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++.

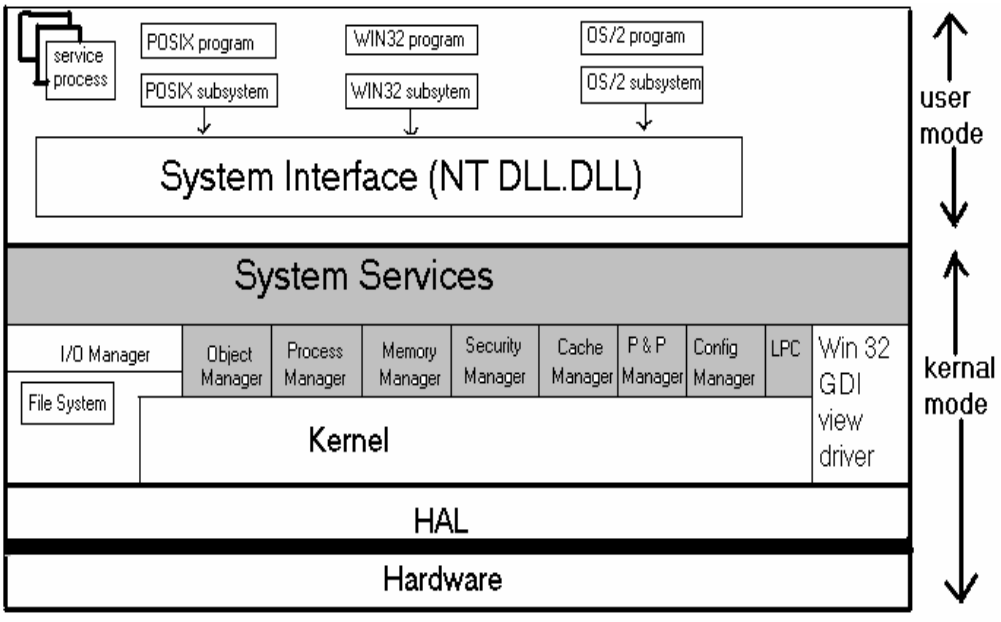

Figure 1: Windows 2000 layered architecture

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*)

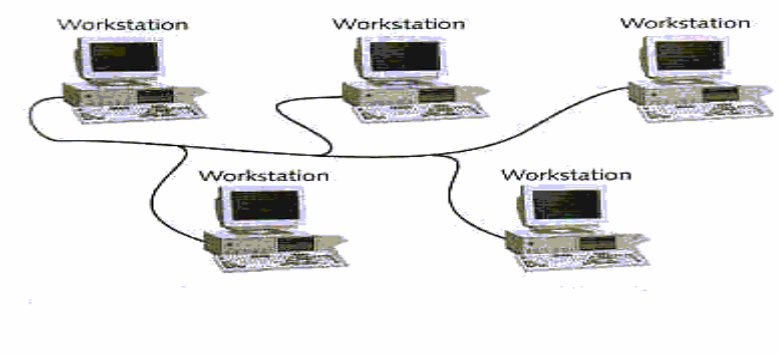

Figure 2: Peer-to-peer Network

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.

UNIT 2 MANAGING WINDOWS 2000 SERVER

Structure **Page Nos.**

2.0 INTRODUCTION

In the previous unit we examined the structure and basic networking support of Windows 2000. In this unit we will explain how to manage Windows 2000 server.

By default Windows 2000 restricts most system management features to specially privileged users called administrators. Unlike Windows 95 and Windows 98, most of the management tasks cannot be performed until the user is logged on using the administrator's account. As a part of the setup process, Windows 2000 creates a built-in account called Administrator and requires that the user may enter a password for that. Windows 2000 also creates a built-in group called administrator. Any user who is a member of this group can perform management tasks as well.

2.1 OBJECTIVES

After studying this unit you should be able to:

- describe Windows 2000 client & Server architecture;
- log onto the network;
- browse network resources;
- access network resources using My Network Places;
- map a drive letter to a network resource (a folder or a shared folder), and
- use Windows explorer.

2.2 USING WINDOWS 2000 SERVER AND CLIENT

Microsoft Windows 2000 Server is a more robust network operating system than Windows 95 or 98. A **server** is a single computer that provides extensive multi-user access to network resources.

Here is a diagram of a server-based network (*Figure 1*) .

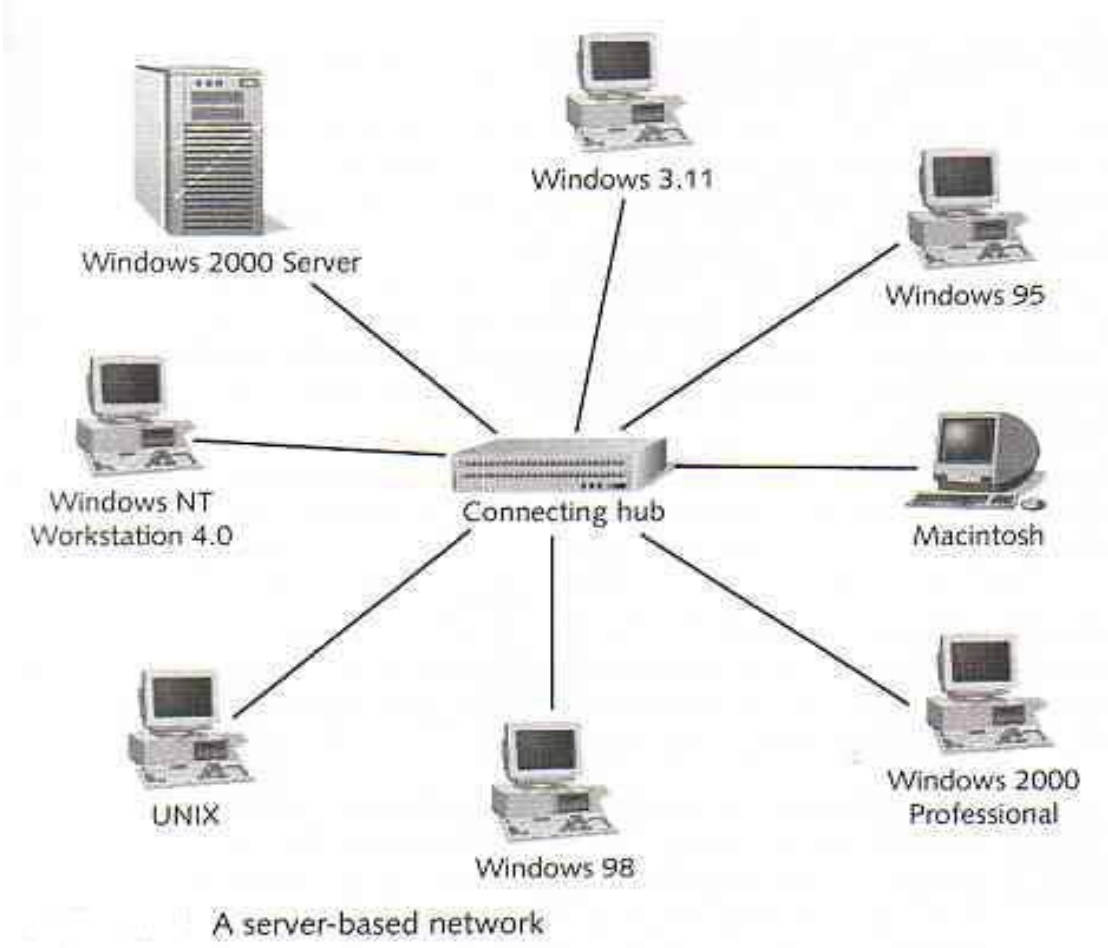

Figure 1: A Server-based network

Windows 2000 Server can provide the following advantages:

- Sharing of files among member computers.
- Sharing of printers and other resources.
- Centralised control and administration of resources.
- The server administrator can save time when installing software upgrades.
- Software applications can be shared among members of a client sever network.
- All computers can be backed up more easily.

Windows 2000 Server and Windows 2000 Professional Compared

The basic server version is called Windows 2000 Server, and Windows 2000 Professional is designed for workstations.

Windows 2000 Server offers services including:

- Virtually unlimited numbers of users simultaneously (optimally for 10 users).
- Active directory management.
- Effective network management.
- Web-based management services.
- Network-wide security management.
- Remote network access.
- Application services management.
- Network printer management through the Active directory.

2.3 LOGGING ONTO THE NETWORK

In Windows 2000 environment a user can log on either as a **local user** or a **domain user.**

Figure 2: Logging on the Window Screen

Domain User Account permits the user to log on to the domain and allows him to access resources on the network whereas a local user can log on to a local computer to be able to access resources on that machine.

Local User Account: Local user accounts are not replicated to domain controller, rather they are created in local machine security database.

By default a user has access to a domain via any other computer in that domain if it is a domain member. Then there are groups, which is a collection of user accounts. Individual users can be members of more than one group.

Windows 2000 supports two types of groups:

- Security Groups
- Distribution Groups.

Security groups are responsible for assigning access permission for resources.

Distribution groups are used for non-security related functions.

Now the actual log on procedure to enter the domain:

Windows 2000 by default assumes that the user wishes to log on as a local user. However in a networked environment in an organisational set up it asks for both user name as well as domain name.

In the Log On to Windows Dialog box as shown in *Figure 2* in the User name box type

Username_+@domainname :

Example: user1@domain2

Where user1 is the user name domain2 is the **domain name as shown in** *Figure 3* and ***Figure 4*** click on it. An expanded dialog box appears and then choose the **domain from log on to:** list box but remember if user name is entered with @ symbol in the user name box then **options** box will be grayed out at the end when the user wants to

log on as another user press ctrl+alt+del and choose log of option then logging off would be confirmed by displaying the **yes**. Click on it to confirm **logging off.** In the process windows shuts down all applications that are currently executing. After this the machine is available for log on. Windows 2000 has a built-in administrator account.

The following windows *Figure 3* and *Figure 4* adds new user, **user1** to the existing network:

Figure 3: User Basic Information Screen

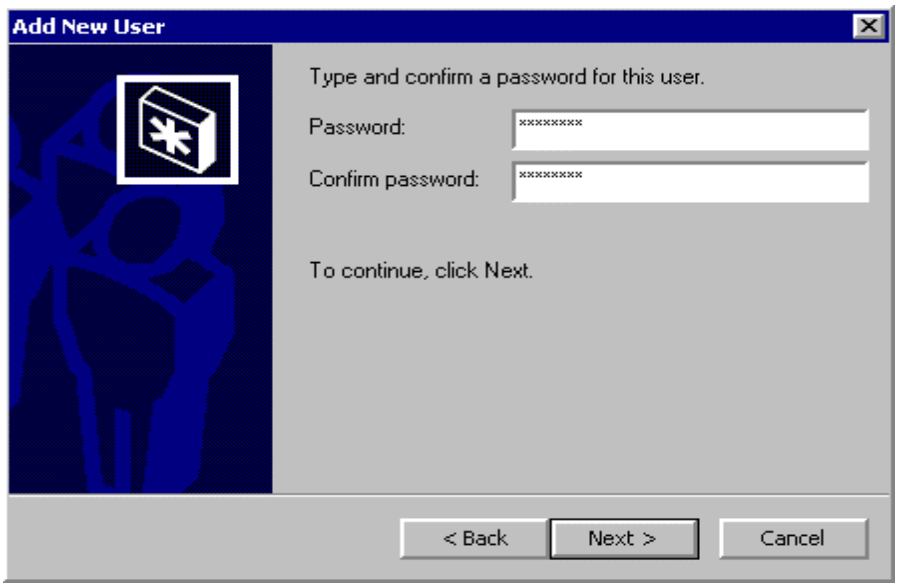

Figure 4: Add User Password Screen

Windows 2000 also supports built-in group accounts.

1. While creating a new user account with the wizard's help, select the Standard user option. With this option the user's account becomes a member of the power user group. Users of this group can participate in installation as shown in *Figure 5* and *figure 6* .

2. If the user selects Restricted User option, user account becomes member of built-in user's group.

Figure 5: Grant Access Level Screen

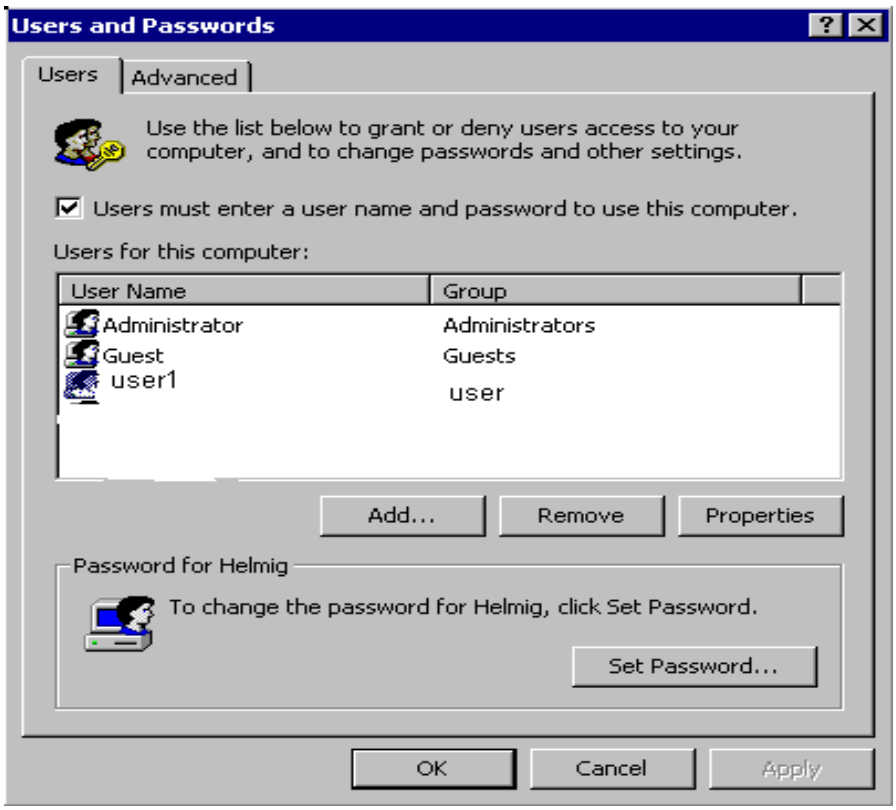

Figure 6: Change User Password Screen

You can view in detail the list of groups with each right/privilege:

The following set of windows add members to a group

While creating a new group, users can be added immediately to become a member of the group. But users can be added later to become a member of a group as well as in *Figure 7* and *Figure 8*.

