

**Chapter
1**

**WINDOWS NT
PLATFORM**

*Get on the
Fast Track!*



TM

**SYS-ED\
COMPUTER
EDUCATION
TECHNIQUES, INC.**

Objectives

You will learn:

- C Product overview.
- C Windows NT architecture.
- C Workgroup and domain models.
- C Logon access - local and network.
- C Networking features.
- C Sharing.
- C Security features.
- C Supported file systems - FAT and NTFS.
- C File naming convention in NTFS.
- C Network sharing and local NTFS shares.

1 Product Biography

Windows NT Workstation and Windows NT Server shipped in July of 1993.

Windows NT Workstation	Windows NT is a workstation operating system that provides you with the power of a workstation with the ease of use, productivity and compatibility of a PC. It is intended for individual users who need the power of a workstation at their desktop.
Windows NT Server	<p>Windows NT Server is a 32-bit network operating system with preemptive multitasking and memory protection.</p> <p>Windows NT Server provides you with the connectivity, the base services and the centralized administrative tools to deliver business information and services across a distributed network of computers.</p> <p>Windows NT Server scales from the small network to the enterprise, providing both basic file and print services as well as application services like database, messaging, communications and software management.</p>

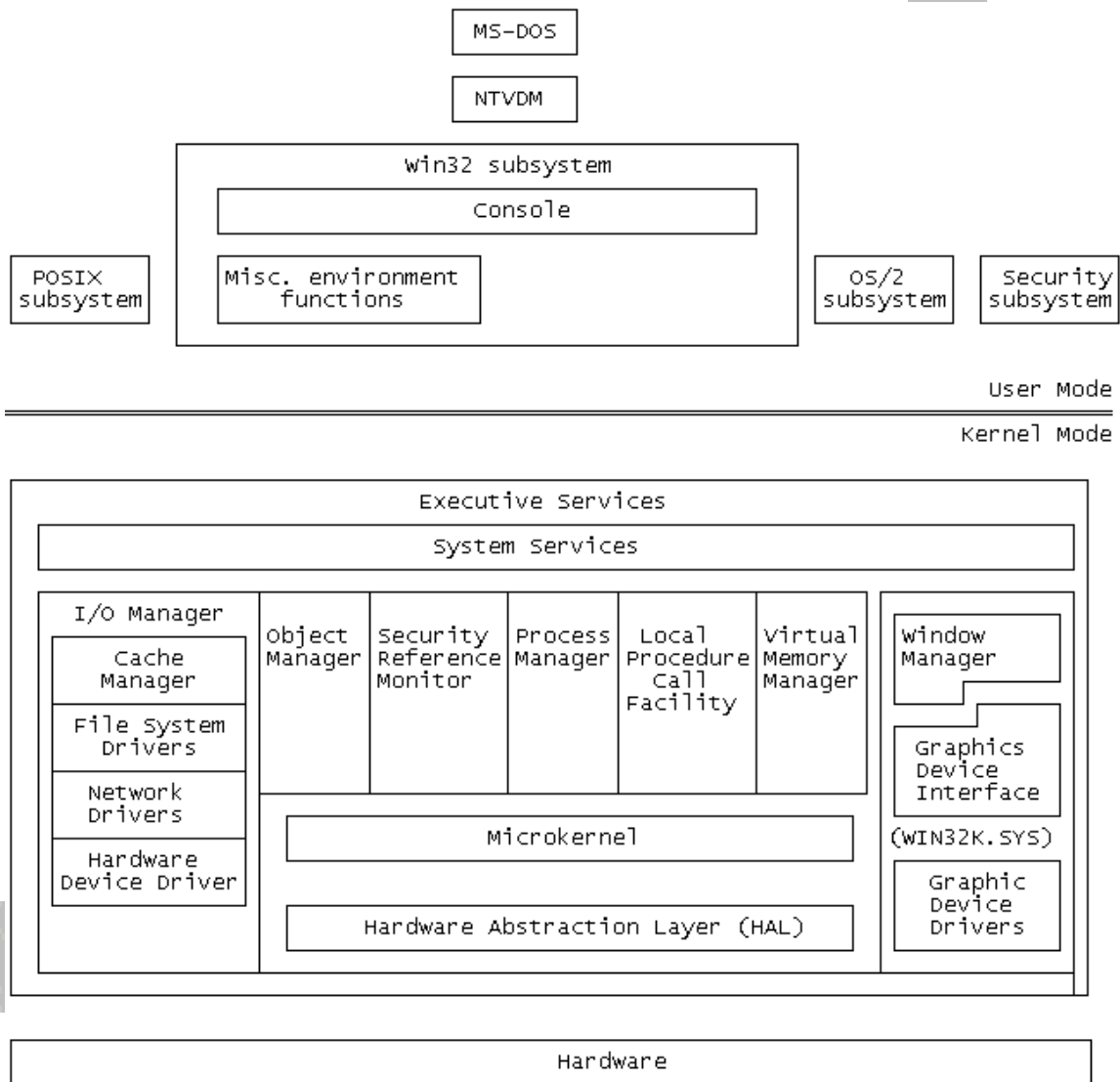
Windows NT:

- C Provides support for symmetric multiprocessing.
- C Has native networking functionality with a graphical user front-end.
- C Takes advantage of advanced processors such as the Intel 80486 and Pentium, as well as reduced instruction set computers (RISC) such as the MIPS R4000 and the DEC Alpha.

