an address. Yet a DHCP does not assign an address permanently, rather it specifies a lease for the address use.

In Windows 2000, configuring TCP/IP using DHCP has many advantages. On Windows 2000 servers that provide Internet communication, when one is configured as a DHCP server, **Windows Internet Naming Service (WINS)** is also installed so that the Windows 2000 Server is both a DHCP and a WINS server.

Domain Name System provides automated mapping between computer names and IP address. Conversion of a domain name into an equivalent IP address is referred to as name resolution, and domain name is said to be resolved to an address.

☞ Check Your Progress 1

1) What is the purpose of a directory service in Windows 2000?

……

……

……

2) In what mode does the console run?

……

……

……

3) How does a domain differ from a workgroup?

……

……

……..

1.2.4 File Services

Windows 2000 provides read and write support for NTFS, FAT 16 and FAT 32 file systems. FAT is designed for small disks and simple folder structure. Windows 2000 supports both FAT 16 and FAT 32 file system and FAT is designed for small disks and simple folder structure.

A FAT 16 partition is divided into 512 byte sectors and disks have files in dusters in the default cluster size dependent on partition size and can range from 8 sectors to 128 sectors. FAT 32 can support partition up to 2047 GB in size. The major advantage of FAT 32 over FAT 16 is larger partition sizes.

NTFS (NT File System)
Windows2000 supports a new version of NIFS, i.e., NTFS version 5.0.
This new version of NTFS is better than in terms of reliability and better performance.

NTFS 5.0 includes the following features:

- All of the new features of Windows 2000 Active Directory Services.
- Storage features like reparse points.
- Features for Software Management.
- Enhanced security features for servers, which provides an authentication mechanism to users before they can actually gain access to network resources.
- It supports CDfs;

The fundamental unit of disk allocation in NTFS is cluster that comprises multiple sectors.

Disk Storage Types:

In Windows 2000 two kinds of disk storage are possible:

- Basic storage
- Dynamic storage.

Disk should be initialised with a storage type before data could be stored on it. Either of the two storage types can be used on one disk. But in a system with multiple disks both storage types can be used. Basic disk storage is the default storage type for Windows 2000. All disks are basic until converted to dynamic. Disks can be managed on local and remote networks. Only Windows 2000 has support for Dynamic storage, which can be resized unlike basic storage type.

Basic disk is divided into partitions. Disk partition can be primary or extended and they function as disks in their own entirety.

Dynamic disk is divided into volumes. Volumes can be simple, spanned, mirrored, striped or RAID-5. Only computers running Windows 2000 can access dynamic disks.

File Replication Service (FRS)

Another file service feature supported by Windows 2000 is File Replication Service (FRS). It is so configured that it automatically starts on all domain controllers and manually on all standalone sectors. Its automatic file replication service is responsible for the copying and maintenance of files across network.

Two kinds of replications are possible:

- Intrasite Replication
- Intersite Replication.

Sites are subnets comprising well-connected computers. Any portion of the network, subnet, is a site.

1.2.5 Shared Folders

The mechanism by which resources across a network are accessible is referred to as sharing. Only those users who have been granted access to the shared folders can use files of a shared folder. By default any user who **logs on** to a computer has access to the shared folders on that computer.

A shared folder data may range from personal to corporate data. A shared folder Permissions may vary depending upon the kind of data a folder contains read, change, and full control permissions.

Shared folders permissions exhibit the following features:

- They provide a **security boundary** not detailed security, since shared folders permissions hold true for the entire folder and not to individual files.
- On a FAT system it is the only way to **secure network**.
- Full control is the **default permission** for a shared folder.

Permissions for a shared folder may be granted or denied to users or to groups. Also if a user is denied permission for a shared folder then even if s/he is member of a group that is granted shared access permissions for the folder, s/he cannot access the folder.

Sharing a folder:

When a folder is shared it can be given a share name, comments can be added to it for the description of the contents of the folder etc.