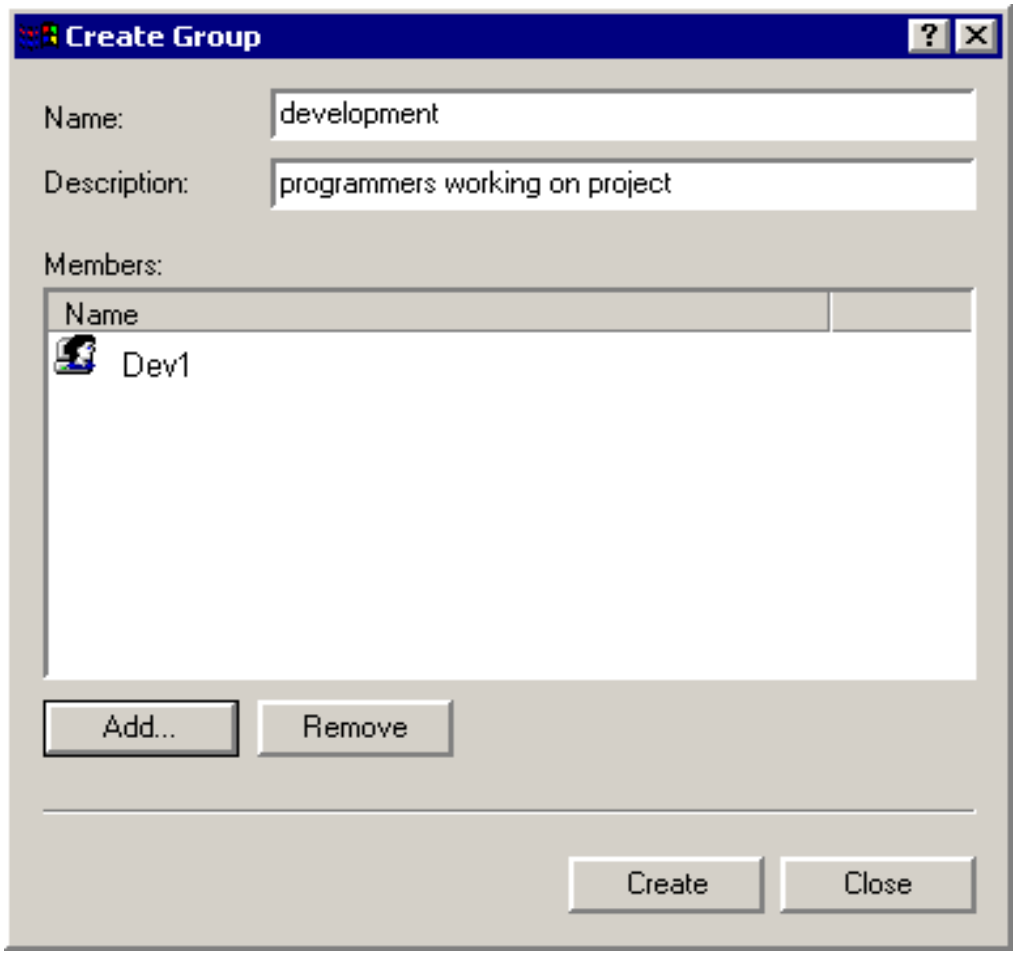

Figure 7: Create Group User Screen

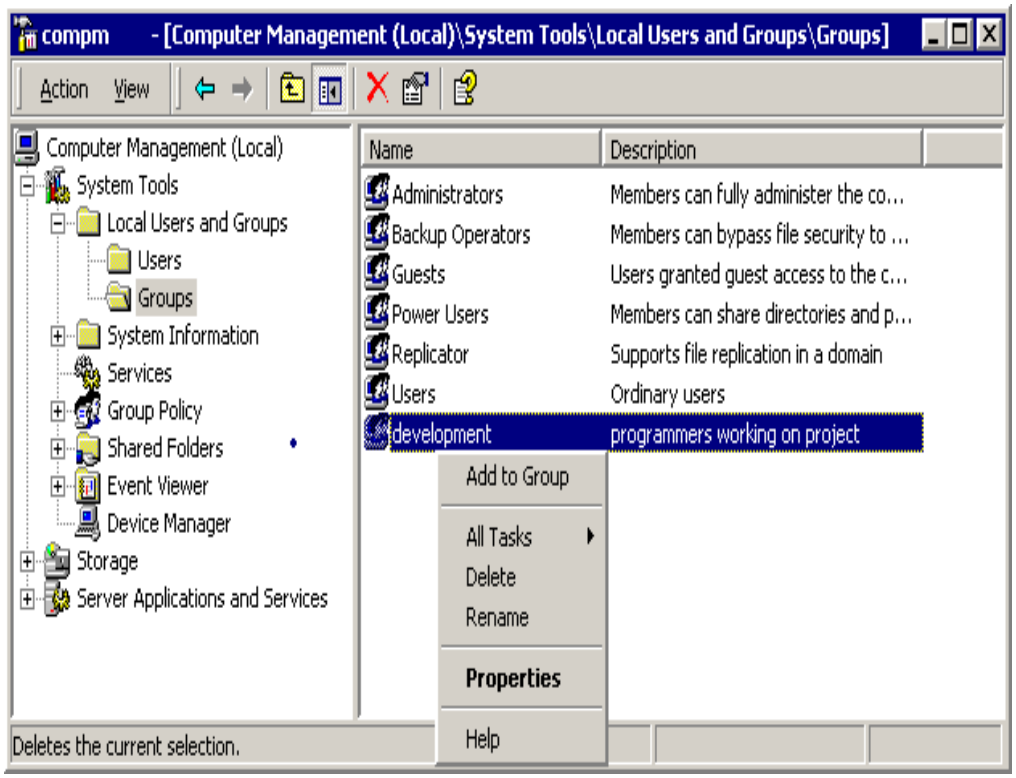

Figure 8: User Addition Screen

But to see in detail the permission/rights/privileges of a group, you need to "**drill down**" in the "***Group – Policies***" **4 levels down** as in *Figure 9*.

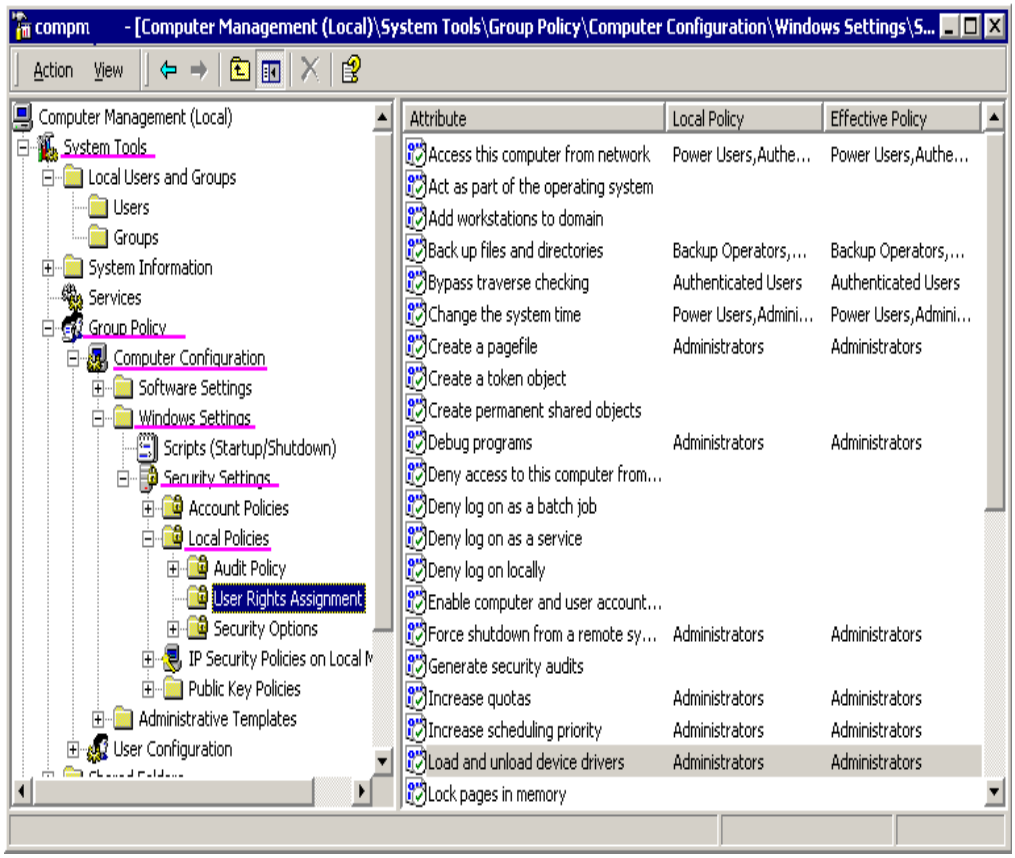

Figure 9: Detailed Permission Screen

For example, “regular users” do not have the right/permission/privilege to make backups.

To enable another group (one of the predefined or our own-defined groups) to have a right/privilege (like: make a backup), you need to add the group to the list: as shown in *Figure 10*.

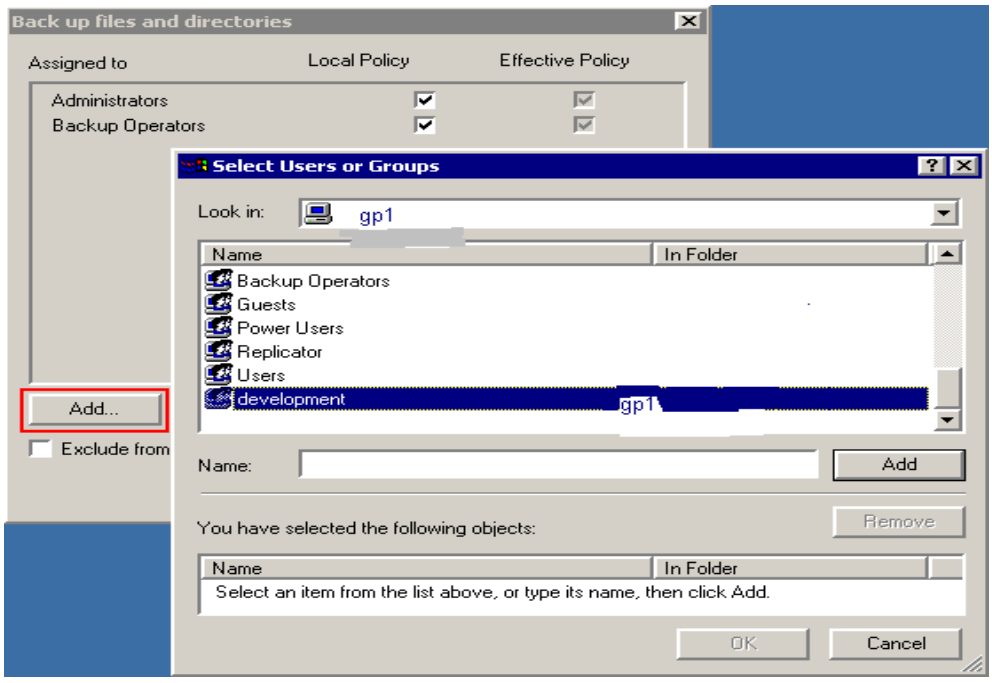

Figure 10: Printages/Permission Screen

2.4 BROWSING NETWORK RESOURCES

When installed, Windows 2000 creates a set of folders to store program and data files. Windows folders and subfolders correspond to DOS directories and subdirectories but system folders do not.

Some of the system folders are:

1. Desktop
2. My Documents
3. My Computer
4. My Network Places
5. Recycle Bin
6. Internet Explorer

Descriptions of these folders are given below:

Desktop 

The desktop includes:

My Documents, My Computer, and My Network Places system folders.
Here Files and folders can be saved and created.

If the user creates folders, save files on the desktop – then these are stored in Desktop render user's own user profile.

My Documents 

This icon is a short-cut of the actual folder that the user uses for data files.

My Computer 

This is responsible for the displaying of:

- All local drives
- Shared network drives
- Mapped drives
- Control Panel icon

This is a completely virtual folder, i.e., no file can be created or saved in this. My Computer folder is a system folder.

My Network Places 

This is another virtual folder; it is responsible for providing access to all the network resources. Here you find the list of rights/privileges for all the jobs on your system.

Job list includes:

- Accessing this computer from the Network
- Backup files and directories
- Restore files and directories (yes, it is a different right/privilege)
- Load and unload device drivers --> Configure hardware, reserved for Administrators.

You can view in detail the list of groups with each right/privilege of networked computers. It provides the same functionality as was provided by the Network Neighbourhood in Windows 95/98.

Recycle Bin 

This folder is used to store files that are temporarily deleted from the system and has options for permanent deletion or restoring of files to their original locations.

Internet Explorer 

Viewing Folders as Web Pages

Windows 2000 provides an opportunity to display each folder as a web page.

This feature can be activated/deactivated for all folders using the option Web View on General tab of the folder options dialog box.

If you check enable web content in folders then info pane is available at all times for all folders.

If a use windows classic folder is selected then only a simple list of icons can be viewed without web content.

Four special attributes are associated with every file and folder for controlled access

On new files that are created by users these four attributes are always off.
These special attributes are:

1. System
2. Archive
3. Read Only
4. Hidden

Windows Explorer

It is an all purpose system utility, it lets the user organise files in folders, allows for searching for documents and also data editing.

Windows explorer supports two views:

1. Single folder view
2. Two-pane explorer view.

Using the single folder view the contents of the current drive or folder can be viewed, whereas using two-pane explorer view all the drives, folders and resources on the user's computer and the network can be viewed in a tree structure. Two-pane view is also possible.

Arranging files and folders

Contents of folder window can be sorted by name, type, size or date. To sort files within a folder, pull down view menu and choose arrange Icons and choose any among the following options:

a. By name
b. By type

c. By size
d. By date

Even the width of folder panes can be changed by pointing to the vertical dividing line between the panes. When the mouse pointer changes to a two-headed arrow, click and drag.

2.5 ACCESSING NETWORK RESOURCES USING MY NETWORK PLACES

My Network places are the system folder. It includes icons for all those computers that are part of the network in our domain (Servers and workstation). In Windows 95 Network Neighborhood was there. Windows 2000 has ***Computer Near Me*** which is similar to network neighborhood of Windows 95.

1. The most convenient way to gain access to or to manage files folders that are stored on another computer on the network is using My Network Places folder.

2. But if the shared folder is in another domain, a user name and a password is required to access the machine's resources. Thus the easiest way to find shared resources on your network is via My Network Places.

In My Network Places Folder

1. Double click on Entire Network icon, then choose Search for the shared resource on a network.
2. After entering the name of the computer that contains the shared resource in computer Name Box, click Search now. Also on double clicking Microsoft windows Network icon you get to see all other computers and domains on your network.
3. Another icon is Computers Near Me icon. This icon is available only if the network is a workgroup not a domain.

Step wise short cut

Double clicking icons on My Network Places can be a tedious task, on large networks Windows 2000 provide a mechanism by which shortcuts can be created.

In order to create a short cut on My Network Places folder double click on add network place icon on Add Network places folder.

For shared computer use \\computer-name. Shows all shares that are available on a given computer.

1. FTTP server – shortcuts, user can browser for files on a server. Using FTP use ftp://server_name
2. Web folder (HTTP Server) – lets the user save files directly on web server. Using http://server_name
3. Shared folder or drive: use \\computer_name\share_name

Following windows (*Figure 11*) describe My Network places:

As shown in *Figure 11* From "***My Network Places"***, we find the equivalent of "*Network Neighborhood*" as "***Computers Near Me"***.(Note: if you make a logon to a domain server, there will be no "***Computer Near Me"*** displayed).

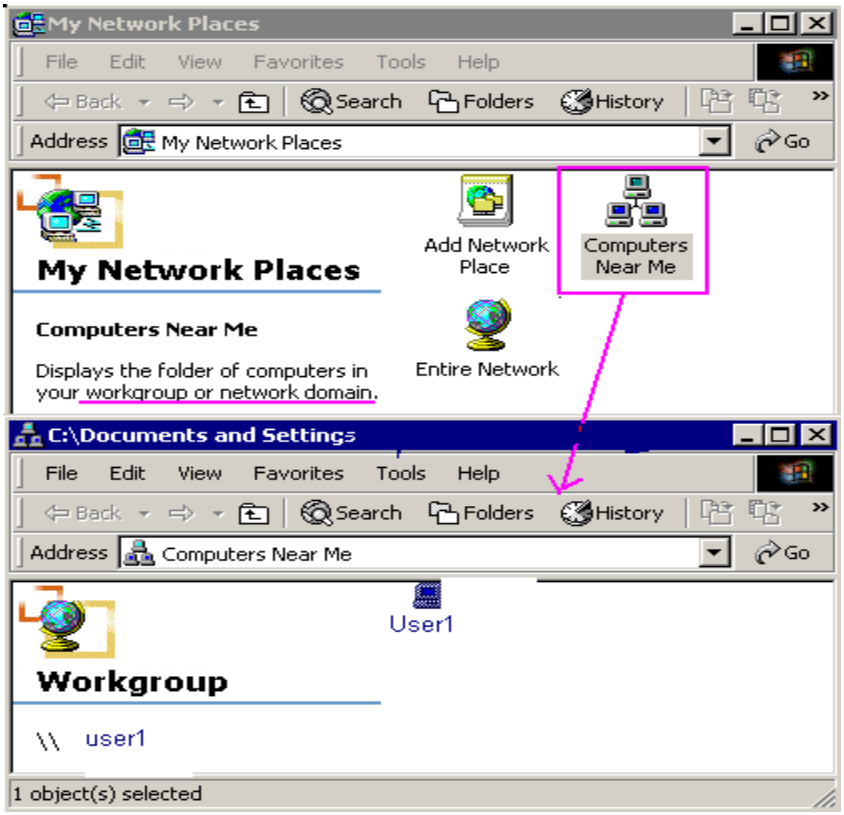

Figure 11: My Network Places

Searching for a particular workgroup (as shown in *Figure 12, Figure 13* and *Figure 14)*.