Advantages/Benefits:

- C Overall throughput, defined as a combination of processor performance, data transfer, and memory access is improved in relation to the existing predominant PC operating systems: DOS and Windows.
- C Memory protection ensures that multiple programs run in their own memory area and don't corrupt the memory read and used by other applications.
- C Symmetric multiprocessing lets Windows NT take advantage of multiple processors.

2 Architecture



3 Accessing the Windows NT System

Local Users

The Windows NT operating system allows multiple users to log on at the physical computer running Windows NT. Windows NT maintains account information for each user and stores customized settings that are restored when a user next logs on.

When a user logs on by typing an account name and password, Windows NT authenticates that user. If the account is valid and has not expired, the user gains access to the system.

Network Users

Network users access an Windows NT system over a network from another computer. Once connected, they can access shared directories, files, and resources such as printers.

Network connections under Windows NT have a client/server relationship. A Windows NT computer that shares its files and resources is the server and computers that access those resources are the clients.

4 Networking Features

Windows NT is an expandable system which supports a variety of network interface cards and network communications protocols.

Windows NT provides the following networking features:

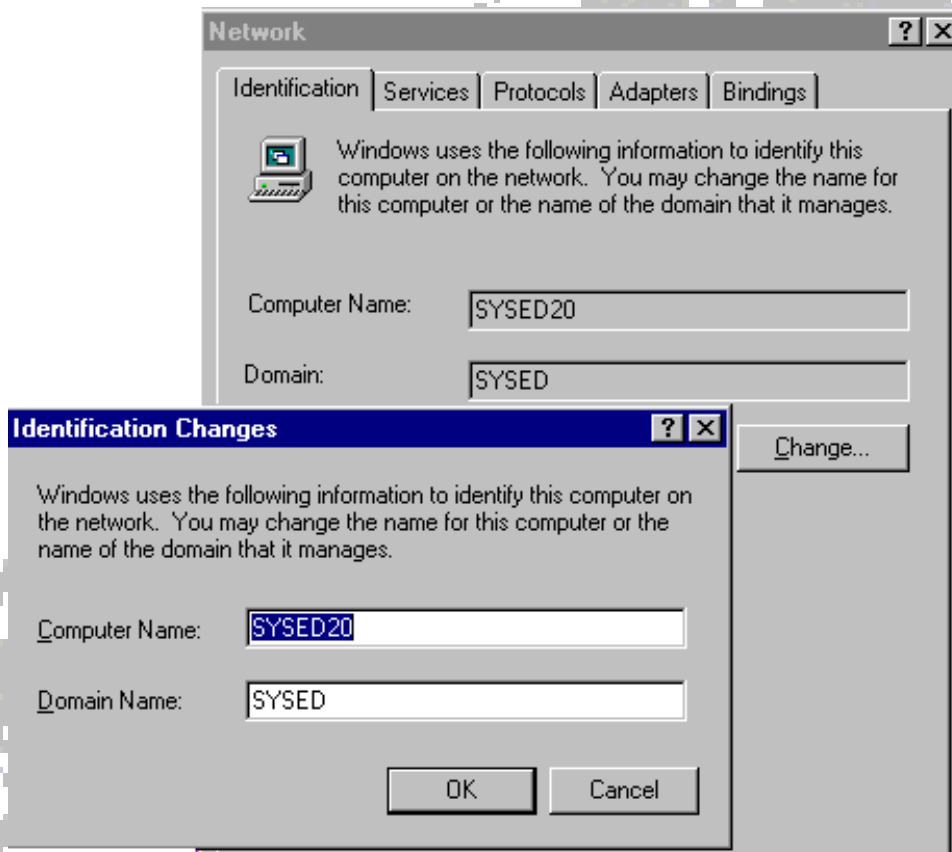
- C Directory and file-saving capabilities, and the ability to connect with shared directories and files on remote computers.
- C Sharing of a local printer and connection to shared printers on remote systems.
- C Messaging and electronic mail capabilities among users in workgroups and domains.
- C Industry-standard methods for establishing network connections and session management.
- C Remote Procedure Call (RPC) which enables a local workstation to run utilities and functions on remote workstations.

5 Computer Name

All Windows NT workstations that participate in a network must have a name assignment. It is usually designated during installation.

The Computer Name field can be changed from the Network Object in the Control Panel or the properties menu choice in the Network Neighborhood icon.

For a computer to participate in a Windows NT Server domain, an account must exist in the domain for the name specified in the Computer Name field.



6 Security and User Hierarchy

Users have accounts that require logon with password identification.

Logon account information is stored in a master database known as a security accounts manager (aka SAM) on each Windows NT system.

