

NETWORK MANAGEMENT AND ADMINISTRATION

Chapter 5

Administering Windows 2000 Server (The Basics)

Detailed Study Notes for Engineering Students

5.1 Working With User Accounts

5.2 Working With Windows 2000 Security Groups

5.3 Working With Shares

5.4 Administering Printer Shares

5.5 Working With Windows 2000 Backup

Includes diagrams, tables, 15 MCQs with answer key and 10 broad questions

Contents

Chapter Overview	3
Windows 2000 Server at a glance	3
5.1 Working With User Accounts	4
5.1.1 Adding a User	4
5.1.2 Modifying a User Account	5
5.1.3 Deleting or Disabling a User Account	6
5.2 Working With Windows 2000 Security Groups	8
5.2.1 Creating a Group	9
5.2.2 Maintaining Group Membership	9
5.3 Working With Shares	11
5.3.1 Understanding Share Security	11
5.3.2 Creating Shares	12
5.3.3 Mapping Drives	13
5.4 Administering Printer Shares	15
5.4.1 Setting Up a Network Printer	15
5.4.2 Print Permissions	16
5.4.3 Managing Printers and Queues	16
5.5 Working With Windows 2000 Backup	18
5.5.1 Using Windows 2000 Servers Backup Software	18
5.5.2 Steps to Back Up Files	19
5.5.3 Steps to Restore Files	20
5.5.4 Backup Planning and Good Practice	20
Chapter Summary (Quick Revision)	22
Multiple Choice Questions	23
Answer Key for MCQs	25
Broad Questions	26

Chapter Overview

Once a network is built, it must be administered every day. Administration means controlling who may use the network (**user accounts**), organizing users for easier control (**groups**), making folders available to others (**shares**), providing printing (**printer shares**) and protecting data against loss (**backup**). This chapter explains these basic tasks on **Microsoft Windows 2000 Server**.

After studying this chapter, a student should be able to:

- add, modify, disable and delete user accounts;
- create security groups and maintain their membership;
- understand share security, create shares and map network drives;
- set up and manage shared network printers;
- plan and perform backup and restore using Windows 2000 Backup.

Windows 2000 Server at a glance

Windows 2000 is built on the Windows NT technology and is a 32-bit operating system. It was released in three server editions: **Windows 2000 Server** (departmental servers), **Advanced Server** (clustering and larger hardware) and **Datacenter Server** (very large systems). Its most important new feature was **Active Directory**, a directory service that stores information about users, computers, groups, printers and shared folders in one searchable database.

Server role	Meaning	Where accounts are kept
Domain controller (DC)	Server that holds a copy of Active Directory and authenticates logons for the domain	Active Directory database (shared by all DCs of the domain)
Member server	Server that belongs to a domain but is not a DC (file, print, database servers)	Domain accounts in AD; local accounts in its own local database
Stand-alone server	Server in a workgroup, not part of a domain	Local Security Accounts Manager (SAM) database on that server

Administrative tools

Most tools are opened from **Start, Programs, Administrative Tools**. They are snap-ins for the **Microsoft Management Console (MMC)**, a common window that can host many tools.

Tool	Used for
Active Directory Users and Computers	Domain user accounts, groups, computers, shared folders and printers listed in the directory (on a DC)
Computer Management	Local users and groups, shared folders, services, disk management and event logs of one computer
Windows Explorer	Sharing folders, NTFS permissions, mapping network drives
Printers folder	Adding printers, sharing them, setting print permissions and managing queues
Backup (ntbackup)	Backup and restore of files and system state

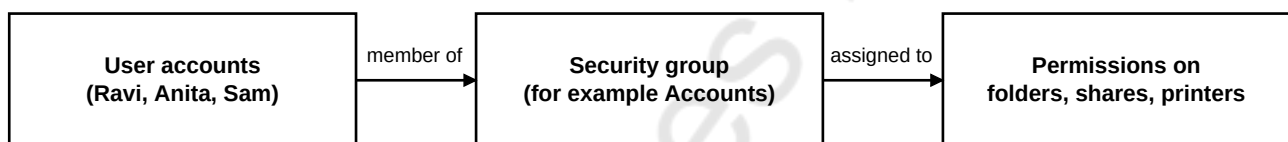
Windows 2000 reached end of support in 2010, but its ideas (accounts, groups, permissions, shares, spooling, backup types) carry over to later Windows Server versions, although menus differ.

5.1 Working With User Accounts

A **user account** identifies a person (or service) to the network. It contains the user name, password and settings, and it is the basis for deciding what the user may do. Every user account receives a unique **Security Identifier (SID)**; Windows uses the SID, not the name, when it checks permissions. The administrator creates accounts so that each person can **log on** (authenticate) and then access only the resources for which permission has been given.

Types of user accounts

Type	Created in	Used for
Domain user account	Active Directory on a domain controller	Logon to any computer in the domain; accounts are central
Local user account	Local database of a stand-alone or member server (Computer Management)	Logon to that single computer only
Built-in account	Created automatically at installation	Administrator (full control, cannot be deleted); Guest (disabled by default)



Assign permissions to groups, not to individual users

Fig. 5.1: Users, groups and permissions

The relationship in Fig. 5.1 is the key idea of administration: accounts are put in groups, and permissions are given to the groups. This is explained in Section 5.2.

5.1.1 Adding a User

To add a domain user the administrator opens **Active Directory Users and Computers**, selects the container (*Users* or an organizational unit) and chooses **Action, New, User** (or right-clicks the container).