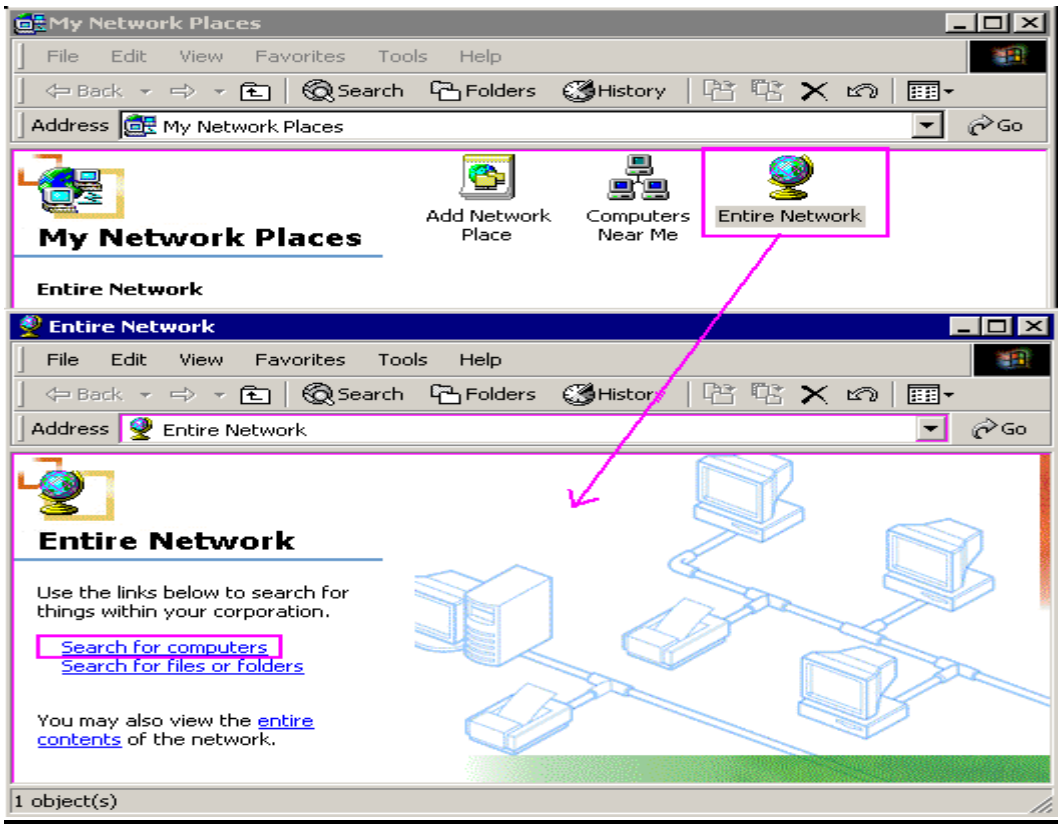

Figure 12: My Network Places Screen

Our search results give location, which is the workgroup only (as shown in *Figure 13*)

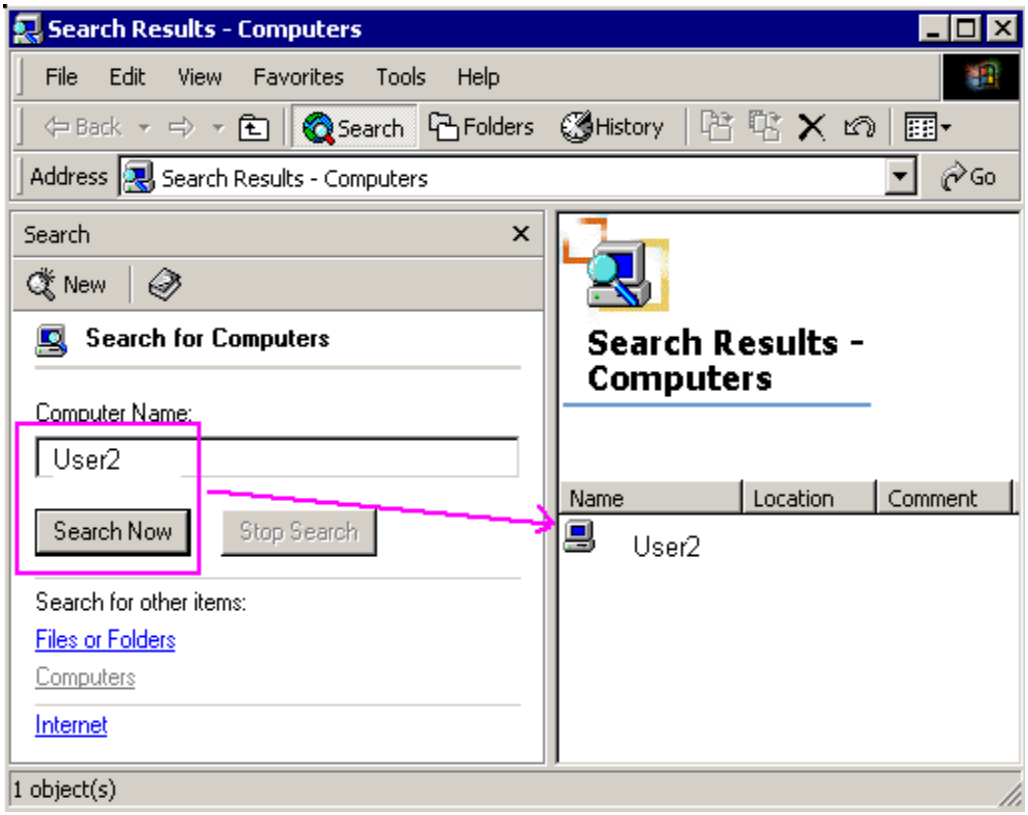

Figure 13: Search Result Screen

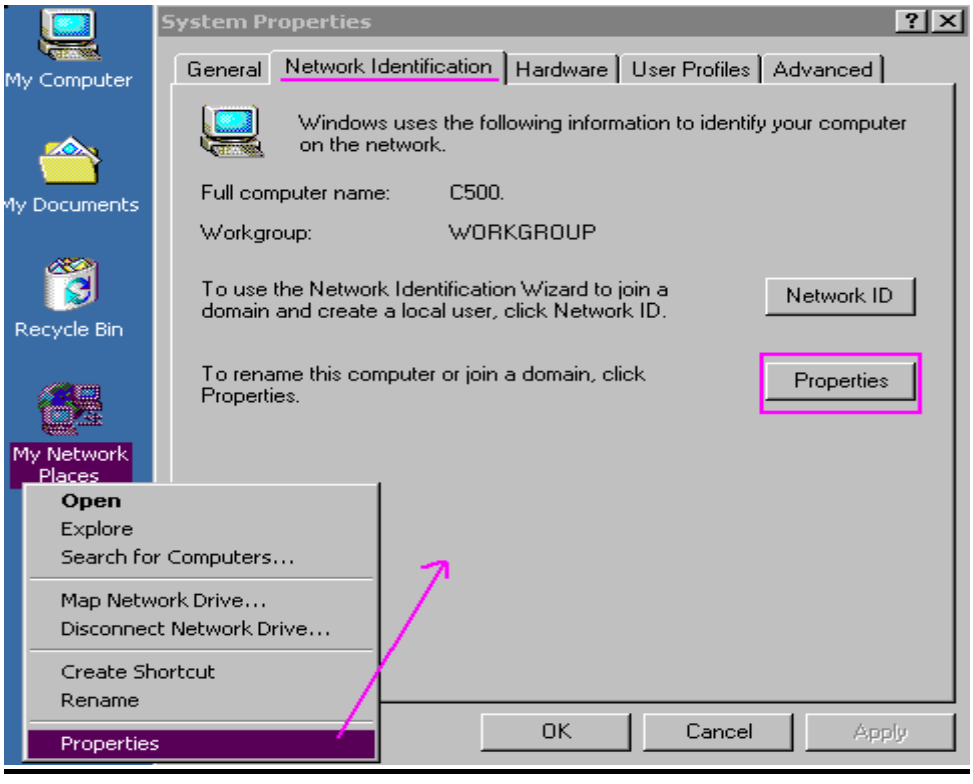

Figure 14: System Properties Screen

The following window is the place to define or make changes (as shown in *Figure 15*)

- Computer name
- Member of Domain or Workgroup
- Domain/Workgroup Name.

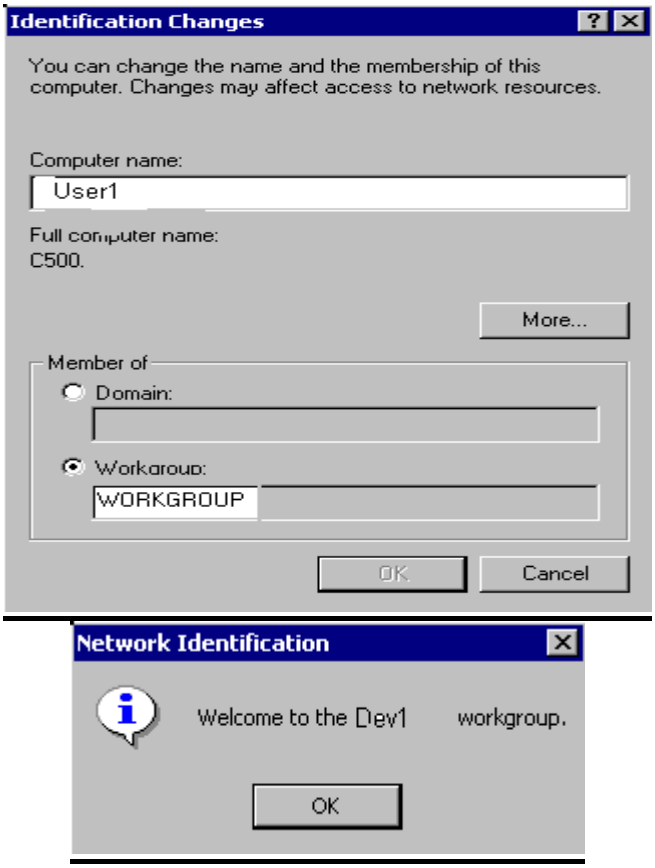

Figure 15: Change/Network Identification Screen

The workgroup, to which your system belongs is defined in the Properties of "My Computer", Tab: "Network Identification". By default, the name of the workgroup is "***WORKGROUP"***

To implement the change click on the button "***Properties"*** as shown in *Figure 16*.

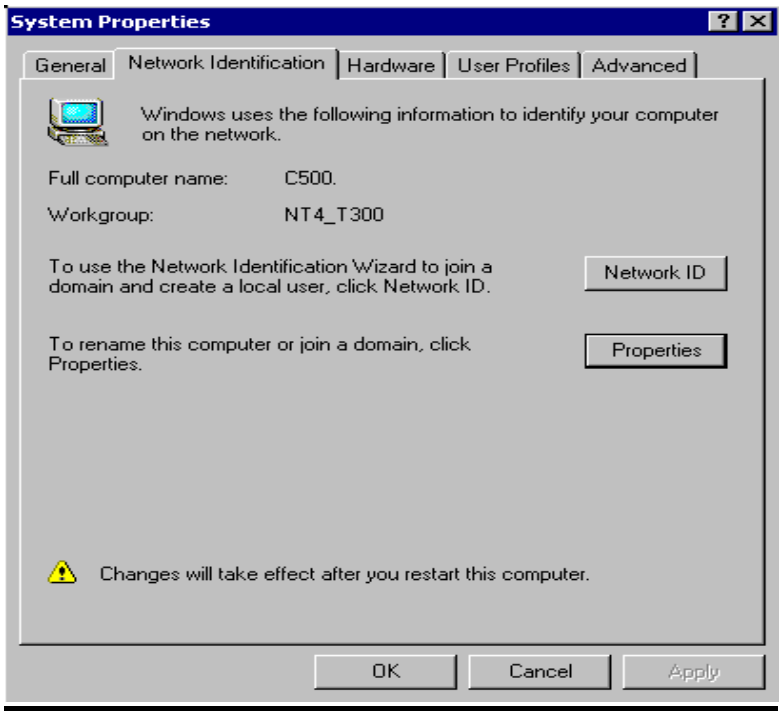

Figure 16: System Properties Screen

☞ Check Your Progress 1

Fill up the blanks:

1) _____ includes icons for all networked computers (servers and workstations) in a workgroup or domain in Windows 2000.

2) By default Windows 2000 assumes that user wants to log in using _____account.

3) In order to lock a local computer press ctrl+alt+del and click_____option.

4) To share a folder, by default Windows 2000 uses name of the _____ as the name of the share.

5) If the user is a member of administrator group on a local computer, the user can see and manage all share folders from a central location in _____.

6) A user name in windows 2000 can be _____ character long.

7) Contents of folder window can be sorted out by _____ regardless of the view, i.e., chosen by the user.

8) For access control every file and folder has four special attributes _____, _____, _____, _____.

2.6 MAPPING A FOLDER

(Using Windows 2000 user can map a drive letter to network resources – **a printer, a drive, a folder.** After mapping a drive letter shared resources can be treated as if they were on a local drive).

To map a network drive, right-click on the network share-name *(NOT on the Computer and not on any folder inside the share)* and select "**Map Network Drive**". Select the drive character to be used, decide on whether to "**Reconnect at Logon**". (If yes select the check box or else leave it).

Select the drive character to be used as shown in *Figure 17*.

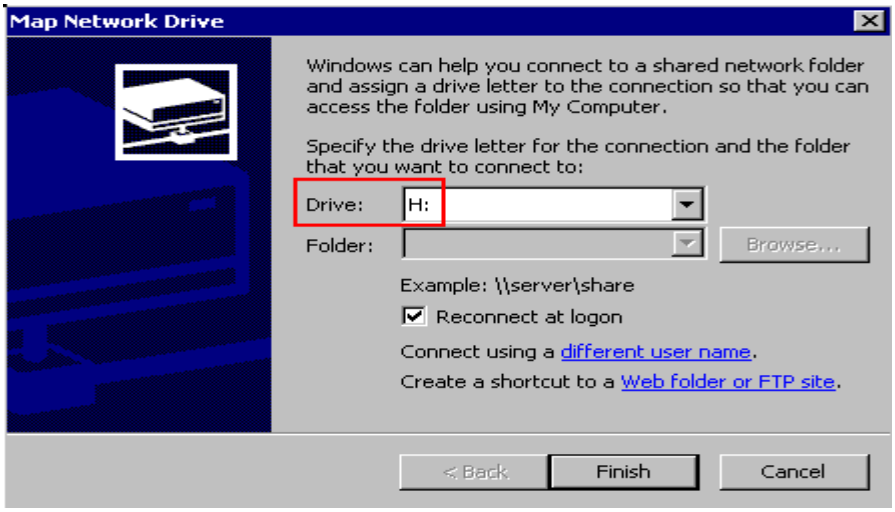

Figure 17: Drive Character Selection Screen

Mapping a network resource to a drive letter from explorer window (*Figure 18*)

1. From pull down Tools menu, choose Map Network Drive.
2. In the drive box, select the drive letter.
3. Write the name of the shared resource in the Folder box.
4. Click finish after you are done with all the steps.

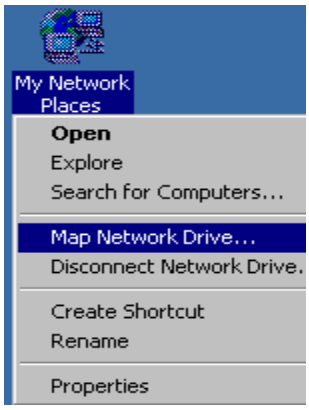

Figure 18: My Network Places

Following these steps can disconnect a mapped drive:

1. In any explorer window, in the Tools menu, choose Disconnect Network Drive. Since window displays a list of all currently mapped drives (as shown in *Figure 21*).
2. In the My computer window, choose mapped drive icon, right click on it, choose Disconnect from the shortcut menu.

Note: In order to assign a mapped drive to different drive, letter drive needs to be disconnected and then remapped to a new drive letter.

2.7 SUMMARY

After reading this unit the user is able to use Windows 2000 server and client. A user can log-on to the network, browse through network resources and access network resources using **My Network Places**. This unit describes the method of Mapping a folders. It also explains how to Map Shared Folders m to devices. There after reading this unit a user can access network resources (files, devices, printers) etc.

2.8 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) My Network Places
2) Local
3) Lock computer
4) Folder
5) Computer management console
6) 64
7) Name,type,size,date
8) System, archieve, read-only, hidden.