The account tracks various actions performed by a user for auditing purposes, such as logons, logoffs, and file accesses. Management tasks such as changing user accounts or server settings can also be tracked.

User Hierarchy

- C Users are prevented from examining the contents of memory.
- C Administrators and users can control file, directory, and resource (printers) access on their own system.
- C System administrators can track and view auditable events.

Permissions can be applied to shared directories, and administrators must create user accounts that require logon passwords and provide logon restrictions.

7 Sharing File Resources

Sharing file resources typically includes setting up shared directories and assigning user access privileges to those directories. The level of control over the shared resources depends on the type of file system on which the shared resource resides.

On a FAT file system, access can be controlled on a directory-by-directory basis, assigning access levels to each shared directory.

Access permissions can be assigned to a directory by group and by user. The only privileges which can be assigned, however, are read, change, and full control.

7.1 Providing Remote Users Access to Resources

Shared directories control remote access to the directory and have no restrictive effect on local users of the computer.

Three conditions must be met before a directory can be shared.

1.	The Server Service must be started.
2.	The user attempting to create the shared directory must be logged on with rights that permit sharing: C Administrators C Power Users C Server Operators (Windows NT Server domain controllers only)
3.	The user must have at least "List" permission (NTFS partition only) to the directory.

7.2 Sharing a Directory

A directory can be shared through the:

- C Explorer
- C My Computer
- C Net share command from the command prompt.
- C Share As command in the File Manager Disk menu.
- C Server Manager on a Server in a Windows NT Domain.

Windows NT Workstation allows a maximum of 10 remote users to be simultaneously connected to any shared directory.

If a session is idle for 15 minutes, the client will be disconnected from the server, although any drive mappings will remain.

7.3 Shared Directory Permissions

Shared directory permissions can provide a level of security to local resources when accessed over the network. Regardless of the partition's file system, permissions can be set on a shared directory.

These permissions are effective only when the directory is accessed over the network, and they apply to all files and subdirectories under the shared directory.

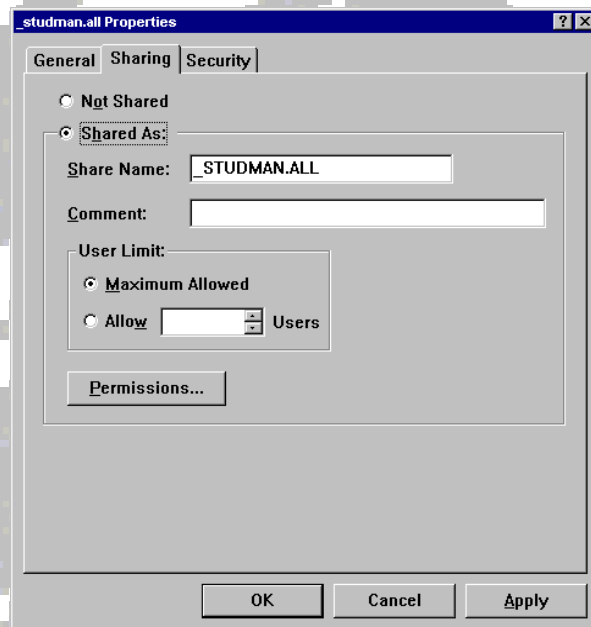
If the shared directory is on an NTFS partition, the permissions that are set on the shared directory operate in addition to the NTFS permissions on the local directory.

In instances like this, where two sets of permission apply, the most restrictive permission takes precedence.

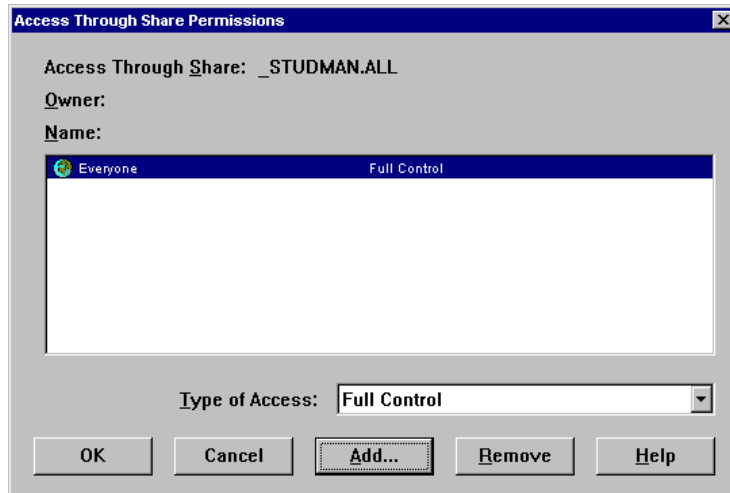
It is possible to give permissions to users or groups of users, or both. Each user or group added can be given different levels of access if necessary.