1.2.6 Distributed File System

Another Windows 2000 file service is *Distributed File System;*
It is an efficient and easy way to access shared folders across the network;
Files are arranged in a hierarchy in DFs. It is a logical tree structure, comprising DFs root and DFs links. In DFs resources from various locations, servers are shared in DFs root.

Features of Windows 2000 DFs:

- Facilitates network administration
- Simplifies network navigation
- Provides a hierarchical logical organisation for shared folders across different computers on a network.

Two types of DFs roots can be implemented on Windows 2000 Servers:

- Standalone DFs roots
- Domain DFs roots.

In standalone DFs roots, DFs is stored on a single computer. It has no support for fault tolerance in case the computer that stores the DFs topology fails. Domain DFs root writes the DFs topology to Active Directory. It supports file duplication in case of failure. Here DFs links point to multiple copies of the same shared folder. When changes are made to a DFs link that is a part of a domain DFs root, the changes are automatically reflected to other members also.

1.2.7 Print Services

Windows 2000 has support for networking printing. Thus, it facilitates printing from any computer in the network. Also printer can be managed from any computer by having just a web browser installed on that computer. Using *Windows 2000* various components with different Operating Systems/platforms can send jobs for printing.

For network printing **basic requirements** are:

- Sufficient memory (RAM)
- Sufficient disk space
- A server computer.

Remote network printing, non-remote local printing and non-remote network printing is supported by *Windows 2000* networking printing. TCP/IP is the default network protocol for *Windows 2000* in use by many network-printing devices. Printers on a network can be shared if printing jobs are more on the network that an unshared printer is unable to handle.

In order to share an unshared printer on a network

In the Printers Windows.

1. Click the properties dialog box and then click on sharing tab.
   This sharing tab acts as an interface for sharing a printer, on the network.

Managing Printing Jobs

Windows 2000 facilitates job management that primarily involves restarting, resuming, pausing and cancelling printing jobs if a problem arises while printing.

Another interesting feature in Windows 2000 is that the user manages print job by setting printing priorities and printing time, provided the user has been granted manage Documents permission for the desired printer.

In a network *Windows 2000* facilitates managing network printers even with Web browsers. Thus eliminating the need for having installed *Windows 2000* on every computer.

Role of a Printer Driver

In a network some computers cannot access the printer installed over the network. This is due to the fact that printer may by attached to a computer that is not having *Windows 2000* installed on it.

Since *Windows 2000* has all the required printer drivers installed within it and printer drivers are responsible for the creation of special printer file that carries requisite information the printer needs. *Windows 2000* always keep the drivers up-to-date.

☞ Check Your Progress 2

1) In a multi-user environment while printing, how can the possibility of a user ending up with a wrong document be avoided?

……

……

……

2) Can a single document be redirected on a network?

……

……

……

3) When do DCHP clients try to renew their leases?

……

……

……

4) Can moving and copying files and folders between disk volumes change their compression state?

……

……

5) What type of data is replicated by FRS?

……

……

……

6) What is the default permission when a partition is formulated with NIFS?

……

……

……

1.3 USING THE MAPPED DRIVE

Windows 2000 allows the user to assign a drive letter to a share network resource **that may be a printer, folder or a drive using the mapped drive. A file server or workstation shares a mapped folder or drive on the network.**

- By default, Windows attempts to reconnect any mapped drives the next time user logs on. If you do not want this to happen, click to clear the **Reconnect at Logon** check box.
- By default, you are connected to the other computer with the logon details that you are currently using. If you want to use other credentials, click **Connect using a different user name**, and then type the appropriate user name and password to connect to this network resource.
- The mapped drive that we create is visible in the Folders, in Windows Explorer, along with all the other drives on our computer. Files in the shared folder can be accessed with any program on our computer by using the mapped drive letter.