Steps to create a user in Active Directory:

- 1 Click **Start, Programs, Administrative Tools, Active Directory Users and Computers**.
- 2 Expand the domain, right-click the **Users** container (or an OU), then choose **New, User**.
- 3 Enter **First name**, **Initials** (optional) and **Last name**. The **Full name** fills automatically.
- 4 Enter the **User logon name** (for example *ravi*) and select the domain suffix. The **pre-Windows 2000 logon name** (up to 20 characters) is used by older clients and usually fills automatically.
- 5 Click **Next** and type the **Password** twice. Choose the password options (see below).
- 6 Click **Next**, check the summary and click **Finish**.

Password option	Meaning	Typical use
User must change password at next logon	Forces the user to choose a private password at first logon	New accounts (recommended)

Password option	Meaning	Typical use
User cannot change password	User may not change the password	Shared or service accounts
Password never expires	Ignores the maximum password age	Service accounts (use with care)
Account is disabled	Account exists but cannot be used for logon	Prepared accounts for future staff

Windows 2000 passwords may be up to 127 characters long. A good password is long and combines upper-case and lower-case letters, digits and symbols, and is not a name, date or dictionary word. The domain **password policy** (minimum length, maximum age, complexity and history) enforces these rules.

Creating a local user (stand-alone or member server)

Open **Computer Management**, expand **System Tools, Local Users and Groups**, right-click **Users**, choose **New User**, fill in User name, Full name, Description and Password, select the password options and click **Create**. The same job can be done from the command line:

```
net user ravi P@ssw0rd1 /add /fullname:"Ravi Kumar" /domain (domain account)
net user ravi P@ssw0rd1 /add (local account)
```

5.1.2 Modifying a User Account

To change an account, double-click it (or right-click and choose **Properties**). The Properties window contains several tabs.

Tab	Contents
General	Name, description, office, telephone, e-mail, web page
Address / Telephones / Organization	Contact details, job title, department, manager
Account	Logon name, Logon Hours , Log On To (computers allowed), password options, Account expires , unlock account
Profile	Profile path, logon script , home folder and the drive letter it is mapped to
Member Of	Groups to which the user belongs; add or remove groups
Dial-in	Remote access permission and call-back settings
Environment / Sessions / Remote control / Terminal Services Profile	Terminal Services (remote desktop) settings

Common modification tasks

- **Reset a forgotten password:** right-click the account, choose **Reset Password**, type the new password and tick *User must change password at next logon*.
- **Unlock an account:** after too many wrong passwords the account is locked out; on the Account tab clear *Account is locked out*.
- **Restrict logon hours:** Account tab, **Logon Hours**, select the allowed time blocks (for example only college hours for student accounts).
- **Limit logon computers:** Account tab, **Log On To**, list the computers the user may use.

- **Set an expiry date:** Account tab, **Account expires**, choose an end date for temporary users such as visiting faculty or trainees.
- **Rename:** right-click, choose **Rename**. Because the SID does not change, the permissions and group membership remain.
- **Move** the account to another container or OU, or **Copy** it to create a similar account quickly (group memberships are copied, but the password and personal details are not).
- **Home folder and profile:** set on the Profile tab so that the user's files follow him or her to any computer.

5.1.3 Deleting or Disabling a User Account

When a person leaves or stops needing the network, the account must not be left active, because unused accounts are an easy way into the network. The administrator has two choices.

Feature	Disable account	Delete account
How	Right-click the account, choose Disable Account (the icon shows a red cross)	Right-click the account, choose Delete and confirm
Can the user log on?	No	No
Is the account kept?	Yes; it can be enabled again	No; it is removed permanently
SID, permissions, group membership	Kept	Lost; a new account with the same name gets a new SID and does not inherit the old permissions
Typical use	Leave of absence, investigation, staff on holiday, unused accounts before final removal	Permanent departure, after files have been transferred or archived

Good practice: first disable the account, keep it for an agreed period (for example 30 to 90 days), transfer or back up the user's files and mailbox, and only then delete it. Never delete the built-in *Administrator* account (it cannot be deleted); rename it and use a strong password instead, and keep the *Guest* account disabled.

Command-line equivalents

```
net user ravi /active:no           (disable the account)
net user ravi /active:yes         (enable the account)
net user ravi /delete             (delete the account)
net user ravi                     (display information about the account)
```

Troubleshooting logon problems

Message or symptom	Likely cause	Remedy
Logon failed: wrong user name or password	Wrong password or Caps Lock on	Retype; if forgotten, administrator resets the password
Account has been locked out	Too many failed attempts	Administrator unlocks the account on the Account tab
Account is disabled	Account was disabled by administrator	Enable the account if the user is still authorized
Account has time restrictions	Logon hours do not allow logon now	Check Logon Hours or log on in the allowed time
Cannot log on to this workstation	Log On To list excludes the computer	Add the computer to the Log On To list
Password has expired	Maximum password age reached	User changes the password at logon or the administrator resets it

5.2 Working With Windows 2000 Security Groups

A **group** is a collection of user accounts (and sometimes other groups or computers) that are managed together. Instead of giving the same permission to 60 students one by one, the administrator gives it once to the group *Students*. When a new student joins, the account is simply added to the group and all the permissions follow. Groups therefore save time, reduce errors and make the system easier to audit.