No Access	With this permission set, a user can establish a connection, but access to the directory is denied and the contents are not listed.
Read	A user or group with the Read permission can perform the following tasks: <ul style="list-style-type: none"> C Display subdirectory names and filenames. C Display the data and attributes of files. C Run program files. C Change to the directory's subdirectories.
Change	A user or group with the Change permission can perform the following tasks, in addition to those of Read: <ul style="list-style-type: none"> C Create subdirectories and add files. C Change data in, and append data to, files. C Change file attributes. C Delete subdirectories and files
Full Control	A user or group with the Full Control permission can perform the following tasks, in addition to those of Change: <ul style="list-style-type: none"> C Change file permission. C Take ownership of files on NTFS volumes.

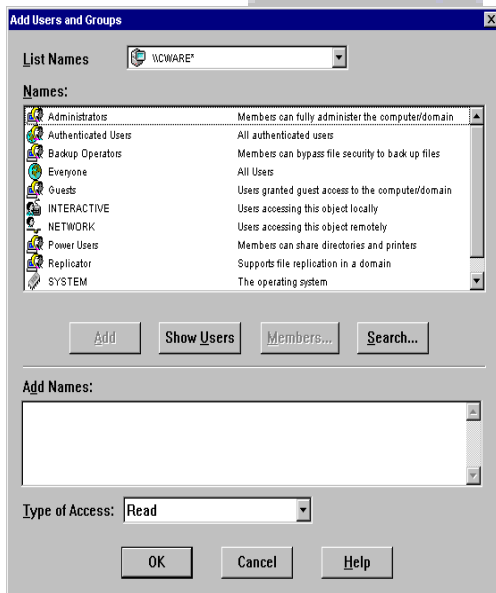
Sharing a Folder (aka Directory)



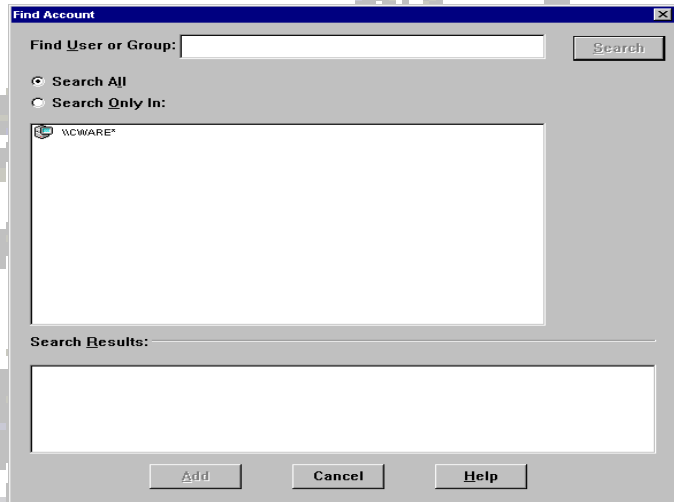
Type of Access



Adding User and Groups



Find User or Group

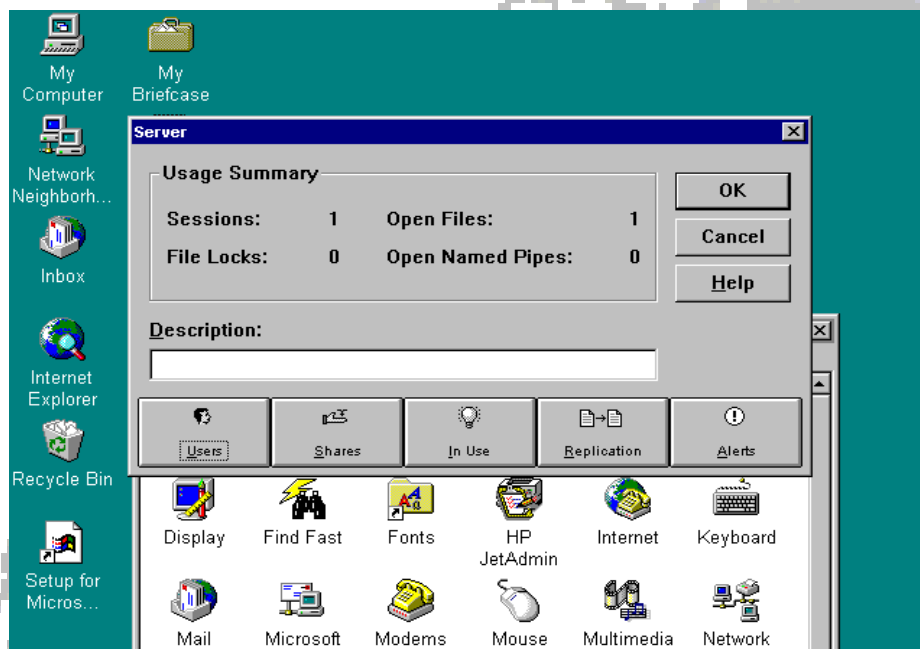


7.4 Stop Sharing a Directory

When a shared directory is no longer needed, sharing can be stopped to prevent remote access to the files. Local access to the files and directories is still maintained, however.