To assign (map) a drive letter to a network computer or folder

1. Click **Start**, point to **Programs**, and then click **Windows Explorer**.
2. On the **Tools** menu, click **Map Network Drive**.
3. In **Path**, type the path to the resource you want. For example:
   \\computername\foldername
   If a password is required, Windows prompts you.

Notes:

- You can also right-click **My Computer** or **Network Neighbourhood**, and then click **Map Network Drive**.
- To map to a computer or folder you have used recently, click the arrow to the right of **Path**, and then click the resource you want.

1.3.1 Printing a Mapped Drive

Once the letter has been assigned to a drive, after selecting a file from the drive, pull down the File menu, choose the Print option. Also by right click any document icon and choose Print.

1.3.2 Disconnecting a Mapped Drive

To disconnect a mapped drive

Click **Start**, point to **Programs**, and then click **Windows Explorer**.

1. On the **Tools** menu, click **Disconnect Network Drive**.
2. In **Drive**, click the resource that you want to remove, and then click **OK**.

Note:

- You can also right-click **My Computer** or **Network Neighbourhood**, and then click **Disconnect Network Drive**.

1.3.3 Viewing Directory Information

From the My Computer window,

1. In order to view the contents of a drive double click on a drive icon.
2. Then select a folder within that drive and double click on it and keep moving down till the desired folder is found.

1.3.4 Creating a shared folder

To specify a path

1. Type the drive letter followed by a colon (:) and back slash (\). See the examples in **Note**.

2. Type the names of the folders and subfolders that contain the file, typing backslashes before each folder name.
3. Type the name of the file. A backslash should precede the file name.

If you use file names that contain spaces or exceed eight characters in length, enclose the path in quotation marks.

Note:

- You can specify a path from within a program, from **Run**, or from the MS-DOS prompt:
    - To specify the location of Disk Defragmenter, which is located on drive C in the Windows folder, type:
    - c:\windows\defrag.exe
    - To specify the location of a document named List.doc, which is located in the l1 folder within the Events folder on drive C, type:
    - c:\events\l1\list.doc
    - To specify the location of a bitmap named Canyon, which is located in a shared folder named Scenic on a computer named Pictures, type:
    - \\pictures\scenic\canyon.bmp

Or, map the shared folder to a drive (for example, drive D), and then type: d:\canyon.bmp

1.3.5 Logging Off a Client

When one is finished working on a shared computer on a network, or when one wishes to log as another user:

1. Press Ctrl+Alt+Del and choose log off option
2. Click Yes when asked if currently an application is running, thus giving the user an opportunity to save any open files.

When the entire process is complete, the machine is available for a new logon.

Note: Windows 2000 may restrict a user from logging on even if the user is entering the correct password.

Such a situation arises when the user has two accounts with the same name but with different passwords one on the network and other on the local computer. And the user may have selected the wrong location.

The *solution* to this problem is that click on the option button to make sure the correct location is selected in the log on list.

1.4 A FEW IMPORTANT FACTS ABOUT WINDOWS 2000 USAGES

1. If your computer is on a local network but you have a local account on your computer that gives you permission to make changes, log off from the network and then log on again to the local computer. Enter your user name and password for the local computer account, and enter the computer name in the Domain box. You would be able to make changes to the computer that you were not allowed to make when you were connected to the network.

2. Folder windows are the gateways to your files and documents. Users folder windows can display all information and these windows can be customised.

3. Windows 2000 uses a single logon system – when you logon to a domain using an authorised user name and password you unlock access to all resources on the network.

4. The difference between logging-off and locking the computer is that Logging-off closes all programme and data files. In order to resume work you need to logon again and restart the entire programme. By locking the computers, however, you keep running programme and memory. When you return, by entering your password, you can resume work.

5. It is not possible to change the letters assigned to the drive that contain systems files or boot files. Also assigning the drive path instead of a letter works only if two conditions are true. First, the drive that contains the path you want to use must be formatted with NTFS, FAT 16 and FAT 32 will not work. Second, the folder path must be empty.