UNIT 3 ADVANCED WINDOWS 2000 NETWORKING

Structure **Page Nos.**

3.0 INTRODUCTION

Windows 2000 provides an efficient networking environment. Domains, workgroups and trusted relationships describe the logical structure of Windows 2000. The physical structure of the domain hierarchy is completely segregated from the logical structure. As described in this unit, logical structure is made up of objects, Organisation Units (Ous), domains, trees and forests. The physical structure of the domain hierarchy is mainly composed of domain controllers and sites. A user account gives the user the ability to log on to the network or to a local machine. Everybody who regularly uses the network should have a network account. Group policies further refine the user management in Windows 2000.

Also discussed in this unit is auditing. Lastly, there is RRAS (Routing and Remote Access Screen) which is a very important feature of Windows 2000 that lets remote access possible and is a tool for maintaining network security in Windows 2000.

3.1 OBJECTIVES

After going through this unit you should be able to:

- describe Windows 2000 domains, workgroups and trusted relationships;
- manage efficiently user accounts in Windows 2000 networking environment;
- describe policies, auditing, active directory service in Windows 2000, and
- describe remote access in Windows 2000.

3.2 WINDOWS 2000 DOMAINS, WORKGROUPS & TRUSTED RELATIONSHIPS

In the following section we will introduce concepts of domains, workshops and trusted relationships.

3.2.1 Concept of Domains

A *Windows 2000* domain is a logical collection of network computers that share a centralised directory database referred to as Active Directory Service. In a domain this centralised information directory resides on a computer called domain controller. In Windows 2000 domain controllers are peers only.

Thus Windows 2000 domains provide the following advantages:

- They provide extensibility features to existing networks.
- Domains provide centralised control of all user information.
- Thus domain can be referred to as the basic unit that is used for network growth and security in Windows 2000 network.

Usually one or more domain controllers are associated with a domain. In Windows 2000 Server a domain controller is the computer that is responsible for storing an entire copy of domain directory. In Windows 2000 it is the Windows 2000 Active Directory service that divides an organisation's network logically and physically. Logical structuring facilitates the finding by a user of a resource by name not by its physical location.

Logical structure of a domain comprises:

- Objects
- Organisation Units (OU)
- Domains
- Trees
- Forests

Physical Structure of a domain comprises:

- Domain controllers
- Sites

Objects: A distinct named network resource can be referred to as an object. This object comprises certain related attributes. As an example, for an object printer, the attribute list may include printer name, make, etc. Similar objects can be grouped into classes.

Organisational Units: This is a container object. Container objects are objects that are residing within other objects. The purpose of an organisational unit is to organise the objects of a domain into logical administrative groups.

Domains: The basic unit of Active Directory Service is a domain. It is also referred to as a partition of an Active Directory Service. It is the domain only that is responsible for containing all network objects within it. It also serves as a security boundary to its objects. None of the security policies and settings, such as administrative rights, ACLs, ACE (Access Control Entries) can cross from one domain to another.

Trees: In order to support global sharing of resources trees are required. In a tree one or more Windows 2000 domains are arranged in a hierarchy. Thus by joining multiple domains in a hierarchy a large namespace can be constructed, which can further avoid name conflicts. All domains that are a part of a tree, or that share a tree can share information and resources. A domain tree has only one directory. As long as the user has the appropriate permissions he can use the resources of other domains in a tree. All domains in a tree share a common schema, which is a layout, a formal definition of all objects.

The central repository of information about objects in a tree or forest is called a **global catalog**. All domains belonging to a single tree share a global catalog. Domains in a tree also share a common namespace.

Forest: One or more trees can be grouped into a forest.

A forest comprises:

- One or more trees
- A common schema
- It serves transitions trust relationships between trees.
- Different namespaces between these trees.
- A global catalog that contains the list of all objects in the forest.

Different users while accessing user objects must be aware of the domain name.

3.2.2 Trust Relationships

A trust relationship refers to a link between two such domains, where one domain is referred to as the trusting domain and other as the trusted domain. Trusting domain lets the trusted domain logon.

User accounts and groups that are defined for a trusted domain can access trusting domain resource even though those accounts are not present in trusting domain directory database.

A **kerberos** (a security algorithm) transitive trust refers to a relationship type where

Domain I trusts Domain II,
Domain II trusts Domain III,
Domain I trusts Domain III.

So a domain joining a tree acquires trust relationships of every domain in the tree. In Windows NT and earlier versions, there used to be only one-way trust relationships among domains.

Physical Structure of an Active Directory Service is responsible for affecting efficiency of replication in domain controllers.

Domain Controllers contains a copy of domain database. Wherever an update in the directory takes place, Windows 2000 automatically replicates the change to all other domain controllers in a domain. In a domain having multiple domains controller's directory information is replicated from time to time.

Only those computers running Windows 2000 Server, Advanced Server, or Data Center server can become domain controllers.

Sites is a grouping of IP subnets (ranges). For example, one site can be 192.168.20.0/24 to 192.168.30.0/24

3.2.3 Building Domains

A computer can join Windows 2000 domain only after an account has been created in or added to the domain database. For that a user must have the **Join A Computer to the Domain permission**.

By default, permission is granted to Administrator Members, Domain Administrator or Members of Administrators, Account Operators and Domain Administrator groups.

To join a domain a computer account for that computer should have been created in advance or it may be created during the installation process by selecting the check box '**Create a Computer Account in the Domain**'.

3.3 USER ADMINISTRATION

This section discusses user account administration. For a user to log onto a Windows 2000 network, a user account must be created. It is unique to every user and includes a user name and a password for authentication. A user can logon as a local user and a domain user as well. Thus by having an account a user has access to all network resources. As discussed in previous sections, in the Windows 2000 operating system two kinds of user accounts can be created:

- Domain account
- Local account

User account Administration includes setting up user profiles and name directories and modifying existing user accounts.

The next section discusses Group Account Administration.

Existing User Accounts Modification

Many different kinds of modifications are required with user accounts. These modifications may be required because of organisational or personal changes. An instance is whenever a new employee joins, the company may want to modify an existing account and give access to the new employee. Also, personal profiles may need to be updated at times.

Modification may include the following:

- Renaming
- Erasing
- Disabling
- Deleting User Accounts

1. To Rename a user Account: Normally renaming an account is done so that all access services to an account remain intact. When an account that has been created for a particular user is to be assigned to another user, all permissions, rights, properties set for that account are retained.
2. To Enable/Disable a user account: A user account is disabled when it is not needed for some time but would be accessed after a certain period of time. It is a situation when a user temporarily disables the account and needs access to it after a fixed period of time.
3. To Delete a user account: When a user no longer needs it, it is deleted.

Use Active Directory Users And Computers Snap-In,

Modify properties. To Reset the User Password:

1. Open Active Directory Users And Computers Snap-In and select the user object.
2. Activate the Action menu, click Reset Password. In the Reset Password dialog box, enter a password and select.

User must change password at next logon to force the user to change his or her password the next time that the user logs on.

Managing User Profiles

A user profile contains all data pertaining to a user. It also contains current desktop settings, all connected networked computers and all mapped drives. Modifying

desktop settings can modify a user profile. It is created the first time when a user logs on to a computer.

When you log on to a network computer in Windows 2000 environment you get individual desktop settings and connections.

Windows 2000 supports Roaming User Profiles (RUPs), for users who work on more than one computer. A user set up a RUP on a network server and it is available to all the computers or the domain network. It is copied to client computer from Windows 2000 server when a user logs on. Thus, unlike user profile, with a Roaming User Profile the user always gets his individual desktop settings. Also a local user profile is on single client computer only.

Home Folder: A home folder is one that is provided to the user in addition to my documents folder to store personal data. It is not included in RISP (Routing and Remote Access Screen).

Group Accounts Administration

User accounts can be collected together. Such collections are called as groups. The grouping simplifies administration as new access permissions are assigned to a group rather than to individual accounts. All user accounts belonging to that group have access privileges. Moreover user(s) can belong to multiple groups.

In Windows 2000 environment there are two kinds of groups, Security groups and Distribution groups.

Windows 2000 has 4 built-in groups:

- Global groups
- Domain Local groups
- Local groups
- System groups.

Common types of user accounts are contained in groups. The group scope is responsible for membership of a group. Active Directory Users and Computers Snap-in are used to create a user group in a domain.

Group Policy

A group policy primarily comprises configuration settings that determine the layout of an object and its successors (children) objects. Group policies provide for controlling the programs, desktop settings, and network. In a network, group policies are normally set for the domain. Policy administrators administer group policies.

Types of Group Policies:

- Scripts: let the policy administrator specify applications and batch files to run at specified times.
- Software settings execute the applications. These policies can automate application installation.
- Security Settings are responsible for restricting user access to files etc.
- Remote Installation Services (RIS).
- While executing client installation wizard, it controls RIS installation options.
- Folder Redirection facilitates movement of Windows 2000 folders from their default user profile location to a place where they can be managed centrally.

- Administration Templates consist of registry based group policies for managing registry settings, etc.

GPO (Group Policy Objects)

These objects contain configuration settings for group policies. Information is stored in two ways in a GPO:

1. In containers
2. In Templates

Creation of GPOs takes place before group policies. Group Policies can be modified using:

1. Group Policy snap-in or
2. Using Active Directory Users and templates snap-in.

Only administrators, creator owner or a user with access to GPO can edit a group policy.

Auditing

Windows 2000 auditing is a facility responsible for security. It is responsible for tracking user activities, keeps a check on them. Windows 2000 maintains a security log. User events are written onto their security log. All the events related actions are entered onto security log. An audit entry in security log not only comprises action that takes place, but also the user and success or failure of the event and when the action occurred. Thus whatever event takes place in Windows 2000, Security Log has an entry for the same.

An audit group policy is configured for all domain controllers in a domain. Auditing is assigned to parent container and it passes it down the hierarchy to the child containers. However, if explicitly a child container is assigned a group policy then child container group overrides parent container settings.

To plan an audit policy, computers must identify on which auditing is to be applied. By default, auditing option is turned off.

Only certain specific events can be audited on computers:

- User logging on and off.
- User accounts and group changes.
- Changes to Active Directory Objects.
- Files access.
- Shutting down Windows 2000 Server
- Restarting Windows 2000 Server.

3.4 REMOTE ACCESS

Windows 2000 remote access mechanism lets remote clients connect to corporate networks or to the Internet. Windows 2000 supports two kinds of remote access connection methods (*Figure 1*).

- Dial up remote access
- VPN (Virtual Private Network) remote access.

VPN provides a secure network connection between two remote machines.

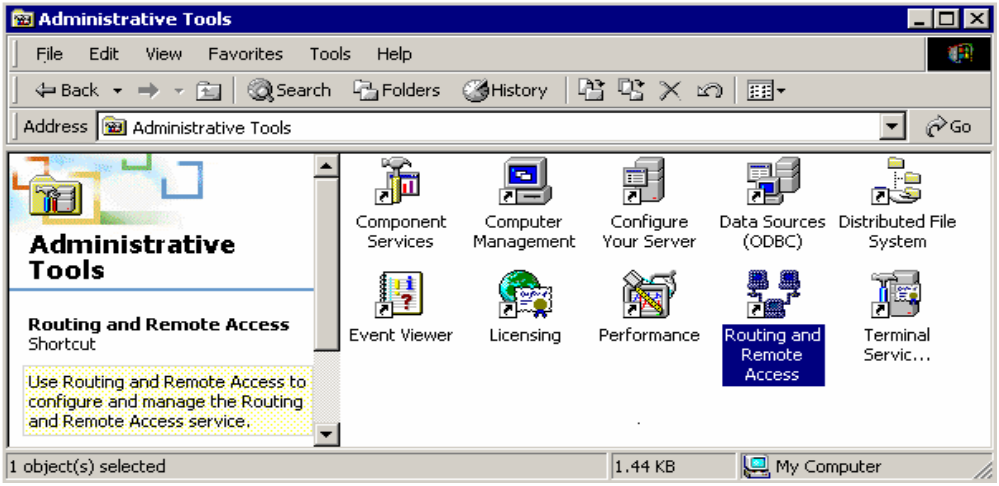

Figure 1: Dial up Remote Access Screen

With **dial up remote access** A remote access client uses telecommunication infrastructure to create a temporary physical structure to create a temporary network or a virtual network.

Right click on the server icon and select "configure and Enable Routing and Remote Access" as shown in *Figure 2*.

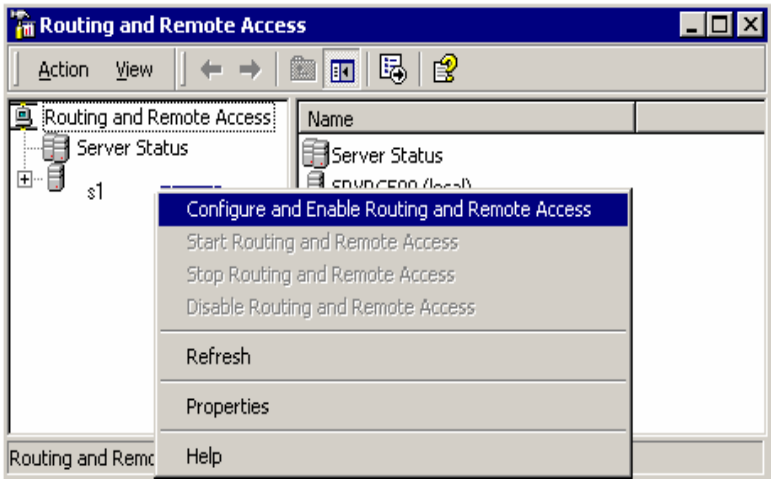

Figure 2: Renting and Remote Access Screen

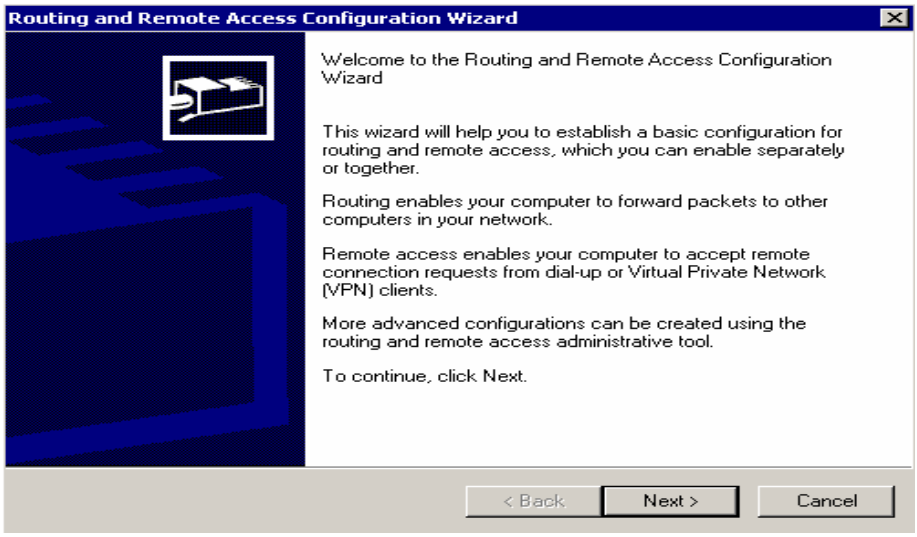

Figure 3: Routing and remote Access Configuration wizard

Using this, all devices for remote access can be enabled and the following screen appears (*Figure 3* (*a*)).