Group types

Type	Purpose	Has a SID?
Security group	Used to assign permissions and rights to resources; can also be used as an e-mail list	Yes
Distribution group	Used only for e-mail and other distribution lists; cannot be used to set permissions	No

Group scope

The **scope** of a group decides where the group can be used and who can be a member. Windows 2000 has three scopes. **Domain modes** matter: a domain in **mixed mode** still supports older Windows NT domain controllers and cannot use universal security groups, while a domain in **native mode** (all domain controllers run Windows 2000) supports all features, including universal security groups and full nesting.

Scope	Members can include	Can be given permissions in
Domain local	Accounts, global groups and universal groups from any domain (native mode: also domain local groups of same domain)	Its own domain only
Global	Accounts and global groups (native mode) from the same domain only	Any domain in the forest
Universal (native mode only for security groups)	Accounts, global groups and universal groups from any domain	Any domain in the forest

On a stand-alone or member server, **local groups** are used; they exist only in that computer's local database and can contain local users and (on a member server) domain users and global groups.

Built-in and default groups

Group	Purpose
Administrators	Full control of the computer or domain
Account Operators	Create and manage user and group accounts (not Administrators)
Backup Operators	Back up and restore files regardless of permissions
Print Operators	Manage printers and print queues on domain controllers
Server Operators	Manage servers: shares, backups, shutdown
Power Users (local)	Limited administrative rights on a workstation or member server
Users / Domain Users	Ordinary users; every new domain account is placed in Domain Users
Guests / Domain Guests	Temporary users with very limited access
Domain Admins	Administrators of the domain; added to every computer's Administrators group
Enterprise Admins / Schema Admins	Forest-wide administration and Active Directory schema changes (very restricted)

5.2.1 Creating a Group

Steps to create a security group in Active Directory:

- 1 Open **Active Directory Users and Computers**.
- 2 Right-click the container or OU where the group will be stored and choose **New, Group**.
- 3 Type the **Group name** (for example **CSE_Students**). The pre-Windows 2000 name fills automatically.
- 4 Select the **Group scope** (Domain local, Global or Universal) and the **Group type** (Security or Distribution).
- 5 Click **OK**. Then open the group Properties to add a description, managed-by information and members.

For a local group on a member or stand-alone server, use **Computer Management, Local Users and Groups, Groups**, right-click and choose **New Group**, then enter the group name, description and use the **Add** button to select members.

```
net localgroup Accounts /add          (create a local group)
net group CSE_Students /add /domain   (create a global group in the domain)
```

5.2.2 Maintaining Group Membership

Membership changes constantly as students and staff join, move or leave. There are two ways to change membership.

- **From the group:** open the group Properties, click the **Members** tab, then **Add** (select the users, computers or groups and click OK) or **Remove**.
- **From the user:** open the user Properties, click the **Member Of** tab and use **Add** or **Remove** to join or leave groups.
- **Several users at once:** select multiple accounts in Active Directory Users and Computers, right-click and choose **Add members to a group**.

- **Delete a group:** right-click and choose Delete. Permissions given to that group are lost, so check where the group is used first.

```
net localgroup Accounts ravi /add          (add a user to a local group)
net localgroup Accounts ravi /delete       (remove the user from the group)
net group CSE_Students anita /add /domain
net localgroup Accounts                    (list members of the group)
```

A recommended strategy for groups

Microsoft recommends the sequence **A, G, DL, P**: put **A**ccounts into **G**lobal groups (organized by job or department), put global groups into **D**omain **L**ocal groups (organized by resource and access level, such as *Lab_Folder_Modify*) and give **P**ermissions to the domain local groups. When the resource or the staff changes, only one link of the chain needs changing.

Rules of good group administration

- Give permissions to groups, never directly to users, wherever possible.
- Use names that show purpose and scope, for example *G_Faculty_CSE*.
- Apply the **principle of least privilege**: add users to Administrators or Server Operators only when unavoidable.
- Review membership of powerful groups regularly and remove users who have left.
- Document each group: purpose, owner and the resources it can access.

5.3 Working With Shares

A **share** is a folder (or drive) on a server that is made available to users across the network. The folder keeps its place on the server disk; the **share name** is the name by which network users reach it, written in **UNC** (Universal Naming Convention) form: \\servername\sharename, for example \\SERVER1\Data. Sharing is the basic way in which a file server delivers its service.

5.3.1 Understanding Share Security

Access to shared data is controlled by two independent sets of permissions. Understanding how they combine is the most important part of this section.

A. Share permissions

Share permissions apply **only to users who connect over the network**. They can be set on any shared folder, whichever file system is used (FAT or NTFS). There are three levels, and the default on a new share in Windows 2000 is **Everyone: Full Control**.

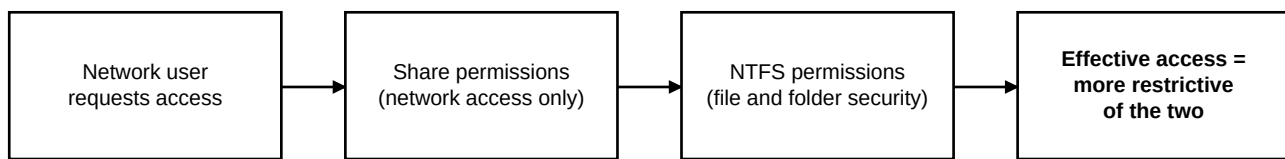
Share permission	What the user can do
Read	View folder and file names, open files and run programs
Change	Everything in Read, plus add files and folders, modify and delete files
Full Control	Everything in Change, plus change permissions and (on NTFS) take ownership

B. NTFS permissions

NTFS is the Windows NT file system. Its permissions apply to every user, **both at the server console and across the network**, and can be set on individual files and folders. They are available only on NTFS volumes (the Security tab does not exist on FAT volumes), which is one reason NTFS is the recommended file system for servers.