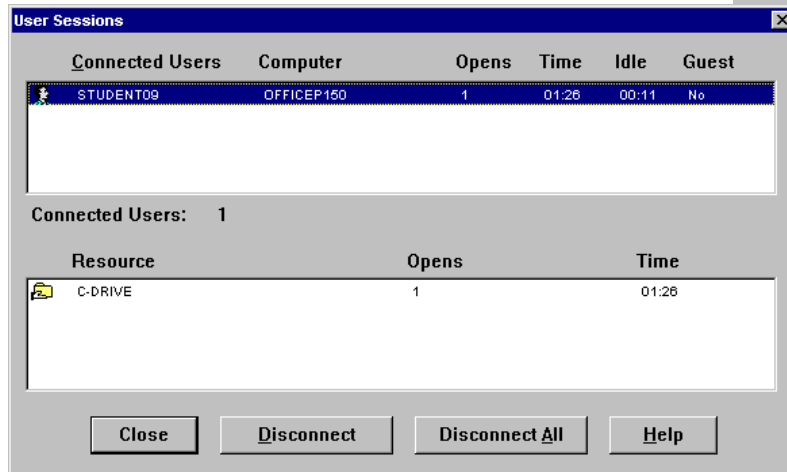
Any users connected to the shared directory at the time sharing is stopped are disconnected automatically and might lose data. If any user has an open file on this share, a dialog box appears, asking the procedure is to be continued.

To view connected users, use the Server tool in Control Panel.



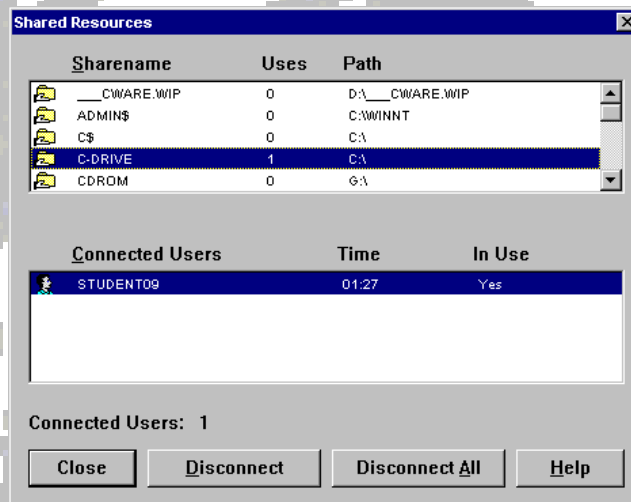
From the Server Utility

Connected Users and Shares



From the Server Utility

Shares and Connected Users



7.5 The Default Administrator Shares

Every time a Windows NT computer starts, it creates some shared resources automatically. The root directory of each hard disk partition is shared, using the drive letter, appended with a dollar sign (\$). This occurs only for hard disk partitions, not floppy or CD-ROM drives.

The \$ makes the sharename invisible to browsing, though still accessible by typing the sharename, such as C\$. A user can connect to an administrative hidden share on another Windows NT computer only when the correct administrative username and password are known.

After connection the user has access to the entire partition.

To view all shares, use the Server tool in Control Panel. ADMIN\$ is one of the special shares. It is a resource used by the system during remote administration of a computer. The path of this resource is always the path to the Windows NT directory.

Hidden shares are protected by an internal permissions list, called the Access Control List (ACL), which allows only administrators to connect to these shares over the network. This internal ACL cannot be modified by any user, including the Administrator.

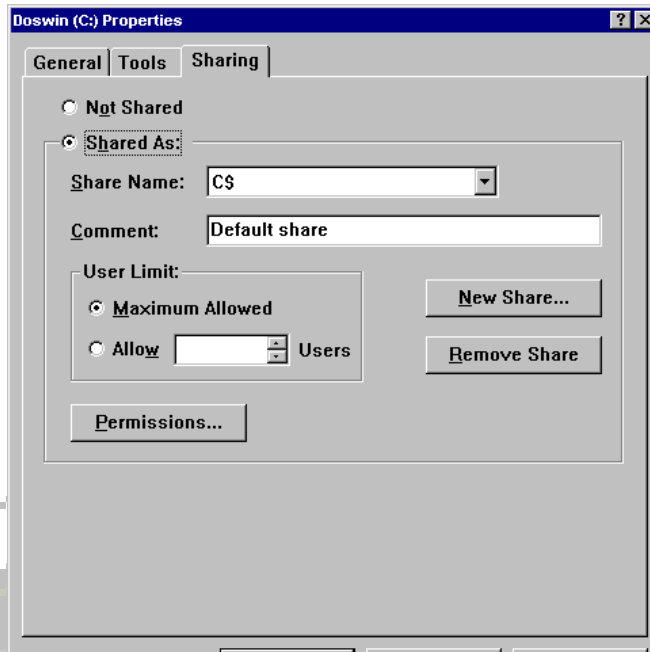
It is possible to stop sharing the default administrator shares.

However, the next time the computer is restarted, all the administrator shares will automatically be shared again.

There is no way to permanently disable the administrator shares on a Windows NT computer.

Anyone with the permission to share a directory can add a \$ to the end of the sharename. Doing so creates a hidden share that does not show up when browsing the network. The creator can apply any permissions wanted to the hidden share.