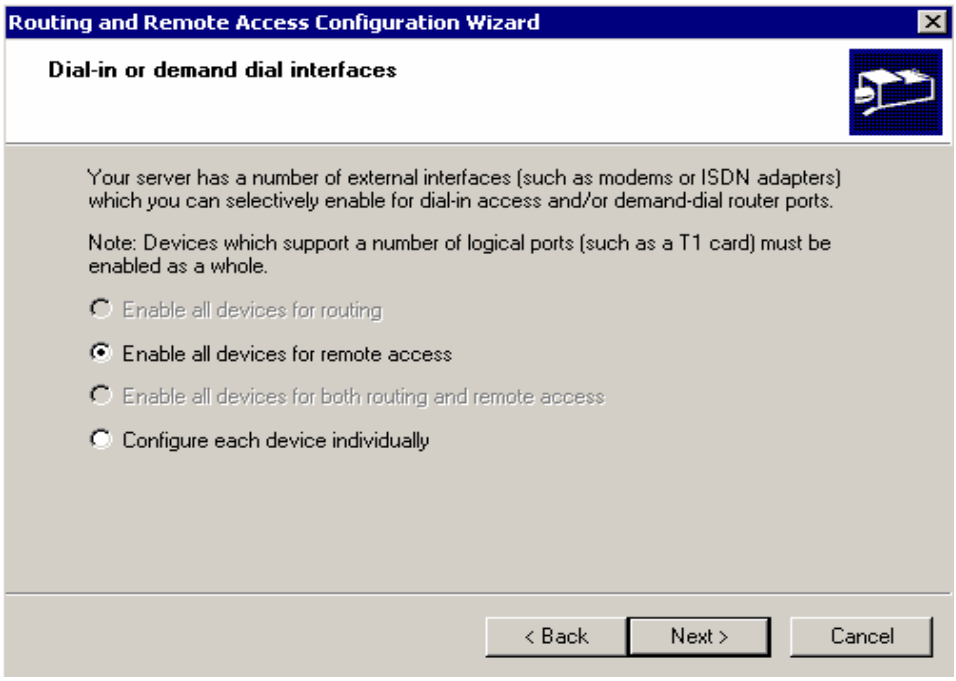

Figure 3(a): Routing and remote Access Configuration wizard

For security reasons use the following option as shown in *Figure 3*(*b*):

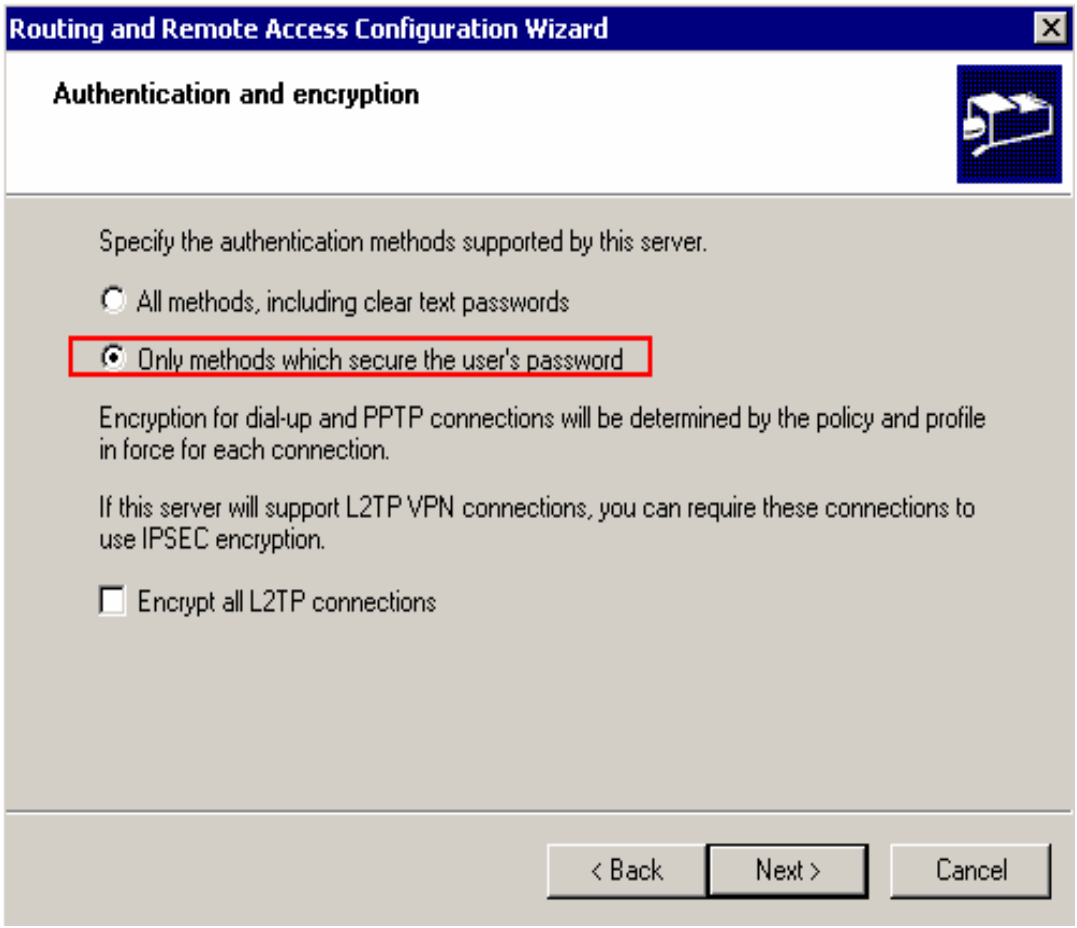

Figure 3(b): Routing and remote Access Configuration wizard

If you have TCP/IP then write TCP/IP as shown below in *Figure 3c*.

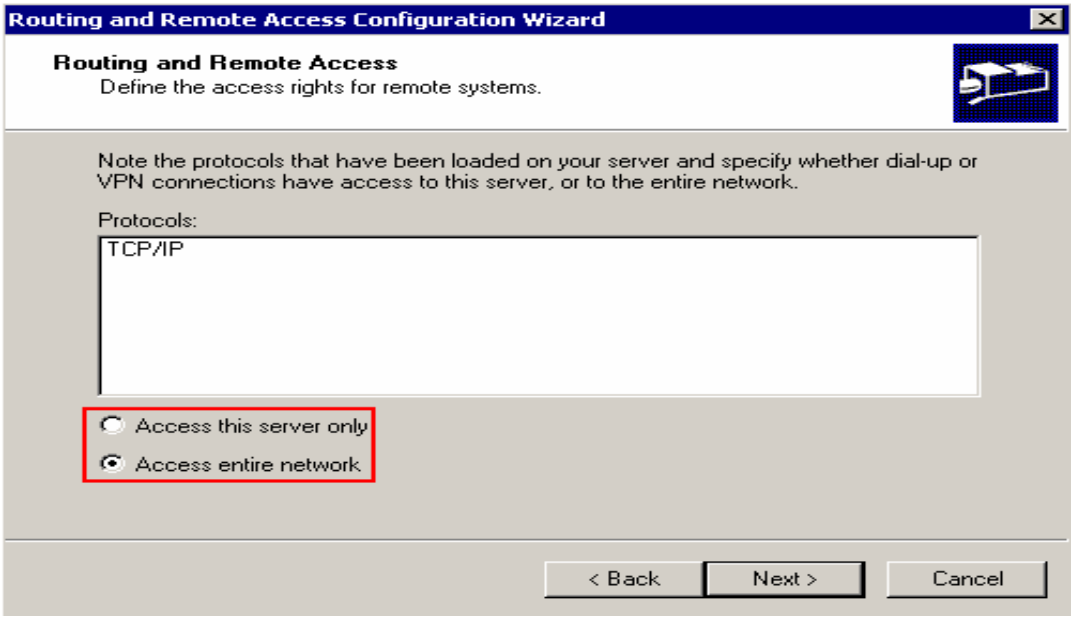

Figure 3 (c): Routing and remote access configuration wizard

Once all the requisites are complete then the following wizards (*Figure 3(c), 3(d*) and *3(f)*) appear:

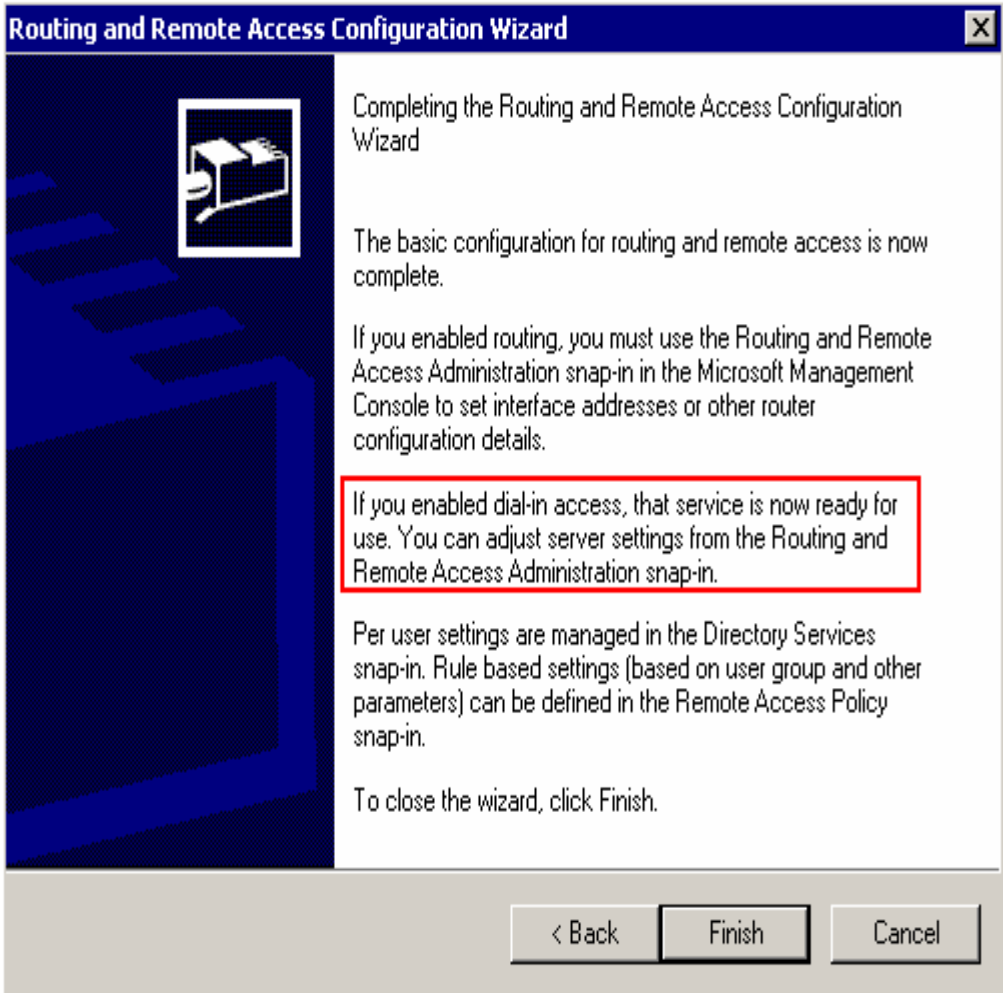

Figure 3(d): Routing and remote Access Configuration wizard

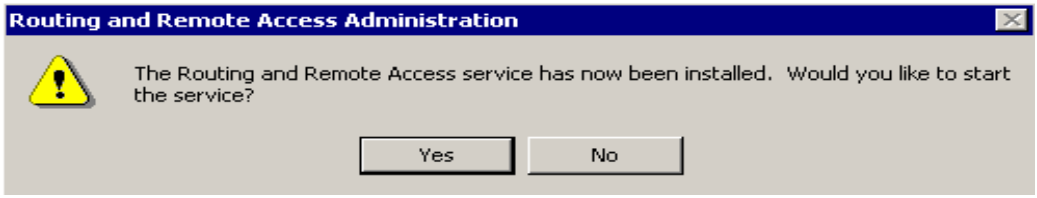

Figure 3(e): Routing and remote Access Configuration (RRAS) wizard

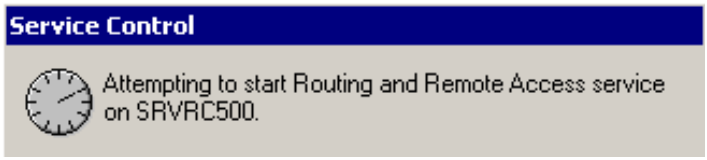

Figure 3(f): Routing and remote Access Configuration wizard

After this screen RRAS is now configured and the contents can be viewed as *Figure 4*:

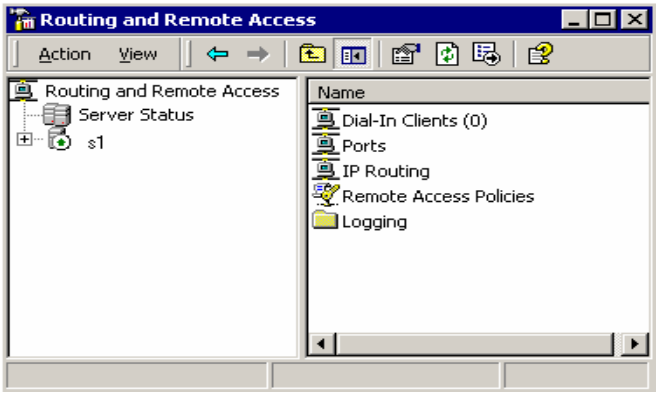

Figure 4: Routing and Remote Access

By default, Windows 2000 creates automatically 5 PPTP and 5 L2TP port for incoming VPN-connections (*Figure 5*).

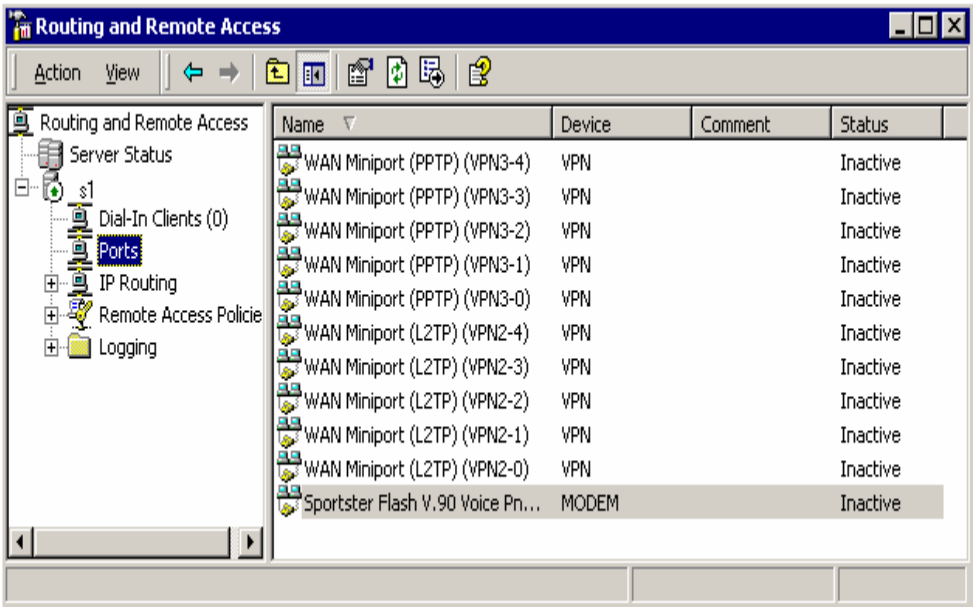

Figure 5: Remote Access Connection Screen

With **VPN remote access** – remote access of a VPN client uses an IP network to create virtual point-to-point connection with a RAS server acting as a VPN server. A dial up Remote Access Connection consist of :

- Remote access client
- Remote access server
- WAN infrastructure.

Remote Access Clients: Windows 2000, Win NT, WIN 98, Windows 95, MS-DOS, MS LAN Manger are remote access clients that can connect to Windows2000 remote access server. Third party clients like UNIX and Apple Macintosh too can connect to windows 2000 remote access server.

Remote Access server: Windows 2000 server accepts requests from client's connections and forwards it to other clients or to the network.

WAN Infrastructure depends upon the type of connection being made. There are various networks like:

PSTN(Public switched telephone network
ISDN(Integrated services digital network
X.25 (ITY-T Protocol based WAN)

Windows 2000 support three types of Remote Access protocols PPP, SLIP and asynchronous NetBEUI, also TCP/IP, IPX, AppleTalk.

Windows 2000 remote Access provides a variety of security features like:

- User Authentication
- Mutual authentication
- Data encryption
- Call back
- Caller id
- Remote access account lock out.

Remote Access Management involves managing users, addresses, accesses and authentication.

Virtual private network is an extension of private network that involves encapsulation, encryption, authentication to links across shared or private networks. A VPN mimics the properties of a dedicated Private network through Internet; allowing data transfer between two computers in a network. Corporate offices can use two different methods to connect to a network over the Internet:

Using dedicated lines or dial up lines VPN uses tunneling to transfer data in a VPN. Tunneling is a secure method of using an internetwork infrastructure to transfer a payload.

A tunneling protocol comprises tunnel maintenance protocol and tunnel data transfer protocols. Two basic types of are:

1. Voluntary tunnels
2. Compulsory tunnels.

Protocols used by WIN 2000 for VPN are PPTP (Print to print tunnel Protocol), L2TP (Layer 2 Transfer Protocol), IPSec (IP security), IP-IP.

VPN management involves managing user addresses, servers access, authentication, and encryption. Troubleshooting VPN involves checking connectivity, remote access connection establishment, routing, IPSec.