NTFS permission	What the user can do
Read	View files and folders, attributes and permissions
Write	Create files and folders, change attributes
List Folder Contents (folders only)	See names of files and subfolders
Read and Execute	Read plus run programs
Modify	Read, write, execute and delete
Full Control	All of the above, plus change permissions and take ownership

C. How permissions combine



A user logged on at the server console is controlled by NTFS permissions only

Fig. 5.2: Share permissions and NTFS permissions work together

- Permissions from **different groups are cumulative**: a user who is in two groups receives the sum of the permissions of both groups (for the same kind of permission, share or NTFS).
- **Deny overrides Allow**: an explicit Deny (for example No Access) always wins over Allow.
- When both share and NTFS permissions apply (a network user on an NTFS volume), the **effective permission is the more restrictive of the two results**.
- NTFS permissions are normally **inherited** by subfolders and files from the parent folder; inheritance can be blocked on the Security tab, Advanced button.
- A new file takes the permissions of its folder, and a file that is **moved** within the same NTFS volume keeps its own permissions, while a **copied** file takes the permissions of the destination folder.

Worked example

Share permission	NTFS permission	Effective permission over the network
Full Control	Read	Read (NTFS is more restrictive)
Read	Full Control	Read (share is more restrictive)
Change	Modify	Change / Modify level (both allow it)
Full Control	No access (Deny)	No access (Deny overrides)

Recommended practice: leave the share permission at *Full Control* for a suitable group (or Change) and control the real detail with NTFS permissions, which are more powerful and apply locally and remotely. Replace *Everyone* by specific groups such as *Authenticated Users* or a department group.

5.3.2 Creating Shares

To share a folder the administrator must be a member of Administrators, Server Operators (on domain controllers) or Power Users (on member servers). The folder is shared in either of two ways.

Method 1: Windows Explorer

- 1 Right-click the folder and choose **Sharing** (the Properties window opens on the Sharing tab).
- 2 Select **Share this folder**.
- 3 Type the **Share name** (this is the name seen by network users) and an optional **Comment**.
- 4 Set the **User limit**: Maximum allowed, or Allow a fixed number of users.
- 5 Click **Permissions**, remove *Everyone* if necessary, click **Add** and choose the groups, then tick Allow for Read, Change or Full Control.
- 6 Optionally click **Caching** to allow offline use, then click **OK**. The folder icon changes to show a hand.

Method 2: Computer Management

Open **Computer Management, System Tools, Shared Folders, Shares**, right-click and choose **New File Share**. The wizard asks for the folder path, share name, description and permissions. This tool also shows all shares, current **Sessions** (connected users) and **Open Files**, and allows the administrator to disconnect a user or stop sharing.

Command line

```
net share Data=D:\Data /remark:"Common data folder" /users:50
net share                               (list all shares)
net share Data /delete                   (stop sharing the folder)
```

Administrative and hidden shares

A share name that ends with a dollar sign (\$) is a **hidden share**: it does not appear when users browse the server but can be reached if its exact name is typed. Windows 2000 creates **administrative shares** automatically for management.

Share	Purpose
C\$, D\$...	Root of each drive, for remote administration
ADMIN\$	The Windows system folder (for example C:\WINNT), used for remote administration
IPC\$	Used for inter-process communication and remote management (named pipes)
PRINT\$	Printer drivers for shared printers
NETLOGON, SYSVOL (on DCs)	Logon scripts and group policy files

Naming and planning shares

- Use short, meaningful share names; for compatibility with older clients keep names to 12 characters or fewer without spaces.
- Share at a high level (for example Departments) and control the sub-levels with NTFS permissions.
- Never share the system folders or the root of the system drive to ordinary users.
- Keep user home folders in one share (for example \\SERVER1\Home\$) with a subfolder per user.
- Review shares regularly and remove those that are no longer required.

5.3.3 Mapping Drives

Mapping a drive assigns a drive letter (such as Z:) to a shared folder on a server. After mapping, the shared folder appears in *My Computer* like a local disk, and applications can use it by the drive letter, as in Fig. 5.3.

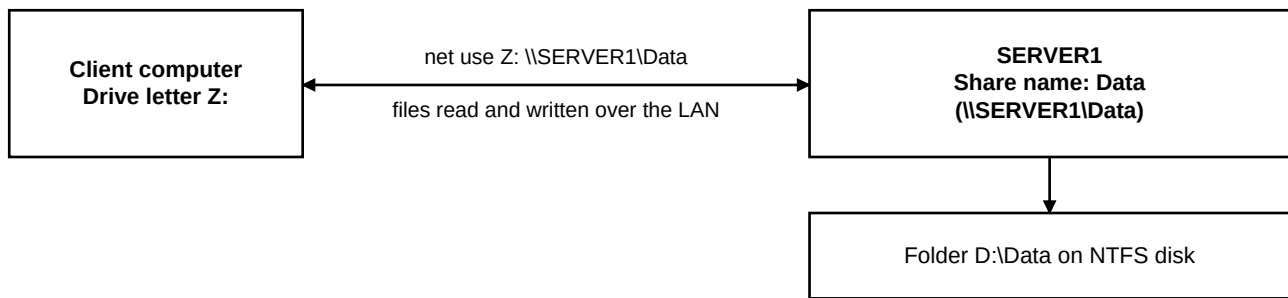


Fig. 5.3: Mapping drive Z: to a shared folder

Steps to map a network drive from the client:

- 1 Open **Windows Explorer** (or right-click *My Network Places*) and choose **Tools, Map Network Drive**.
- 2 Select a free **Drive** letter from the list.
- 3 In **Folder**, type the UNC path such as `\\SERVER1\Data` or use **Browse** to find it.
- 4 Tick **Reconnect at logon** so that the drive appears every time the user logs on.
- 5 If the user has a different account on that server, click *Connect using a different user name* and enter it.
- 6 Click **Finish**. The mapped drive opens and is shown under My Computer.

```

net use Z: \\SERVER1\Data /persistent:yes      (map drive Z:)
net use                                       (list current connections)
net use Z: /delete                          (disconnect drive Z:)
  
```

Administrators often put `net use` commands in a **logon script** (a batch file named on the user's Profile tab) or use group policy, so that all users automatically receive the correct drives. A home folder set on the Profile tab (for example `H:` connected to `\\SERVER1\Home$\%username%`) is mapped in the same way.

Troubleshooting shares

Problem	Likely cause	Remedy
Access is denied	Share or NTFS permission missing, or a Deny entry	Check both sets of permissions and the groups of the user
Network path not found	Wrong server or share name, DNS/name resolution or network fault	Check the UNC path; ping the server by name and by IP address
Share not visible in browse list	Hidden share (\$) or browsing service problem	Type the full UNC path; check the Computer Browser service
Too many users connected	User limit reached	Raise the limit in the Sharing tab
Mapped drive missing after restart	Reconnect at logon not selected	Map again with Reconnect at logon, or use a logon script

5.4 Administering Printer Shares

A network printer allows many users to use one expensive printing device. A Windows 2000 server can act as a **print server**: it receives jobs from clients, stores them, sends them to the printer one by one and lets the administrator control the whole service from one place (Fig. 5.4).

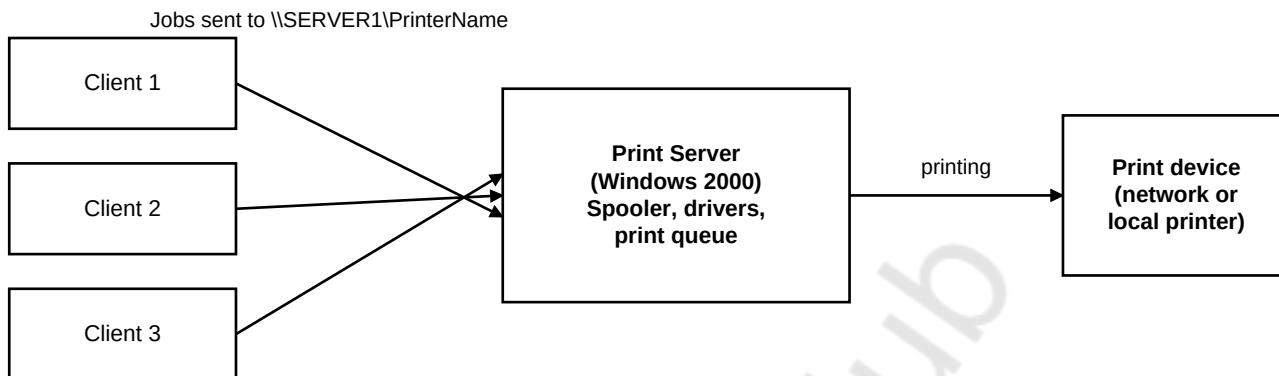


Fig. 5.4: Network printing through a print server

Printing terms in Windows 2000

Term	Meaning
Print device	The physical machine that produces the printed pages
Printer	The logical printer: the software interface on the server between the application and the print device. One printer can use several devices, and several printers can use one device
Print server	The computer where printers are defined and shared
Print driver	Software that converts documents into commands the print device understands
Spooler (spooling)	Service that stores a job on disk first so that the application is free again quickly; the job waits in a print queue
Print queue	List of documents waiting to be printed
Port	Connection used to reach the device: LPT1, USB, or a Standard TCP/IP port for network printers

5.4.1 Setting Up a Network Printer

There are two parts: installing the printer on the print server and sharing it, then connecting the client computers.

Part 1: Add and share the printer on the server

- 1 Connect the print device to the network (or to the server) and switch it on. Note its IP address if it is a network printer.
- 2 Click **Start, Settings, Printers** and double-click **Add Printer**. The Add Printer Wizard starts.
- 3 Choose **Local printer** to create a printer on this server. For a plug-and-play device keep the option to detect it automatically; for a network-attached device clear it.
- 4 Select the port: an existing port (such as LPT1), or **Create a new port, Standard TCP/IP Port** and enter the printer IP address.
- 5 Select the **Manufacturer** and **Model** to choose the driver (or click **Have Disk** for a driver you supply).

- 6 Type the **Printer name** and choose whether it is the default printer.
- 7 Choose **Share as** and type the **Share name**; add the **Location** and **Comment** so users can find it in Active Directory.
- 8 Print a **test page** and click **Finish**.

Part 2: Connect client computers

- On the client open **Start, Settings, Printers, Add Printer**, choose **Network printer**.
- Type the UNC name \\SERVER1\HPLaser, or browse through My Network Places, or search Active Directory, and click **Next**.
- The driver is normally copied automatically from the server (**Point and Print**). Choose whether it is the default printer and click **Finish**.