Folder Properties Accessed via Explorer



NET SHARE from the Command Prompt

Share name	Resource	Remark
F\$	F:\	Default share
IPC\$		Remote IPC
ADMIN\$	C:\WINNT	Remote Admin
C\$	C:\	Default share
D\$	D:\	Default share
E\$	E:\	Default share
print\$	C:\WINNT\System32\spool\DRIVERS	Printer Drivers
C-DRIVE	C:\	C: on Courseware machine
CDROM	G:\	
D-Drive	D:\	D: on Courseware machine
E-Drive	E:\	E: on Courseware machine
F-Drive	F:\	F: on Courseware machine
SasrawCD	E:\SasrawCD	
SmartSuite97	E:\Cdbak\SmartSuite97	
WINNT	D:_CWARE.WIP\WINNT	
HPLaserJ	LPT1:	Spooled HP LaserJet Series II

The command completed successfully.

7.6 Locating Hidden Shares

To identify the hidden shares on the Windows NT Workstation.

1. Log on as an administrator and start Control Panel.
2. Start Server, and then choose Shares.
Notice that all shares, including hidden shares, are listed in the Sharename column.
3. Locate the shares which have a \$ sign added to the end of the sharename.
4. Choose Close.

7.7 Managing Shared Directories

Both the Explorer and Server can be used for managing shared directories. File Manager and the command prompt could also be used.

Using Server has the advantage of bringing all shared directories at once.

To control the directory shares on a computer, go to Control Panel and open the Server and select the shares to be managed.

7.8 Shares - Connecting / Disconnecting

The Server application from the Control Panel can be used to disconnect all connected users or a single connected user.

1. Select the share to be managed.
2. Select the user to be disconnected via the Disconnect button.
or
Select the Disconnect All button.

Both the Users pushbutton and the Shares pushbutton can be used.

Disconnecting a user who is using resources can result in the loss of data. It is a good idea to warn connected users before disconnecting them.

While you are administering another computer remotely, your user account is listed as a connected user for the IPC\$ share. It will not be disconnected.

8 File Systems

File Allocation Table File System

FAT is the file system for DOS. It uses a file naming format with an eight-character filename and a three-character extension.

Windows NT can access FAT drives, but if you boot the system with DOS, you cannot access NTFS drives.

8.1 NTFS

The New Technology File system provides long filenames, data protection/recovery, and security through directory and file permissions.

NTFS supports large hard disks and the storage of files over multiple hard disks; this is known as spanning volumes.

NTFS provides built-in security features that control file ownership and access.

Files on an NTFS volume are not accessible from DOS or other operating systems.

NTFS is part of the Windows NT security system, but only when you use NTFS.

File naming rules:

C Maximum of 256 characters in file and directory names.

You can use multiple period-separated extensions, if necessary, to create filenames such as REPORTS.SALES.SMITH.JUNE93.

C Names cannot include these symbols:

? \ * " < > | : .

C Windows NT preserves the uppercase/lowercase format of the name specified but does not use case to distinguish between filenames.

Wildcard characters (? and *) can be used for searching and listing filenames.

8.2 File Naming Conventions

The file systems supported by Windows NT have naming conventions.

Files within the same directory cannot have the same name, but you can use names that have characters in common as part of a strategy to keep your files organized.

Windows warns you if you try to create a file with a name that's already in use by another file.

Only drives formatted to the NTFS file system can store files with long filenames and security attributes. Use a mix of periods and upper and lowercase letters to differentiate parts of the filename.

Not all Windows NT applications let you save or open files that have long filenames.

All NTFS files are assigned a name that follows the DOS convention if copied to a DOS file system.

8.3 Recoverable File System

Windows NT has a recoverable file system, which adds very little overhead to the file system. All modifications to files on an NTFS volume are logged with redo and undo information.

- C Redo provides information on how to repeat transactions while undo provides information on how to "roll back" transactions.
- C With undo information, the disk can be restored to the state it was in before the transaction was ever started.

The recovery options work on all drives formatted to the NTFS file system; no special equipment is required to use this option.

Consider a scenario where the power goes out while a transaction is being written, the disk contains only half the correct information.

Upon rebooting, Windows NT scans the disk and determines whether it needs to redo transactions, it looks up the undo information and restores the records to their pre-transaction state.

9 Printing

In Windows 3.1, you had to install a printer driver on your own system when accessing a printer of that type on a remote network computer.

The location where printer drivers are stored for shared network printers has been changed. In Windows NT, printer drivers are stored on the computer where the printer is connected (ie. the server). When you access the printer, your application uses the printer driver on that computer.

Permissions can also be set that control the type of access users have to printers.