Windows 2000 provides a set of RRAS tools:

- **Routing And Remote Access Snap In** enables RRAS, management of routing interfaces, IPX routing configuration, creation of static IP address pool, configuring remote access policies. This is available from Administrative Tools folder.
- **Net Shell Command:** Windows 2000 Netshell command is a command line and scripting utility. It is named Netsh.exe and is installed in % systemroot %\system32 when a Window 2000 is installed.

☞Check Your Progress 1

1) Give the default order of group policy implementation through Active Directory service hierarchy.

……

……

……

2) Is it possible to set up encryption on a compressed folder?

……

……

……

3) When should security groups be used instead of distribution groups?

……

……

……

4) If the domain mode is switched over from mixed mode to native mode, what are the implications?

……

……

……

5) If a remote access client wants to connect to RAS server but connection is not allowed how will this error be solved?

……

……

……

6) Write the purpose of VPN and name VPN technologies supported by Windows 2000?

……

……

……

3.5 SUMMARY

This unit highlights working of a domain, workgroups and trusted relationships in a Windows 2000 network. Windows 2000 provides a secure network environment for efficient resource sharing. Logical structure of domain hierarchy comprises objects,

organisational units, domains, trees and forests. Domain controller and sites make up the physical structure of a domain. Many types of group policies exist, software settings, scripts, security settings, folder redirection etc. Group policies are a set of configuration settings that apply to one or more objects in the directory store. The structure of a group policy is made up of group policy objects, templates and containers. Group objects must be created before the creation of group policies.

Auditing is the process of tracking both user and Windows 2000 events. Windows 2000 writes the events to the security log on each computer. An audit entry contains information about the event that occurred, user responsible for performing that event, success and failure of that action. Another interesting feature in Windows 2000 is RRAS that lets the remote access possible.

3.6 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) Group policy is implemented in the order site, domain, and organisational unit.

2) Encryption and compression cannot be applied simultaneously to a file. In order to set up encryption on a file it needs to be decompressed first.

3) Security groups are used to assign permissions. Whereas it is recommended to use distribution groups only when the group is required to perform a security related function.

4) Once you switch from mixed mode to native mode you cannot revert to mixed mode.

5) Do the following measures to correct the error:

   i. Verify Event logging enable (d) and view System Event Log, on computer running RRAS.
   ii. On the server, open Authentication Methods dialog Box and check Allow Remote systems to connect without authentication check box.
   iii. On remote access client, access the properties the dial up device like a modem, click Diagnostic tab check the Record a Log check Box.

6) It provides secure data transfer over a public network. Windows 2000 supports PPTP and L2TP.

3.7 FURTHER READINGS

1. www.microsoft.com/ windows2000 OS living

2. "*Operating system concepts*" Silberschatz, Galvin & Gagne Sixth Edition, John Wiley and Sons.

UNIT 4 WINDOWS XP NETWORKING

Structure **Page Nos.**

4.0 INTRODUCTION

Windows XP is a network operating system. Microsoft introduced Windows XP so that it can be used in small networks as well as in networks spanning a large area. Windows XP comes with Windows XP Home Edition and Windows XP Professional. Home Edition supports workgroup networking but does not support domain networking. Windows XP also supports most of the networking features that were there in Windows 2000. Our objective in this unit is to highlight the features of Windows XP professional edition.

4.1 OBJECTIVES

After going through this unit you should be able to describe:

- Windows XP networking features;
- file sharing features in Windows XP;
- folder sharing in Windows XP;
- disk sharing features in Windows XP;
- file Encryption in Windows XP, and
- offline features in Windows XP.

4.2 INTRODUCTION TO WINDOWS XP NETWORKING

In this subsection we will take up some standard protocols supported by Windows XP system.

4.2.1 TCP/IP Protocol Setting for Windows XP

TCP/ IP Protocol is a suit of protocols that provides a set of vast networking capabilities. In Windows networking environments TCP/IP is the default protocol for

both user group and domains. Windows XP has many built in features for configuring and monitoring TCP/IP.

Configuring IP settings in Windows XP:

TCP/IP protocol suite is the default installation on all Windows XP systems.

To access TCP/IP properties:

1. Initially log as administrator
2. Open network Connections:
   From windows XP start menu, choose connect to
3. Right click local area connection icon, choose properties from shortcut menu.
4. On the general tab, select Internet Protocol (TCP/IP) and click properties.

The *Internet Protocol (TCP/IP)* Properties dialog box opens. Through this dialog box the computer can be configured to use static or dynamic addressing.

A new feature in Windows XP is Alternate IP Configuration tab in *Internet Protocol* (*TCP/IP*) Properties dialog box.

It allows an automatically assigned:

- IP addresses if a DHCP server is available.
- Static IP configuration when a DHCP server is not available.

Thus this option enables the user to connect to two different networks and get address assigned.

4.2.2 To Select a Network Protocol

Click the network protocol that you wish to work on (as shown in *Figures 1 & 2*):

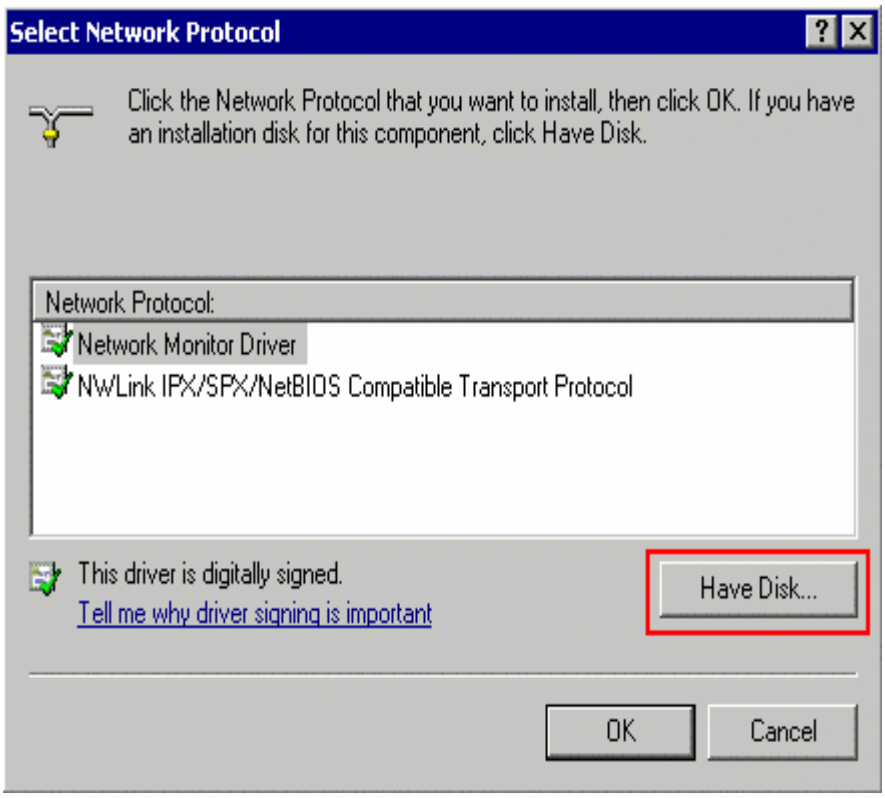

Figure 1: Network Selection Screen

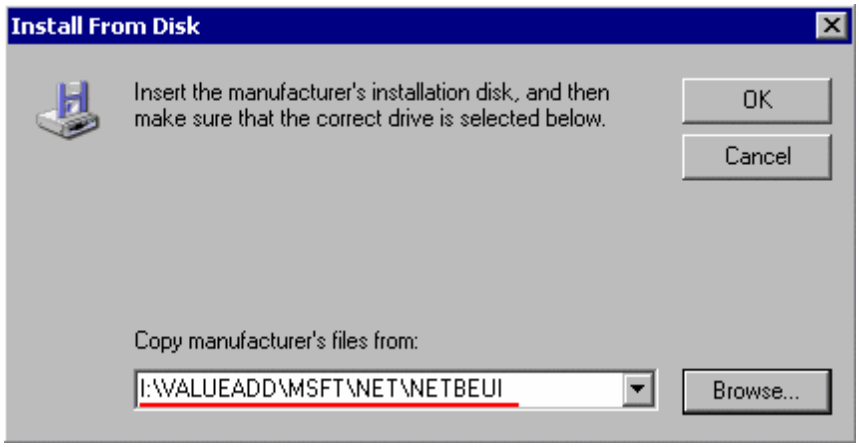

Figure 2: Installation Screen

If we right click on My Network Places to display network properties, this window (*Figure 3*) appears on the screen,

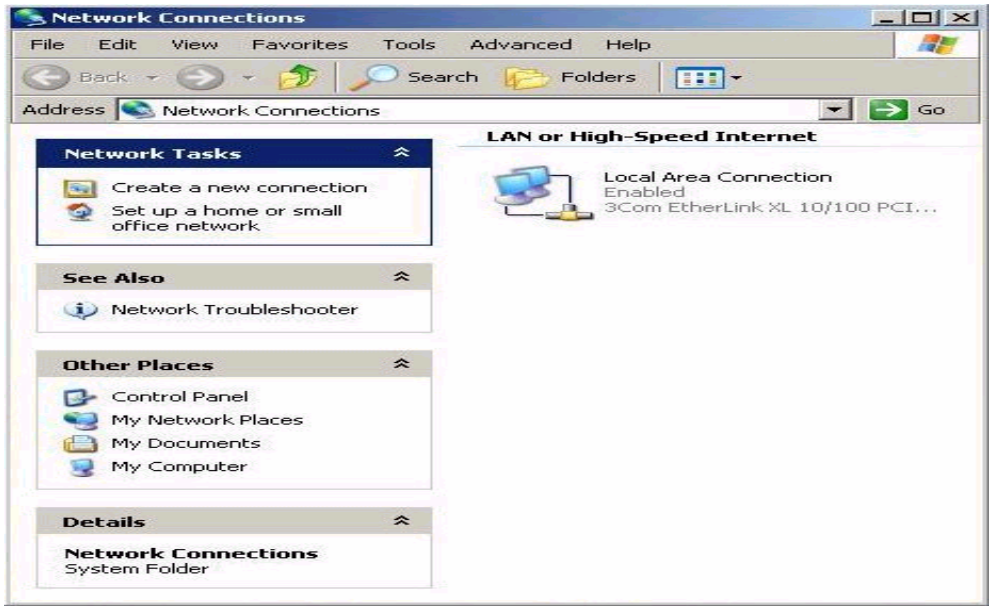

Figure 3: Network Connection Screen

Then the following windows (*Figure 4*) for LAN connection properties appear:

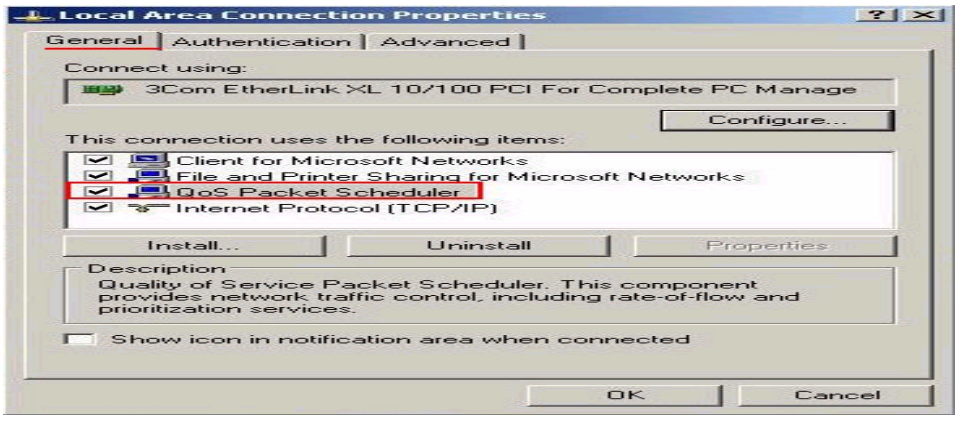

Figure 4: LAN Connection Properties Screen

Windows 2000

For authenticated network access the following screen (*Figure 5*) is used.

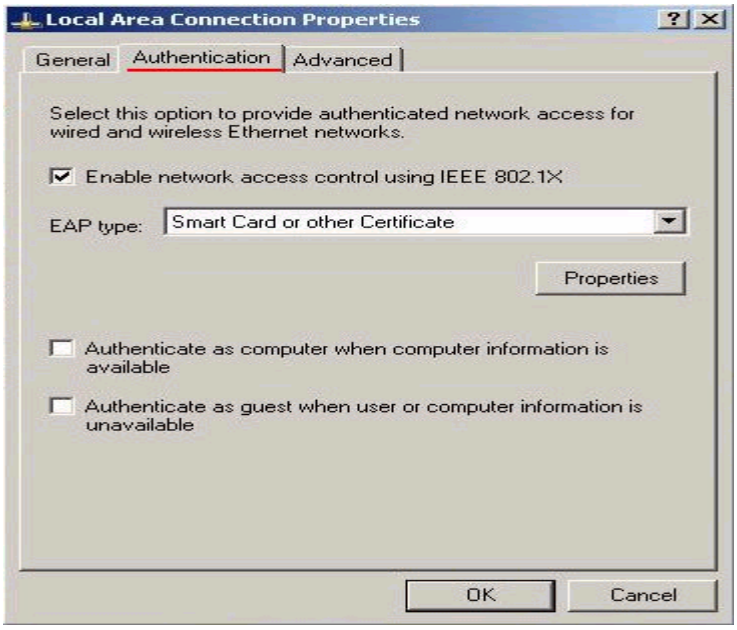

Figure 5: LAN Properties Screen

For selecting network components that you wish to install on your network use the following screens (*Figure 6):*

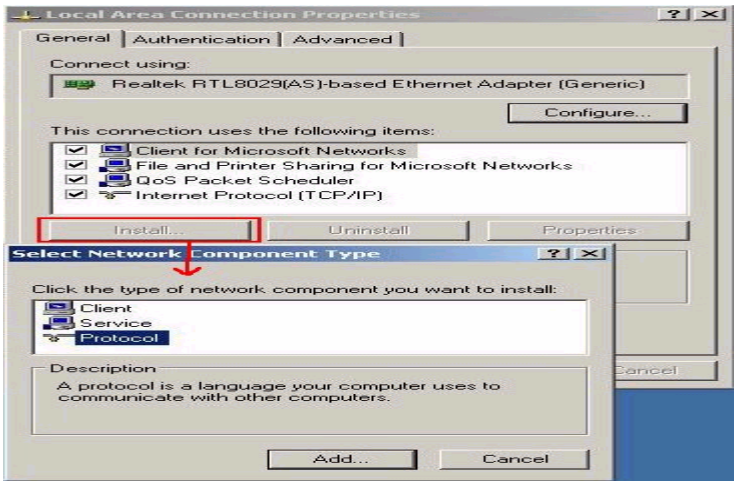

Figure 6: Network Component(s) Selection Screen

The NetBEUI Protocol is not available in Windows XP:

Support for the NetBIOS Extended User Interface (NetBEUI) network protocol has been discontinued in Windows XP. This protocol is not available for installation in Windows XP.

If you upgrade from a previous version of Microsoft Windows with NetBEUI installed, the Compatibility Wizard displays the following message:

The currently installed driver for the NETBEUI Transport Protocol is not compatible with Microsoft Windows XP and will be uninstalled during the upgrade. This protocol is removed from this new version of Windows as shown in *Figure 7*.

Figure 7: Network Protocol Selection Screen

For more information about this driver, visit the manufacturers Web site at http://www.microsoft.com. Web addresses can change, so you may be unable to connect to this Web site.

For a list of protocols supported by Windows XP, see the Microsoft Windows Whishtis Protocols Compatibility List at the Microsoft Web site.

4.2.3 Virtual Private Networks and Remote Networking

Windows supports Virtual private networks connection to access machines remotely. A VPN connection lets one system connect securely to another machine over the network. A VPN is an extension of a private network that comprises links across shared or public networks. But here in VPN, local network data is encrypted and is secure (referred to as tunneling), for security considerations. For VPN connection either use Point to Point (PPTP) or Layer 2 tunneling protocol (L2TP).

4.3 WINDOWS XP IN FILE SYSTEMS

File Systems manage the way in which system resources are shared. All network file sharing are based on it. By default NTFS is the file system for fixed storage in Windows XP.

To connect a drive to NTFS, follow these steps:

1. Choose Start, Run, Type cmd and click Ok.
2. At command prompt, type convert C:\FS: NTFS where C is the letter of the your drive.
3. Press enter to run the command.

Note: If any of the files on a disk volume are open then volume won't be converted.

