

NEW EDITION



OPERATING SYSTEM

D.I.T Part-1
(NEW COURSE)

perfect24u.ocm

M. Khalid Khan

M.Sc. Computer Science
(Gold Medalist)

Cell: 0333-9112578

Email: mkk9020@yahoo.com

Recommended by:

TTB/BTE, Khyber Pakhtunkhwa

For order contact

Shah Faisal Khan

0300-5712412

0937-872412

- Configure wireless network connectivity on a windows 7 client computer. (Bluetooth, Wi Fi) 31
- Secure Windows 7 client desktop computers. 43
- Optimize and maintain the performance and reliability of a windows 7 client. computer 45
- Remote access setting for a windows 7 client computer. 46

Windows Server

- Installing Windows Server 2008 48

Introduction to Administrative Tasks in Windows Server 2008 Environment

- Managing Server Roles and Features. 55
- Overview of Action Directory. 56
- Using Windows Server 2008 Administrative Tools. 56

Creating Action Directory Domain Services User Computer Objects

- Managing User Accounts. 57
- Creating Computer Accounts. 67

Creating Groups and Organizational Units

- Introduction to Groups . 68
- Managing Groups . 68
- Creating Organizational Units. 69

Creating and Configuring Groups Policy

- Overview of Groups Policy. 69
- Configuring the Scope of Groups policy Objects. 72
- Managing Groups policy Objects. 73
- Delegating Administrative Control of Group Policy. 75
- Configuring Group policy setting. 76
- Configuring Security Policies. 77
- Configuring an Audit Policy. 78

DNS	79
• Installing and Configuring the DNS Server Role.	79
• Managing and Troubleshooting DNS.	85
Managing Windows Server 2008 Backup and Restore	
• Backups with windows Server 2008.	92
• Planning Backups Policy on Windows Server 2008.	92
• Planning a Server Restore Policy.	95
Linux	98
Installing Linux (Red Hat).	107
File System Management.	111
Creating user accounts	112
Installing application software's in Linux.	115
Configuring device drivers	116
Executing basic commands in Terminal .	117
<u>Reference Books / Helping Material</u>	
1. DIT-I by Mohammad Khalid.	
2. Operating System concept by William stalling.	
3. Operating System by Andrew S.Tanenbaum.	

ACKNOWLEDGMENTS

The author wishes to acknowledge the assistance of the following reviewers whose constructive criticism and suggestions helped invaluable in shaping the form and content of this text.

Mr. Hazrat Zubair, Associate Professor in Comp. Sc., GCMS-2, Ring Road, Peshawar.

Mr Riaz Assistant Professor GCMS-1 Mardan.

Mr Fzali Akbar Lecturer Computer Science GCMS-1 Mardan

Mr Rahat Ullah Lecturer Computer Science GCMS-2 Mardan

Mr Tufail Lecturer Computer Science GCMS-2 Mardan

Mr Muhammad Waseem Lecturer Computer Science GCMS, Hari Pure

Mr Miskeen Shah A/P Computer Science GCMS Hari Pure Mardan

Mr. Rahim Shah, Lecturer in Computer Science GCMS, Peshawar

Mr. Younas Lecturer in Computer Science, GCMS, Thana

Mr. Riaz Assistant Professor in Computer Science, GCC, Swat

Mr. Naeem Ullah Lecturer in Computer Science, GCC, Swat

Mr. Yaseen Assist Professor in Computer Science, GCC Kohat

Mr. Mujeeb ur rehman Lecturer in Computer Science, GCMS, Peshawar

Mr. Fazli Wahab Lecturer in Computer Science, GCMS, Swabi

Mr. Nasar Jamal Lecturer in Computer Science, GCMS, Nowshera -2

My Special thanks are to my honourable friend and all staff member of Government College of Management Sciences, Peshawar for their valuable suggestions.

Thanks to all my colleagues especially Mr. Tariq Siddique, Ali Yar and Naveed Iqbal for participating in various technical discussions which has led to the significant improvement in the book.

M Khalid Khan

Part-1/ First Semester

Diploma in information Technology

OPERATIONG SYSTEM.**(PAPER-I)****Total Th Hrs 40****Total Th Mks 50****Total Pr Hrs 80****Total Pr. Mks 100****OBJECTIVES**

- Understanding Desktop Operating System and Server Operating System.
- Understanding the role of Operating System in computing environment.
- Hands on practice on Windows 7, Windows 2008 Server and Linux.
- Networking Features in Operating System.