The Sharing tab also contains the **Additional Drivers** button. Here the administrator can add drivers for other client systems (for example Windows 95/98 or Windows NT 4.0), so that those clients can install the printer without a disk. The option **List in the Directory** publishes the printer in Active Directory so users can search for it by location.

5.4.2 Print Permissions

Permission	What it allows	Given by default to
Print	Send documents to the printer; pause, resume or cancel own documents	Everyone
Manage Documents	Control all users' documents: pause, resume, restart, cancel (not change printer settings)	Creator Owner, Print/Server Operators, Administrators
Manage Printers	Full control of the printer: share it, change properties and permissions, delete it	Administrators, Print Operators, Server Operators

Permissions are set on the **Security** tab of the printer Properties. Restricting *Print* to a department group prevents other users from wasting paper on an expensive colour printer.

5.4.3 Managing Printers and Queues

Double-clicking a printer icon opens its queue window. From the **Printer** and **Document** menus the administrator can control printing.

Task	How
Pause or resume the whole printer	Printer menu, Pause Printing (use again to resume)
Delete all waiting documents	Printer menu, Cancel All Documents
Pause, restart or cancel one document	Right-click the document, choose Pause, Restart or Cancel
Give an urgent document priority	Document properties, General tab, set Priority (1 is lowest, 99 is highest)
Allow printing only at certain times	Printer Properties, Advanced tab, Available from ... to ...
Use several print devices as one printer	Printer Properties, Ports tab, tick Enable printer pooling and select the ports
Use one device with different settings for different groups	Create two printers for the same port with different priorities and permissions

Task	How
Separator page, change spool folder	Advanced tab (Separator Page); Print Server Properties, Advanced tab (spool folder)

Troubleshooting printing

Problem	Likely cause	Remedy
Jobs stay in the queue and nothing prints	Printer offline or paused, or a stuck job	Check the printer, clear the Pause and Offline settings, cancel the stuck job
Cannot delete a stuck job	Spooler is hung	Restart the Print Spooler service: net stop spooler, then net start spooler
Prints garbage characters	Wrong or corrupt driver	Install the correct driver for the printer model
Access denied when connecting	No Print permission for the user	Add the user or group with Print permission
Server disk becomes full	Large queue in the spool folder	Move the spool folder to a bigger disk and clear old jobs

5.5 Working With Windows 2000 Backup

Data can be lost because of disk failure, accidental deletion, virus attack, theft, fire or human error. A **backup** is a copy of data stored on a separate medium so that it can be **restored** after a loss. Backup is the last line of defence of every network, and a backup that has never been tested cannot be trusted. Windows 2000 includes a backup program, **Windows 2000 Backup** (file name *ntbackup.exe*).

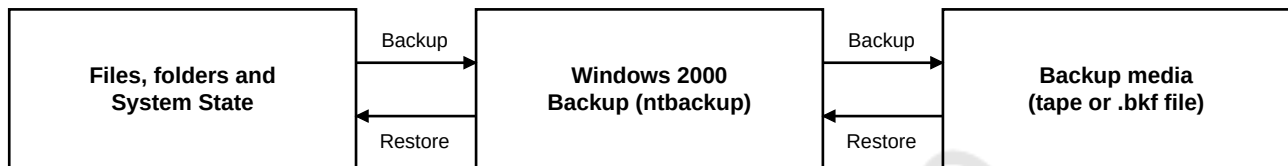


Fig. 5.5: Backup and restore with Windows 2000 Backup

5.5.1 Using Windows 2000 Servers Backup Software

Starting the program

Click **Start, Programs, Accessories, System Tools, Backup** or run *ntbackup* from **Start, Run**. The window has these tabs.

Tab / feature	Purpose
Welcome	Starts the Backup Wizard, Restore Wizard and Emergency Repair Disk creation
Backup	Select drives, folders, files and System State to back up, choose destination and options
Restore	Select the backup set and the files to restore
Schedule Jobs	Run backups automatically at chosen times using the Task Scheduler service

Who may back up and restore?

Members of **Administrators** and **Backup Operators** can back up and restore all files on the computer, whatever the file permissions. Ordinary users can back up and restore only the files they own or have permission to use. Because a backup contains all the data, the backup media must be kept physically secure.

Backup media

- **Tape drive:** traditional, large capacity and low cost per gigabyte; ideal for off-site storage.
- **File:** the backup is saved in a single file with the extension **.bkf** on a hard disk, network share or removable disk. Easy for small servers, but the file must then be copied to a different place.
- Never store the only backup on the same disk or in the same room as the original data.

Types of backup

The type of backup decides which files are copied and whether the **archive attribute** (a marker that shows a file has changed since the last backup) is cleared afterwards.

Type	What is copied	Archive attribute	Use
Normal (full)	All selected files and folders	Cleared	Basis of every backup plan; simplest restore
Copy	All selected files	Not cleared	Extra copy that does not disturb the regular schedule
Incremental	Only files changed since the last normal or incremental backup	Cleared	Fastest backup, smallest size; restore needs normal plus every incremental
Differential	All files changed since the last normal backup	Not cleared	Restore needs only normal plus the last differential; each day larger than the previous
Daily	Files modified on the day the backup is made	Not cleared	Quick end-of-day copy of that day's work

Example weekly schedule

Day	Strategy A: Normal + Incremental	Strategy B: Normal + Differential
Sunday	Normal	Normal
Monday to Saturday	Incremental each day	Differential each day
Restore on Thursday needs	Sunday normal + Mon, Tue, Wed incrementals (all, in order)	Sunday normal + Wednesday differential only
Backup time	Short every night	Grows each night
Restore time	Longer and more media	Shorter and simpler

Many organizations use the **Grandfather-Father-Son** rotation: daily (son) tapes are reused every week, weekly (father) tapes are reused every month and monthly (grandfather) tapes are kept for a year or longer. Some of the tapes are stored off-site.