File Encryption

Windows XP Professional lets the user encrypt any of the files or folders using EFS. The user can still use that file or folder but no one else will be able to access it, if that file is not shared.

To encrypt a file or folder:

1. Right click the file and choose properties.
2. On the General tab, click the Advanced option.
3. In the Advanced Attributes dialog box, select Encrypt contents to secure data and click OK.

This EFS service in Windows XP includes a new feature that allows sharing an encrypted file or folder.

1. Right click the encrypted file and choose properties.
2. On the General tab, click advanced button, then click details button in Advanced Attributes Dialog Box.
3. In encryption Details Dialog box, click the Add for multiple users.
4. In select user's dialog box select the additional users and then click ok.

☞ Check Your Progress 1

1) _____ allows users to keep copies of network files on a local machine.
2) By Default windows XP computers contain _____file-sharing feature.
3) By Default _____is the file system for fixed storage in Windows XP.
4) Command line option in any environment lets the user interact with the _____.

4.4 SHARING NETWORK RESOURCES IN WINDOWS XP

In the subsection we will describe the process of sharing files, folders and devices in Windows XP.

4.4.1 Sharing Files in a Windows XP

By default, Windows XP computers that do not belong a domain use a new feature called Simple File Sharing.

New Feature in Windows XP:

Simple File sharing makes NTFS permissions easy for users to manage.

While sharing a resource with simple file sharing enable others users have read only access to the file. Also Full Control can be given to the users.

But Windows XP computers that belong to a domain cannot use simple File sharing.

4.4.2 Sharing Folders in Windows XP

To share a folder with **Simple File Sharing** enabled, you first need to ensure that the folder does not currently reside in a private folder. If the folder does, it is either removed from the parent folder or to another location (as in *Figure 8*(*a*)).

To share the folder, follow these steps:

1. Right click the folder that user wishes to share. Choose sharing and security.
2. On the sharing tab, select share this folder on the network; give a name for the folder in the share name box.

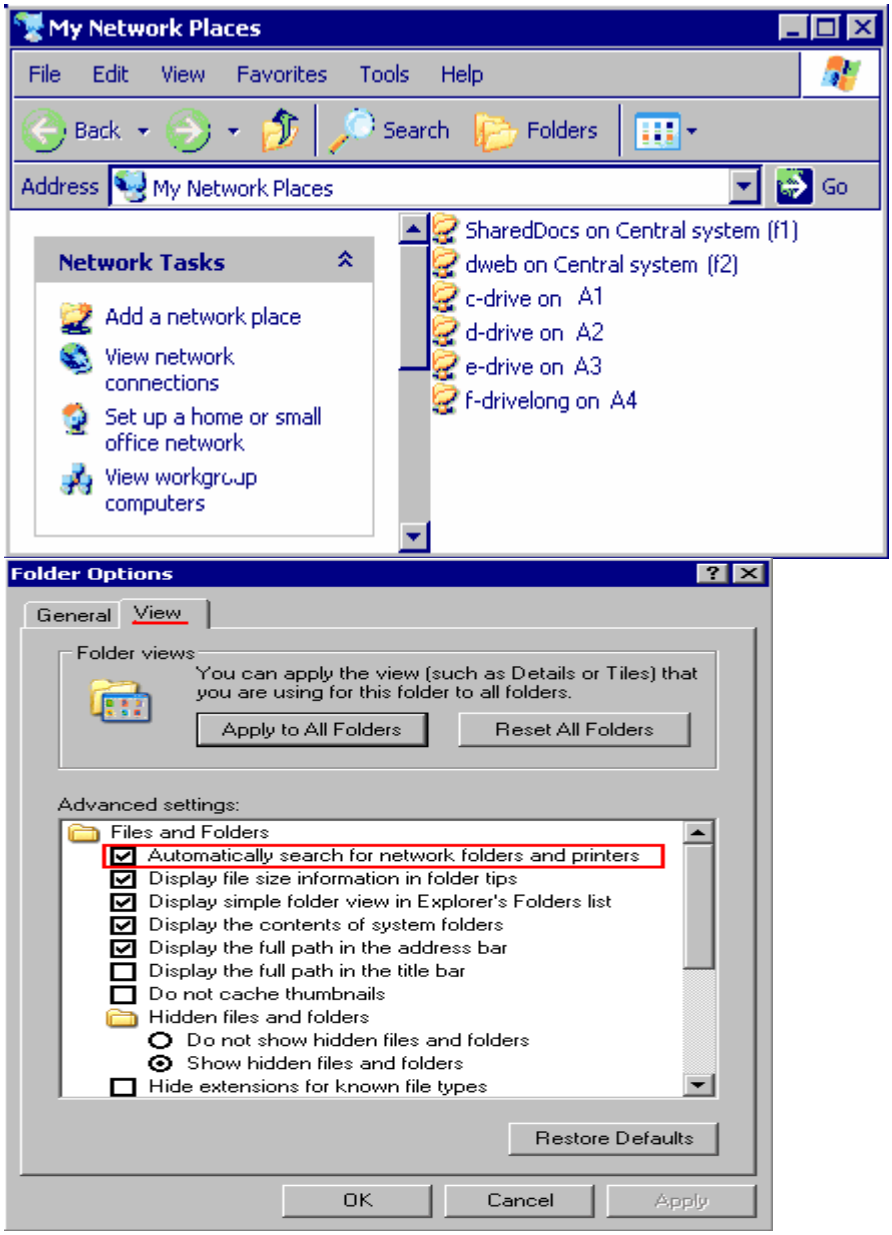

Figure 8(a): Sharing Folder Screen(s)

Following *Figure 8*(*b*) is a list *of shares* (shares refer to shared resources over the network) on the network: if the permission for sharing has not been granted then a dialog box appears as it is shown in *Figure 8 (b)*.

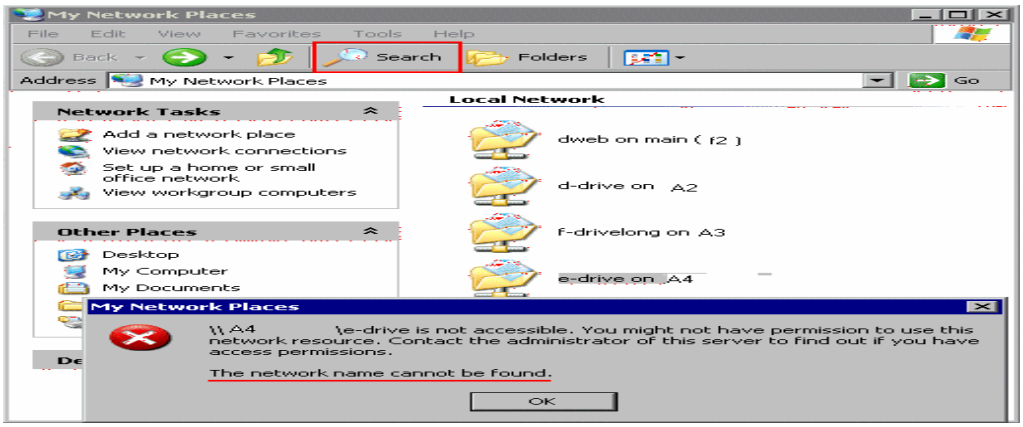

Figure 8(b): Drive Mapping Screen

Windows 2000

The following screen (*Figure 8*(*c*)) & (*Figure 9)* share a given folder on the network.

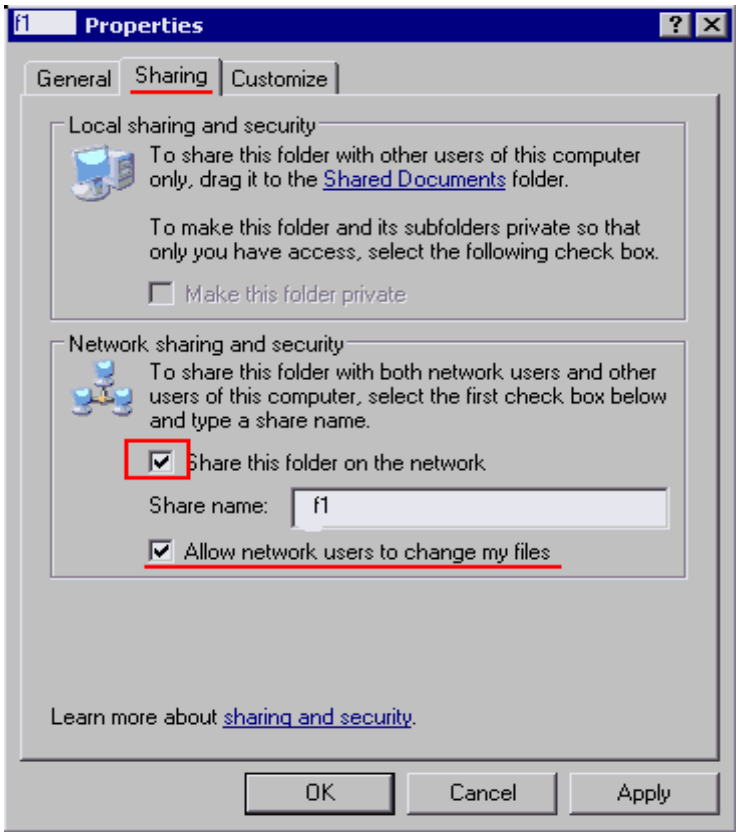

Figure 8(c): Resource Properties Screen

When this folder f1 is now shared using the "Simple File Sharing " then also the security settings are modified. Thus the option – Allow Network Users to change my files is enabled and users will have full control to edit and delete files. But if you want users to be able to read your files only, clear this check box.

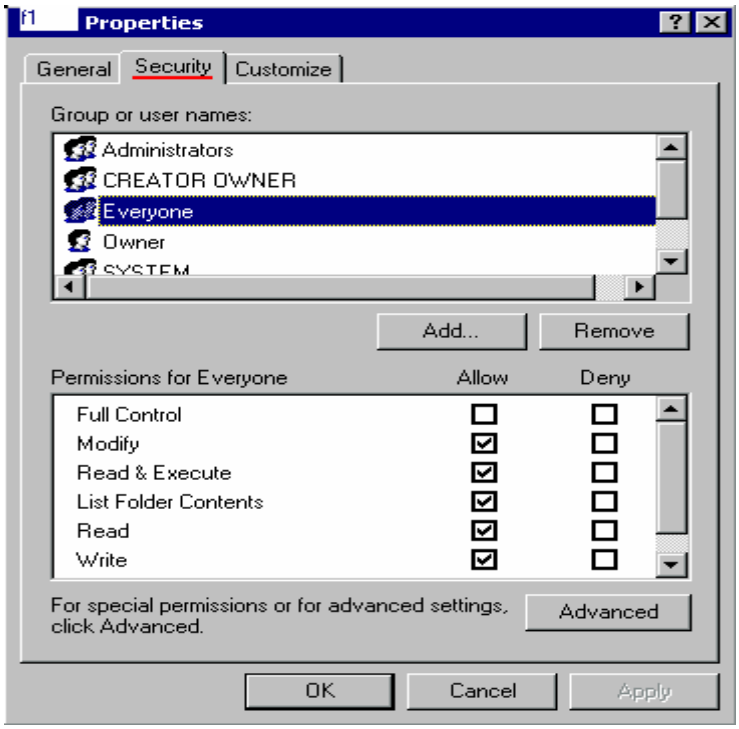

Figure 9: Advanced Properties Screen

4.4.3 Sharing Drives in Windows XP

To share a drive (*Figure 10*),

1. Right click the drive letter that the user wishes to share.
2. Choose sharing and Security.

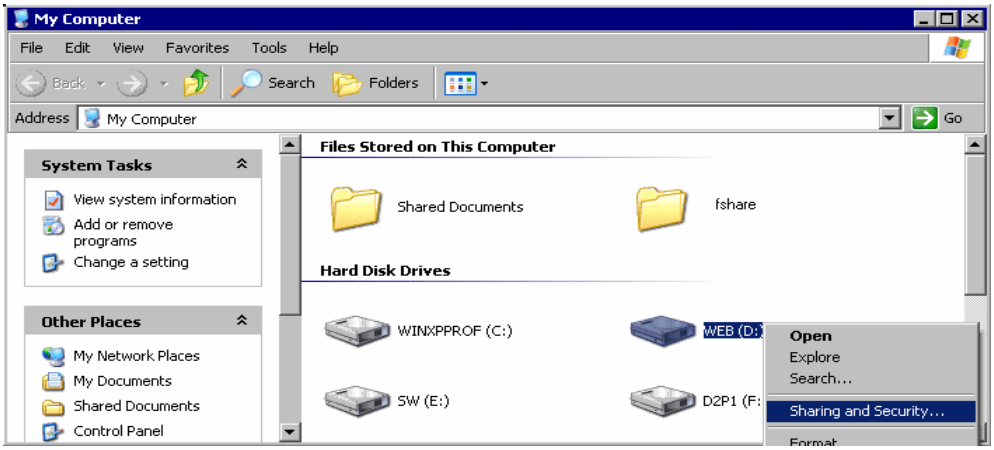

Figure 10: Drive Sharing Screen

Windows XP lets the user handle security issues (*Figure 11*)

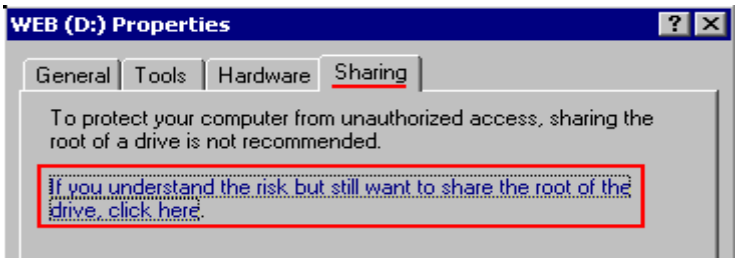

Figure 11: Web (D:) Properties

1) Select the desired folder from the share.
2) Right click on the folder and select "Sharing and Security".

or

3) On the left side select "Share this Folder" (*Figures 12 and 13*).

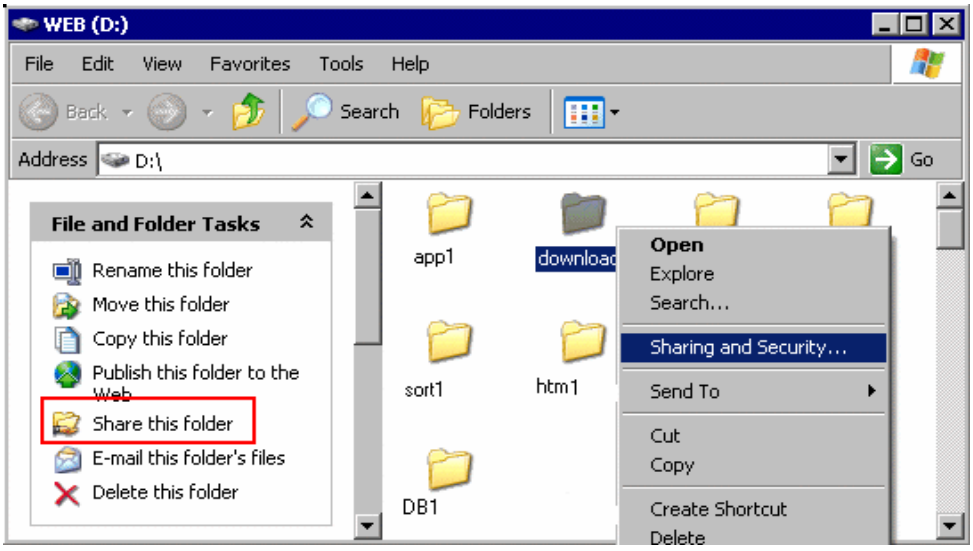

Figure 12: Web (D:)

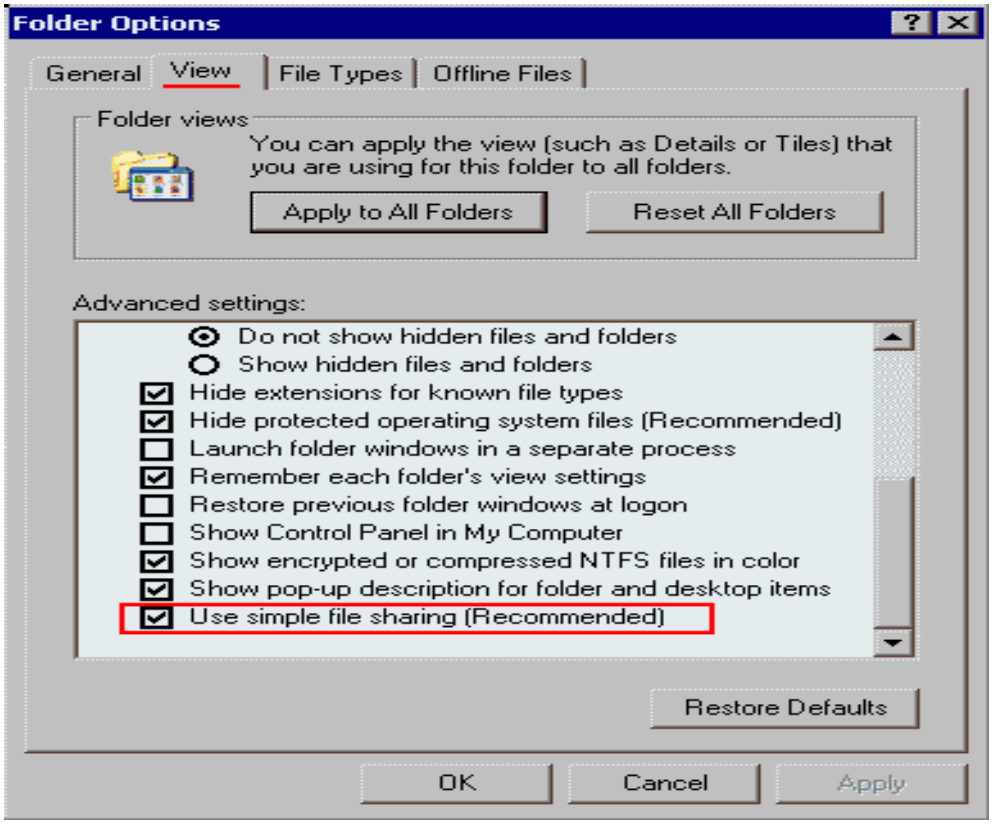

Figure 13: Folder Option Screen

The process of sharing a disk is identical (*Figure 14*) to the procedure used on Windows NT4 and Windows 2000.