COURSE CONTENTS**General**

What is an Operating System and its role in the Computing environment, Desktop Vs Server base Operating System, Major parts/function of Operating System. Classification of Operating System. Function of Operating System

1-7

Scheduling, Deadlock

8-11

Windows 7

13

- Installing Windows 7
- Configure disks, Partitions, volumes, and device Driver
- Configure file access and printers on a Windows 7 client computer.
- Configure network connectivity on a windows 7 client computer.

13

17

24

29

Q) WHAT IS OPERATING SYSTEM?

Ans: Operating System is a group of program that controls all the operation of computer system and its components. An operating system is an integrated set of specialized programs that is used to manage the resources and overall operation of a computer. A computer can do nothing without operating system. Operating System must be installed on every computer. User interacts with computer through Operating System. When computer is turned on, the operating system runs and checks that all parts of the computer are functioning properly. Operating system manages all operation on computer after loading.

Some popular operating system is IBM PC-DOS, MS-DOS, UNIX, XENIX, LINUX, WINDOWS-98, WINDOWS-2000, OS/2, and WINDOWS-XP. perfect24u.ocm

CLASSIFICATION/TYPES OF OPERATING SYSTEM.

Operating system is classified according to the following criteria's.

i-Single User Operating System .ii- Multi User Operating System. iii Time Shared System

i. SINGLE USER OPERATING SYSTEM.

Single User Operating system allows only one user to use the system. For Micro-computer single user operating system offer the following function.

1- Initialization of System in which the OS must have initial loader program to initialize the system properly

2- File Management An operating system contains file management programs that control the creation, deletion, and access of files of data and program

3-Memory management. In type of operating system, this memory management is simple, as only one application is executed at one time. If there is another application to be run the previous is remove from the memory.

4- Input Output management: I/O management in this type of O.S is more simpler as compare to other because one I/O device is made active at a time.

ii. MULTI USER OPERATING SYSTEM .

Multi User Operating system allow more then one user at a time to use the system.

The function provide by OS are:-

1- Initialization.

Initialization is more complex than single user operating system because it is possible that more than one computer be initialized by server.

2- File Management.

File Management is more complex in this case because a file maybe access or shared by more than one user. If a user is using currently a file and another user also trying to access this file than it is duty of operating system to lock the file for other user and also set Security (permissions) on file also share a file to available it on Network

3- Memory management

available memory of server is divided among different user the rest of memory management is the same as the single OS. It also uses a technique called paging to allow your computer to run more programs than its physical memory by storing memory pages not currently in use on a mass storage device called virtual memory

4- Input Output Management.

It is also complex because more than one devices manage by OS

5-Resource Management

Resources (Printer, CD Drive, Floppy Drive etc are available to all user on network)these Device can be share to access from other computer.

6- Process Management. In multi-user operating system more then one application are executed at a time this capability is called multitasking.

7- Processor Management. In multi-user operating system more than one user connected to the system. Hence the processing speed must be fast to manage all user requests. For this reason a system must have more than one processor. multi-user system has capability to manage all these processors.

8- Communication Management

In multi-user operating system one computer is connected with more than one systems. Hence it has capability to create new user, groups and assign Passwords, and permissions .

iii TIME SHARED SYSTEM:-

It usually consists of a "dumb" type terminal connected by data lines to a centralized Micro-Computer based system that controls all operations.

Q) DISCUSS MAJOR PARTS/FUNCTION/ROLE OF OPERATING

SYSTEM FUNCTIONS/ROLE

An OS performs the following basic functions in the operation of computer system:

BOOTING

Booting is a process of starting the computer. Operating system the computer to work. It checks the computer and makes it ready to work. There are two type of booting

- **Cold Boot:** When computer is turned on by on/off button it is called cold boot.
- **Warm Boot:** When computer is restarted, it is called warm boot.

The User Interface. User interface is used to interact with computer. User interface controls how you enter data and instructions and how information is displayed on the screen. Three main types of user interfaces

- **Command-driven:-** In command-line user interface the user enter data and instructions by typing keyword or pressing special keys on keyboard.
- **Menu-Driven interface:** In menu-driven interface, the user enter data and instruction by using menu. It is easier to use.
- **Graphical User Interface:** graphical user interface is a visual environment that is used by the user to communicate with computer. It uses windows, icon,, menu and other graphical objects to issue commands.