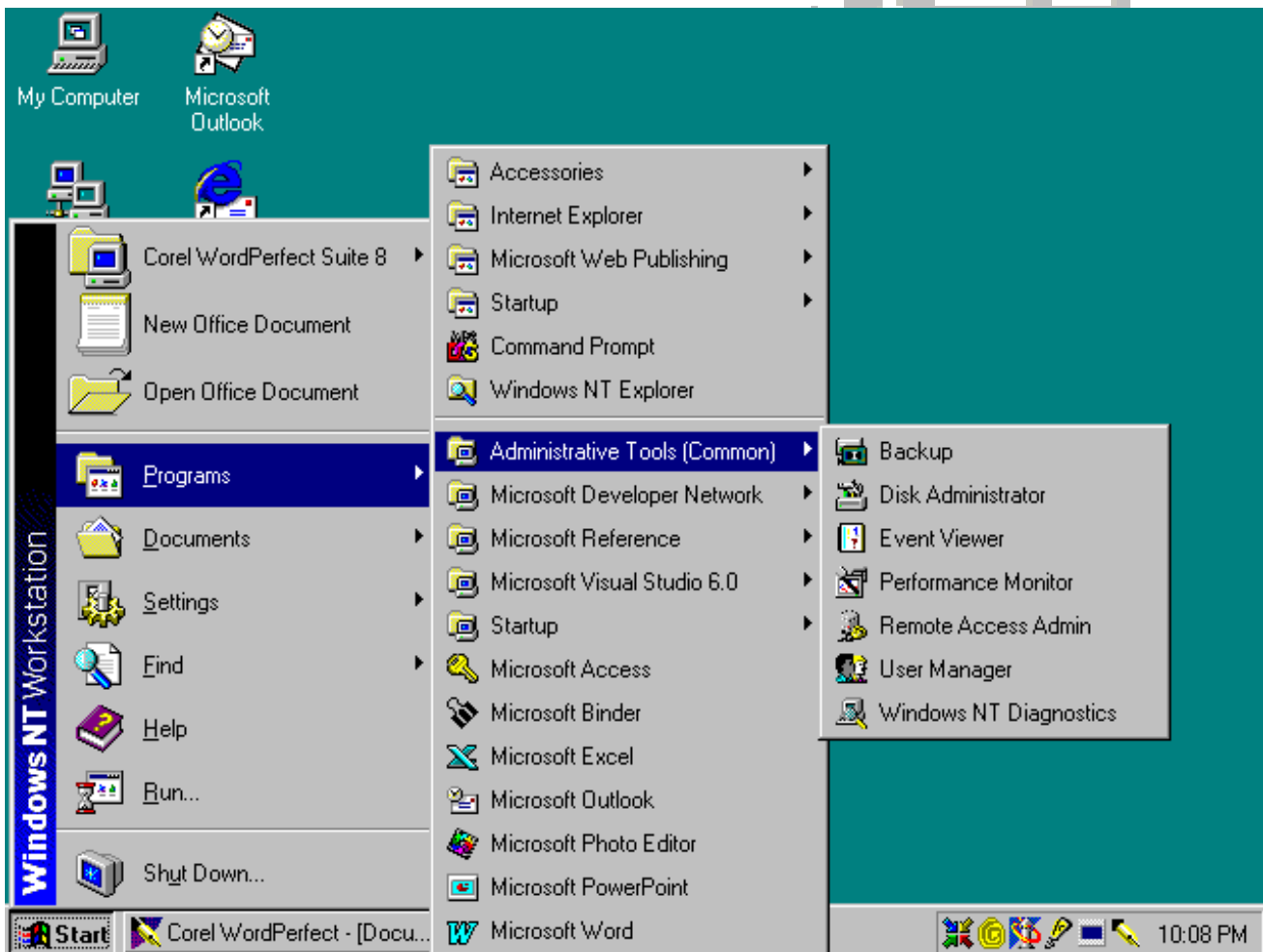
Users can be prevented/allowed access to a printer or granted the ability to control documents in the printer's queue.

Administrators have full control over printers.