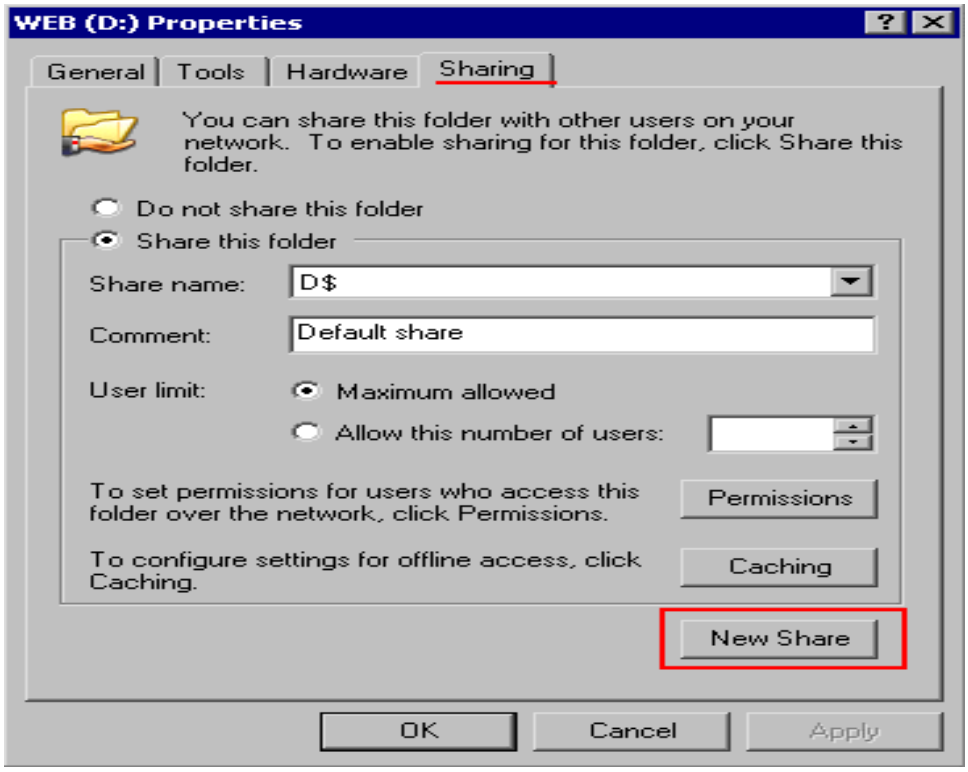

Figure 14: Web (D:) Properties

Enter the name of the share, as to be used on the network and as to be displayed in the Network Neighborhood as given in the above screen (*Figure 15*).

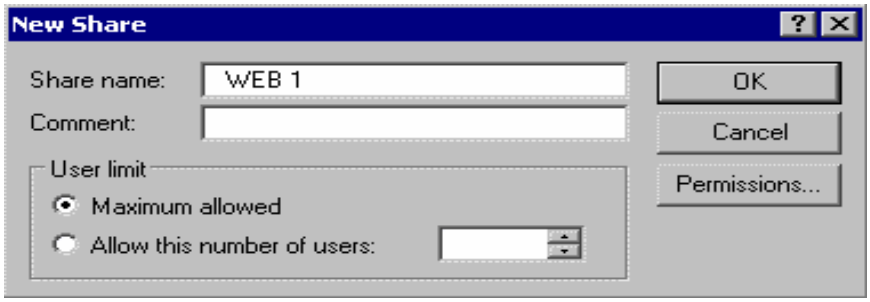

Figure 15: New Share Screen

By default all users in a network have access for a share, Even this group can be reduced (*Figure 16*).

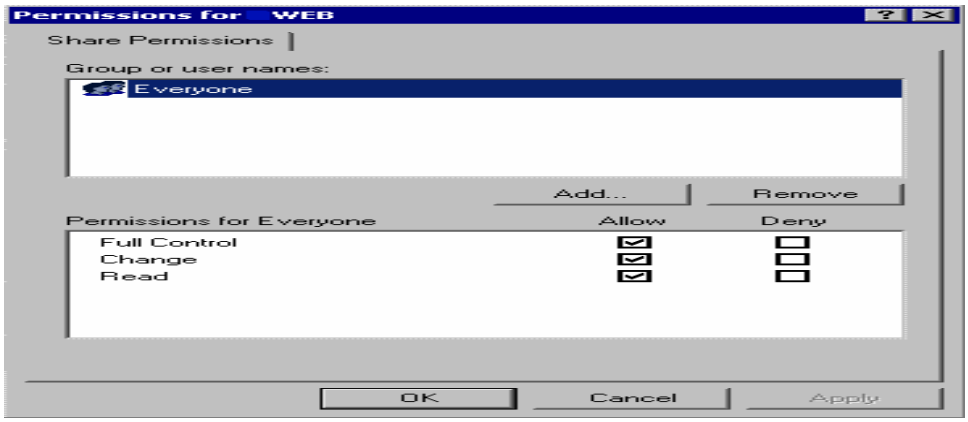

Figure 16: Share Permission Screen 1

To view/modify the permissions or to remove the sharing you can select the share names from the drop down list as shown in *Figure 17*:

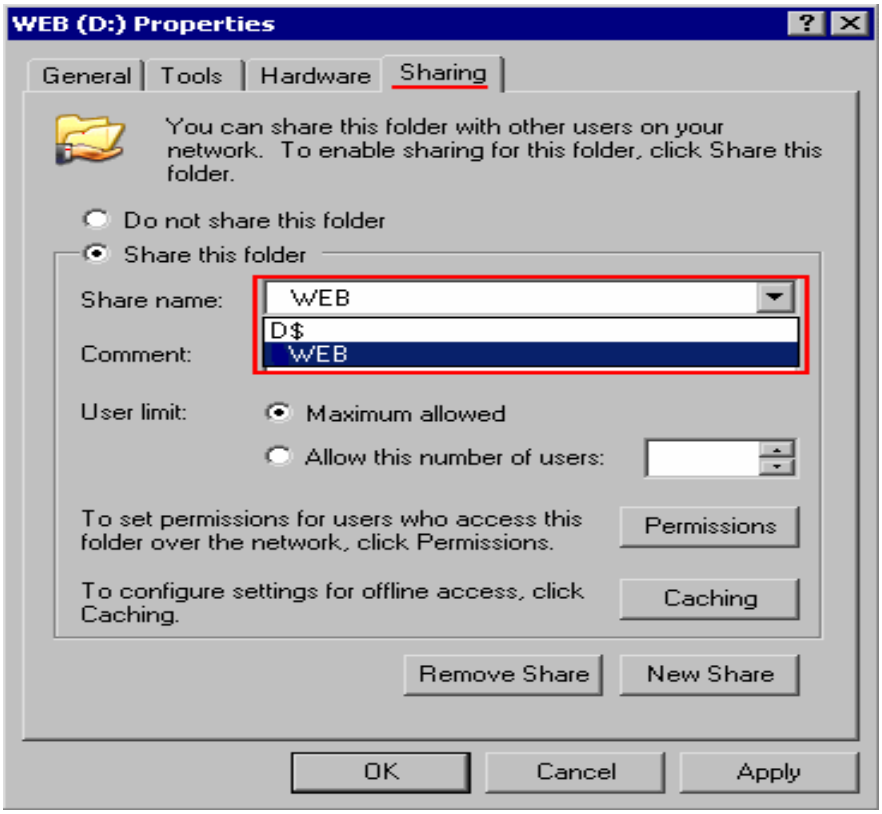

Figure 17: Share Permission Screen 2

Then the following screen *Figure 18* shows Files and the Hard disk drives on the shared network.

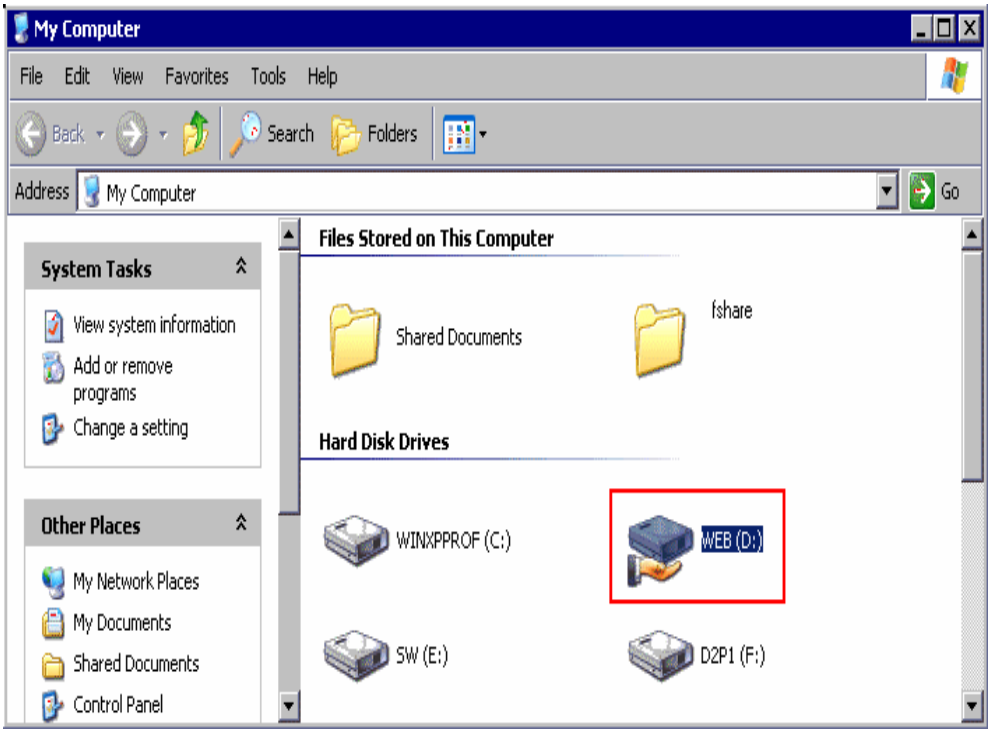

Figure 18: My Computer

While sharing a drive system warning is invoked that sharing an entire drive is not recommended but sharing the entire drive is recommended for several situations as well. But under circumstances, access should be given to everyone group (as shown in *Figure 16*), but doing so makes the shared drive highly vulnerable.

4.5 ENABLING OFFLINE FILE FEATURES

Offline file allows users to keep copies of network files on a local machine. When say not connected to network, the user can use cached copy. When the user again reconnects to the network, offline file is synchronized with the online copy.

If changes have been made to the offline copy, offline file is copied to the network copy. If network version is changed but offline copy has not changed, the online copy is copied over the users offline versions.

If both online and offline versions of the file have changed, a dialog box appears that lets the user select either of the two versions and also gives an option to retain both the versions of different filenames with the same name.

This feature is useful for:

1. Users working on a network.
2. Mobile Users
3. Users with an unreliable network connection

In order to make a file offline **fast user switching** feature has to be disabled first. This new Windows XP feature lets one or more additional users logon to the local computer without the other users logging off.

This **fast user switching** option is to be turned off first before making a network file offline.

1. From Start, Control Panel chooses open folder option.
2. Select offline file option
3. Here select drive, ok.

While working with offline files (in Windows XP environment) following options can be set:

1. **Synchronize all offline files when logging on:** If the users choose this option it synchronizes all files as the user logs on to the network.

2. **Synchronize all offline files before logging off:** This is by default i.e. before logging off all files are synchronized. This option makes sure that all users' files are synchronized before logging off from the networks. For most users, this option is the best while working with offline files.

3. **Display a reminder every x minutes:** A balloon reminder appears in the notification areas, when the user is working offline. By default, this message appears every hour. This time interval can be adjusted.

4. **Create an offline File shortcut on the Desktop:** In order to make shortcut to the Offline files folder on your desktop you can easily access any offline files.

5. **Encrypt offline files to secure data:** This option facilitates the encryption of files on the local hard disk.

6. **Amount of disk space to use for temporary offline files:** This option lets the user control the amount of disk space that is allocated for temporary offline files.

4.6 SUMMARY

Windows XP provides networking features that are capable of supporting a wide range of networks. In this unit Windows XP networking has been discussed, since TCP/IP is the de facto protocol for the Internet so it is also considered the favoured protocol for Windows XP machines. Windows XP does not support NetBEUI. File sharing, disk sharing folder sharing is very much similar to Windows and Windows 2000 environment. Also supported with this network operating system is file Encryption. Offline features are very useful for mobile users. And a window XP does support many offline features.

☞ Check Your Progress 2

1) Which operating systems support NTFS file system? Two computers are connected using a Local Area Network; Machine A is running on a 98 second Edition with FAT 32 file system. Machine B is running on XP Pro with NTFS file system. Will the Machine A be able to view and access files on XP, which are shared. Assume ideal situations with no group policies. Also answer, if not why?

2) Mrs. Smith had Windows XP Pro on her Office desktop. She had some critical data on his computer as password protected and secure. Due to some error, she called a technician, who did a parallel installation of Windows XP on different folder and removed the initial installation of XP. Will Mrs. Smith still be able to access the shared File/Folders (assuming no recovery systems installed)? If not,

can you enable it? Also what difference had it been if we had FAT32 or XP Home Edition and why?

3) Mr. Smith wants to computerize his office. He has a Medium Scale business with plans of growing in near future. What type of operating system and network structure would you design for them?

4.7 SOLUTIONS /ANSWERS

Check Your Progress 1

1) Offline file feature
2) Simple file sharing
3) NTFS
4) Operating system

Check Your Progress 2

1) Operating systems that support NTFS are:
   Windows 2000
   Windows XP
   Yes, although win 98 sec does not support NTFS, yet it is not reading physically.
   XP is reading the disk physically and transferring data using NIC card. There fore, 98 Sec can read NTFS of XP.

2) No, there is no way to access them.
   In FAT32, we could access using a different machine
   We can physically attach the drive as secondary drive to a system and access the files; this is because NTFS uses file encryption.
   In XP home, we don't have File Encryption.

3) Ideal Operating system: Windows XP
   Ideal Network Structure: Server Based.

   Reasons:

   1. Not computerized at all: XP's easy user interface would be better than 9X or 2000.
   2. Plan to grow in near future: Server based is better over peer-to-peer with more security and ease in increasing users and handling them.

4.8 FURTHER READINGS

1. www. microsoft.com
2. *Survey of operating system*. John Holcombe & Charles Holcombe, Tata McGraw Hill.