What is backed up: System State

Besides files, Windows 2000 Backup can save the **System State**, which contains the data needed to rebuild the operating system configuration: the **registry**, the **COM+ class registration database**, the **system boot files**, and on a domain controller the **Active Directory** database and the **SYSVOL** folder (also the Certificate Services database if installed). Back up the System State regularly, because Active Directory cannot be recovered without it.

5.5.2 Steps to Back Up Files

- 1 Start Backup and click the **Backup** tab (or use the Backup Wizard from the Welcome tab).
- 2 In the left pane tick the **drives, folders or files** to back up (and **System State** if required).
- 3 Under **Backup destination** choose File or the tape device, and type the **Backup media or file name** (for example E:\Backup\Data.bkf).
- 4 Click **Start Backup**. In the dialog, give the backup set a **label** and choose **Append** or **Replace** existing data on the media.
- 5 Click **Advanced** to select the **backup type**, tick **Verify data after backup** and, if supported, **Use hardware compression**.

- Click **Start Backup**. A progress window appears; when it finishes, click **Report** to read the backup log and check for skipped files.

Backup options (Tools, Options)

- **Backup Log:** Summary only, Detailed (lists every file) or None. Use Summary or Detailed to find errors.
- **Verify:** compares the backup with the original after writing; it takes time but shows faulty media.
- **Exclude Files:** skips unnecessary files such as temporary files.
- Files that are open and locked by programs may be skipped; close programs (or use the database's own backup tool) before backing up.

Scheduling a backup

Select the **Schedule Jobs** tab, click **Add Job** and follow the Backup Wizard: choose what to back up, the destination, the type, the options, a job name, and the schedule (daily, weekly, at start-up and so on) together with the account under which the job runs. The Task Scheduler service must be running, and the media must be available when the job starts.

```
ntbackup backup "D:\Data" /J "Nightly Data" /M normal /V:yes /F "E:\Backup\Data.bkf"
ntbackup backup systemstate /J "SystemState" /F "E:\Backup\State.bkf"
```

The command line allows backups to be started from batch files and the Task Scheduler. Options differ slightly between versions, so check them with `ntbackup /?`.

5.5.3 Steps to Restore Files

- Start Backup and click the **Restore** tab (or the Restore Wizard).
- Expand the backup **media** (tape or .bkf file) in the left pane. If a file is not listed, use **Tools, Catalog a backup file** to read it.
- Tick the **drives, folders or files** (and System State) to restore.
- Under **Restore files to** choose **Original location**, **Alternate location** or **Single folder**. Restoring to an alternate location is safer when only checking the data.
- Click **Start Restore**, then choose how to treat existing files: **Do not replace**, **Replace if the existing file is older** or **Always replace**.
- Wait for completion and read the report. If incremental backups are used, restore the normal backup first and then each incremental set in order (a differential needs only the last set).

System State on a domain controller is restored in a special way: the server is started in **Directory Services Restore Mode** (press F8 at start-up), and an *authoritative restore* is used when deleted Active Directory objects must be brought back to all domain controllers.

5.5.4 Backup Planning and Good Practice

- Write a **backup policy**: what is backed up, how often, who does it, where media are kept and how long.
- Automate with Schedule Jobs so that backups do not depend on memory.
- Keep copies **off-site** (or in a fireproof safe) and label media clearly.
- **Test restores** regularly; a backup that cannot be restored is useless.
- Review the backup log every day and fix errors immediately.
- Back up System State and create an **Emergency Repair Disk** after major changes.
- Protect backup media from unauthorized access and replace old tapes before they wear out.

- Remember: RAID and shadow copies protect against disk faults and mistakes but are **not a replacement** for backup.

Troubleshooting backup

Problem	Likely cause	Remedy
Backup cannot find the tape drive	Driver or device problem	Check connection and driver; Removable Storage service must be running
Files skipped in the log	Files were open or in use	Close applications or schedule backup at night
Backup job does not run	Task Scheduler stopped, wrong password or media missing	Start the service, update the job account and load media
Out of space on destination	Backup bigger than disk or tape	Use incremental backups, compression or a larger medium
Cannot restore on a new computer	Different hardware or no catalog	Catalog the backup file first; use identical or compatible configuration

Chapter Summary (Quick Revision)

- **User accounts** identify users. Create them in Active Directory Users and Computers (domain) or Computer Management (local). Each account has a unique SID. Use *User must change password at next logon* for new accounts.
- **Modify** accounts through Properties tabs (Account, Profile, Member Of). **Disable** keeps the account and its SID; **delete** removes it permanently and the SID cannot be recovered.
- **Groups** simplify administration. Types: security and distribution. Scopes: domain local, global, universal. Strategy: A-G-DL-P. Maintain membership from the group Members tab or the user Member Of tab.
- **Shares** make folders available as \\server\share. **Share permissions** (Read, Change, Full Control) apply only over the network; **NTFS permissions** apply everywhere; the effective permission is the more restrictive, and Deny overrides Allow.
- **Mapping a drive** gives a share a drive letter (Tools, Map Network Drive or *net use*). Hidden shares end with \$.
- **Printer shares**: print device vs logical printer, spooler and queue. Add Printer Wizard, share, add additional drivers; permissions Print, Manage Documents, Manage Printers.
- **Backup** with ntbackup: Normal, Copy, Incremental, Differential and Daily types; System State; schedule jobs; test restores; keep copies off-site.