10 Administrative Tools

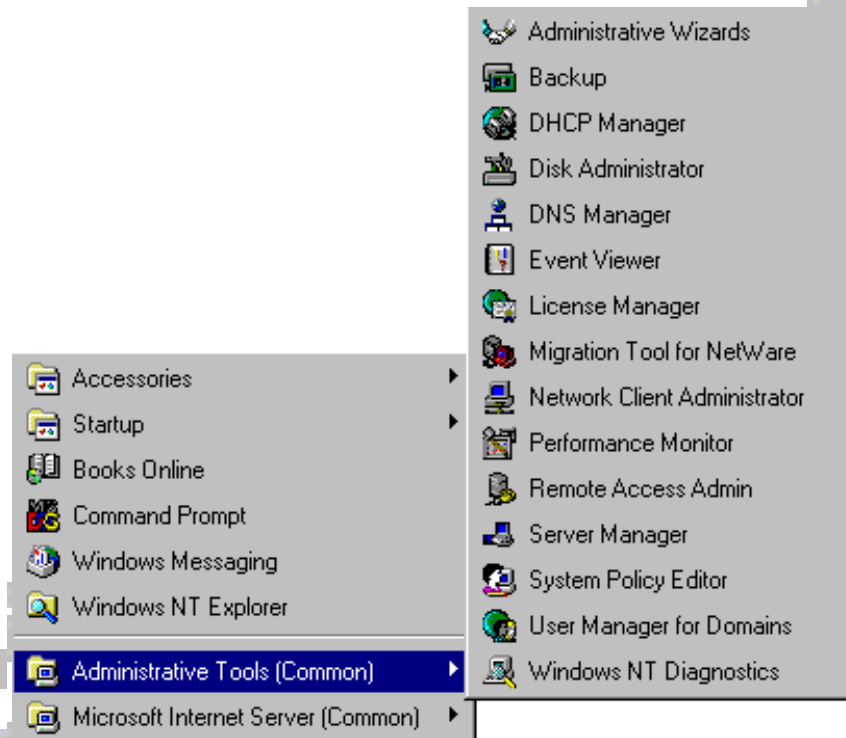
10.1 Windows NT Workstation

The standard Administrative tools which can be accessed through the Start Menu and cascaded menu submenus are:



10.2 Windows NT Server

The standard Administrative tools which can be accessed through the Start Menu and cascaded menu submenus are:



Tool	Purpose
Administrative Wizards	Step-by step instructions for user accounts, group management, file and folder access, add printer, add/remove programs, install new modem, network client administrator, and license compliance.
Backup	Used to back up directories and files on the system.
DHCP Manager	Used for managing DHCP servers and the configuration options.
Disk Administrator	Used to prepare and manage the disks on the system.
DNS Manager	Used for configuring/add servers which map IP addresses to host names on workstations which have TCP/IP installed.
Event Viewer	Used to view logs that display system, security, and application events for troubleshooting and auditing purposes.
License Manager	Tracks the software product history of software licenses by product and per seat on Windows NT Server across the browsable network.

Tool	Purpose
Migration Tool for NetWare	Program for converting the Novell bindery and NDS accounts database to a structure/format which can be utilized by Windows NT Server.
Network Client Administrator	Used to make Network Installation Startup and Installation Disk Sets, copy client-based administrative tools, and Remote Boot Client Information.
Performance Monitor	Used to track system usage, monitor performance, perform troubleshooting, and plan for system expansion.
Remote Access Admin	Used for managing communication ports, starting/stopping/pausing RAS and granting permissions to user accounts on RAS servers.
Server Manager	Used to manage domains and computers.
System Policy Editor	Used for creating policies and modifying policies on a per user/group or machine basis.
User Manager for Domains	Used to create accounts that other users log onto and groups that provide system security. Also provides for creating customized user profiles.
Windows NT Diagnostics	Used for gathering information and troubleshooting.
WINS	Used for mapping NetBios names to IP addresses and configuring Windows NT Server options and replication services.

11 Control Functions/Control Panel

11.1 Windows NT Server

Name	Description
SCSI Adapters	Add/Remove SCSI adapters and view their properties.
Printers	Adds, removes, and changes printer properties.
Microsoft Postoffice	Administers a Microsoft Workgroup Postoffice.
HP Jet Admin	Allows to configure and monitor HP printers
Licensing	Change licensing options.
Accessibility Options	Changes accessibility options for your system.
Date/Time	Changes, date, and time zone information.
Display	Changes display settings.
Keyboard	Changes keyboard settings.
Mouse	Changes mouse settings.
Multimedia	Changes multimedia devices settings.
Sounds	Changes system and program sounds.
Regional Settings	Changes the appearance of numbers, currencies, dates, and times.
Internet	Changes your Internet settings.
Telephony	Configure Telephony Drivers and Dialing Properties.
Monitoring Agent	Configure the Network Monitoring Agent software.
Console	Configures console properties.
Network	Configures network hardware and software.
UPS	Configures the Uninterruptible Power Supply.
Tape Devices	Detect tape devices and view their properties.
Server	Displays and manages local server properties.
Fonts	Displays, adds, and removes fonts.
PC Card (PCMCIA)	Enables PCMCIA sockets and changes PC Card (PCMCIA) settings.
Modems	Installs a new modem and changes modem properties.
ODBC	Maintains ODBC data sources and drivers.
Mail and Fax	Microsoft Windows Messaging Profiles.

Name	Description
Dial-up Monitor	Monitors status of dial-up connections.
System	Provides system information and changes environment settings.
Add/Remove Programs	Sets up programs and creates shortcuts.
Ports	Specifies serial port communications settings.
Devices	Starts and stops device drivers.
Services	Starts, stops, and configures services.

12 Widely Used Microsoft Clients

The preferred client for Windows NT Server domain is Windows NT Workstation.

Other Microsoft clients, Windows for Workgroups and Windows 95/98 are widely used and will continue to be so for many years to come. Both Windows for Workgroups and Windows 95/98 can be configured to participate both in peer-to-peer based networks and domain based networks.

Networking for Windows for Workgroups can be done during the initial installation or configured later. The basic steps in the configuration are setting up drivers for the network interface card (NIC), selecting the access protocol, and making the appropriate choices for enabling resource sharing, logon user id, specifying the network server, and choosing other NOS specific features.