6. If your computer is part of domain, any member of the domain Administrator group is a member of Administrator group on your computer automatically.

1.5 SUMMARY

Windows 2000 consists of a family of four products namely Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Data Center Server. It is an object based operating system, supports networking and provides centralised control of data. It supports both type of networks: workgroups and domains. An important feature of Windows 2000 is its Active Directory Service that not only allows removing, adding or relocating users and resources but also completely segregates the physical structure of domain from its logical structure. And thus presents a layer of abstraction. Windows 2000 includes support for following different protocols TCP/IP, IPX/SPX, Net BIOS Enhanced user Interface (NETBEUI), Data link control (DLC), ATM (Asynchronous Transfer Mode), AppleTalk, Infrared Data Association (IrDA), Default protocol in Windows 2000 is TCP/IP. Since TCP/IP is the universal protocol of the Internet, thus enabling access to Internet resources. TCP/IP allows communication over a network that is otherwise a collection of computers with different architecture and operating systems. Two commonly used troubleshooting Windows 2000 utilities for TCP/IP are Ping and IpConfig. Windows 2000 supports two versions of FAT file systems: FAT 16 and FAT 32.It also supports NTFS. FAT originally was designed for small disks; FAT 16 can support partition up to 4 GB in size, while FAT 32 can support up to 2047 GB size partitions. The process by which resources across a network are accessible is referred to as sharing. Windows 2000 has support for shared folders. A shared folder data may range from personal to corporate data. Shared folders Permissions vary depending upon the kind of data a folder contains read, change, and full control permissions.

Distributed file system is an advanced file service in Windows 2000. Files are arranged in a tree hierarchy in DFs. It is a logical tree structure, comprising DFs root and DFs links. In DFs resources from various locations servers are shared in DFs root. Two types of DFs roots –standalone DFs root and domain DFs root. Windows 2000 has support for networking printing. It supports printing from any computer in the network. Printer can be managed from any computer by having just a web browser installed on that computer. Windows 2000 being a network operating system supports sharing of all the resources across the network.

Hands On

1. Your campus has installed an additional network and you are the network administrator for the new network. Your job is to configure the DNS naming scheme for both the networks new and the existing one. Both the networks are installed in different departments and operate independently but there needs to be a communication between the two. How should the DNS be configured between the two networks?
2. Try CMD rather than COMMAND to open Windows 2000 command line arguments.
3. Just like shared files and folders, try to hide the shared printer on Windows 2000 environment.
4. What will happen if instead of using a screen saver you try to lock your computer?

1.6 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) Since an Active Directory Service is essentially but a database of information about network resources-printers, computers etc. and so it provides services that make this information available to the user and the applications.
2) In author mode and is shown in console mode drop down list box.
3) A domain is a centralized repository of resources maintained by domain controller and is supported by Active Directory Services whereas a workgroup is a distributed directory maintained on each computer within the workgroup.

Check Your Progress 2

1) A separator page, if created, ably separates printed documents thus avoiding the risk.
2) No, only the configuration of the printer server can be changed so to send the documents to another printer; this change would redirect all documents on that printer. The currently spooled or active document cannot alone be redirected.
3) DHCPclients try to renew the lease when 50 percent of the lease has expired. if the lease is not renewed , the DHCP client would renew its lease with any other DHCP server after 87.5 percent of its current lease has expired.
4) Yes, moving and copying files and folders between disk volumes can change their compression state.
5) Data replicated by FRS is domain Dfs roots, Dfs links that are configured for replication only and Dfs roots.
6) The everyone group is granted full control permission. Default Permission is full control. Since all users are members of this group, so they all can access it.

1.7 FURTHER READINGS

1. www.microsoft.com web site for a detailed description of Windows 2000 environment
2. White paper for distributed file systems at www.microsoft.com
3. "*Operating System Concepts*", Silberschartz, Galvin and Gagne, Sixth Edition, John Wiley & Sons.