Multiple Choice Questions

Choose the correct option for each question. The answer key is given after the questions.

Q1. Which tool is used to manage domain user accounts on a Windows 2000 domain controller?

- (a) Active Directory Users and Computers
- (b) Device Manager
- (c) Disk Defragmenter
- (d) Event Viewer

Q2. The maximum length of the pre-Windows 2000 logon name of a user account is:

- (a) 8 characters
- (b) 15 characters
- (c) 20 characters
- (d) 64 characters

Q3. Which option forces a new user to choose a private password at first logon?

- (a) Password never expires
- (b) User must change password at next logon
- (c) User cannot change password
- (d) Account is disabled

Q4. The best way to stop a user from logging on temporarily while keeping the account is to:

- (a) Delete the account
- (b) Rename the account
- (c) Disable the account
- (d) Remove the password

Q5. A new account with the same name as a deleted account does not get the old permissions because:

- (a) Passwords are stored in the registry
- (b) Names are case sensitive
- (c) The group scope is different
- (d) Every account has a unique SID

Q6. Which type of group can be used to assign permissions to resources?

- (a) Security group
- (b) Distribution group
- (c) Print group
- (d) Local profile

Q7. Universal security groups can be used only when the domain is in:

- (a) Mixed mode
- (b) Native mode
- (c) Both modes equally
- (d) Workgroup mode

Q8. Which share permission lets a user add, modify and delete files but not change permissions?

- (a) Read
- (b) Full Control
- (c) Change
- (d) No Access

- Q9.** When share permissions and NTFS permissions both apply to a network user, the effective permission is:
- (a) The share permission only
 - (b) The NTFS permission only
 - (c) The more permissive of the two
 - (d) The more restrictive of the two
- Q10.** Which of the following is an administrative (hidden) share?
- (a) Public
 - (b) C\$
 - (c) Data
 - (d) Temp
- Q11.** Which command maps drive Z: to the share \\SERVER1\Data?
- (a) net use Z: \\SERVER1\Data
 - (b) net share Z: \\SERVER1\Data
 - (c) net map Z: SERVER1
 - (d) net drive Z: Data
- Q12.** In Windows 2000 printing terminology, the physical machine that produces the output is called the:
- (a) Printer
 - (b) Print server
 - (c) Print device
 - (d) Spooler
- Q13.** Which print permission lets a user pause, restart or cancel documents of other users?
- (a) Print
 - (b) Manage Documents
 - (c) Manage Printers
 - (d) Read
- Q14.** Which backup type copies all selected files and clears the archive attribute?
- (a) Copy
 - (b) Differential
 - (c) Incremental
 - (d) Normal
- Q15.** Windows 2000 Backup saves a backup to a disk in a file with the extension:
- (a) .bkf
 - (b) .bak
 - (c) .zip
 - (d) .tmp

Answer Key for MCQs

Q. No.	Answer	Explanation
1	(a)	Domain accounts and groups are managed in Active Directory Users and Computers.
2	(c)	The pre-Windows 2000 (SAM) account name can be up to 20 characters.
3	(b)	This option makes the user change the administrator-supplied password.
4	(c)	A disabled account keeps its SID, permissions and groups and can be enabled again.
5	(d)	Permissions are linked to the SID, and a new account receives a new SID.
6	(a)	Distribution groups are only for e-mail; security groups hold permissions.
7	(b)	Native mode (all DCs run Windows 2000) is required for universal security groups.
8	(c)	Change allows modification; Full Control adds changing permissions.
9	(d)	The most restrictive combination applies.
10	(b)	A name ending with \$ is hidden; C\$ is the automatic administrative share for drive C.
11	(a)	net use connects (maps) a drive letter to a shared resource.
12	(c)	The printer is the logical software interface; the print device is the hardware.
13	(b)	Manage Documents controls all documents in the queue without changing printer settings.
14	(d)	Normal (full) backup copies everything and marks files as backed up.
15	(a)	ntbackup file backups use the .bkf extension.

Quick key: 1-a, 2-c, 3-b, 4-c, 5-d, 6-a, 7-b, 8-c, 9-d, 10-b, 11-a, 12-c, 13-b, 14-d, 15-a

Broad Questions

Answer the following questions in detail.

1. Explain the procedure to add a user account in Windows 2000 Server. Describe the password options and the settings available on the Account tab.
2. How is a user account modified in Windows 2000? Differentiate between disabling and deleting a user account and explain why the SID matters.
3. What are security groups? Explain the types and scopes of groups in Windows 2000 and describe the built-in groups.
4. Describe the steps to create a group and to maintain its membership. Explain the A-G-DL-P strategy with an example.
5. Explain share security in Windows 2000. Distinguish between share permissions and NTFS permissions and explain how they combine, with examples.
6. Describe the procedure to create a share and to map a network drive on a client, using both the graphical tools and the command line.
7. Explain the printing terms print device, printer, spooler and print server. Describe the steps to set up and share a network printer and connect clients to it.
8. Describe the print permissions in Windows 2000 and explain how a print queue is managed and how common printing problems are solved.
9. Explain the types of backup supported by Windows 2000 Backup. Compare a normal plus incremental strategy with a normal plus differential strategy, and describe how to restore data.
10. Write short notes on any three: (a) hidden and administrative shares, (b) System State, (c) printer pooling and priorities, (d) scheduling a backup job, (e) local and domain user accounts.