The trend towards an easy-to-use graphical user interface (GUI), which uses icon, bars, button, boxes and images. GUI applies by the pointing devices like the electronic mouse etc.

Resource Management. An operating system uses a variety of resource management programs to manage the hardware and networking resources of a computer system, including its CPU, memory, secondary storage devices, telecommunications processors and input/output peripherals. For example, management programs keep track of where data and programs are stored.

Memory Management: Memory management is a process of optimizing the use of main memory. RAM is used to store data and instructions temporarily during execution. Operating system allocates memory area to different programs. The allocated memory area is de-allocated when the program finishes.

File Management. An operating system contains file management programs that control the creation, deletion, and access of files of data and program. File management also keeping track of the physical location of files on magnetic disks and other secondary storage devices.

Task management/Job scheduling. The task management programs of an operating system manage the completion of the job of end users. They give each task a slice of a CPU's time and interrupt the CPU operations to substitute other tasks. Task management may involve a multitasking capability where several computing tasks can occur at the same time.

New microcomputer operating system and most minicomputer and mainframe operating systems provide a multitasking capability. With multitasking, end user can do two or more operation (e. keyboard and printing) or use of application (e.g Ms-Word, Excel) concurrently, that is at the same time.

A single CPU can run a number of programs at the same time. The numbers of program that can be run concurrently depend on the amount of memory that is available and the amount of processing each job demands. That is because a microprocessor (or CPU) can become overloaded with too many jobs and provide unacceptably slow response. Multitasking allow end user to easily switch from one application to another.

Monitoring Performance

Operating system also monitors the performance of the computer. A performance monitor is a program that checks and reports information about different systems resources and devices. For example it monitors the processor, disk, memory, and network.

Accessing the Web

Operating system provides the facility to connect to the Web. It guides the user to set up a connection between computer and Internet Service Providers. Some operating system provides the facilities of Web browser and email program.

Administering Security

Operating system manages the security of computer system as well as data and program stored on it . Security is normally maintained by using UserID and passwords.

Device Controlling

Operating system controls all devices attached to the computer. The hardware devices are controlled with the help of small software called device drivers.

DISCUSS DESKTOP VERSUS SERVER BASE OPERATING SYSTEM OR POPULAR OPERATING SYSTEM

Ans:- Earlier, many operating system were device-dependent. A type of software that runs only on a specific type computer is called device-dependent.

There are generally two categories of operating systems.

1- Desktop/Stand-alone operating systems

An operating system that works on desktop or notebook computer is called stand-alone operating system. Some example of stand alone operating system are DOS, Windows 95, Windows NT Workstation, Windows Me and Windows XP Home Edition, Windows XP Professional Edition, Windows 2010, Mac OS, OS/2 etc.

Some popular stand alone/desktop operating system are following.

i) DOS

DOS stand for Disk operating System. It was develop by Microsoft in early 1980s for personal computers. It is a single-user, single-tasking operating system.

ii) Windows 95, 98, Me

In 1995 Microsoft introduce Windows 95 operating system, includes the feature of Graphical User Interface. Windows 95 are multitasking, networking, multimedia, and many other capabilities operating system. Microsoft introduced an enhanced Windows 98 version during 1998, Windows Me (millennium Edition) in 2000

iii) Windows XP

Windows XP is a product of Microsoft Corporation. It was released in 2001. XP stand for experience. It is fastest and most reliable operating system. Three versions of Windows XP are Windows XP Home Edition, Windows XP Professional and Windows XP Server.

iv) MAC

Macintosh operating system is a product of Apple. It was one of the first successful GUI. It was release with Macintosh computer in 1984. The latest version of this operating system is called Mac OS X.

2- SERVER BASE/NETWORK OPERATING SYSTEM.

An operating System that supports network is called network operating system. It normally works on a server. Some example of network operating system are Windows NT Server, Windows 2000 Server, Netware, Unix, Linux and Solaris. Some popular Server base/Network operating system are following.

i) NETWARE

Novell's Netware is network operating systems. It is designed for client/server networks.

ii) WINDOWS NT SERVER

Microsoft introduced its Windows NT (New Technology) operating system in 1995. It is designed for client/server networks. The server in the network uses Windows NT Server. The client computer use Windows NT Workstation.

ii) UNIX

UNIX is multitasking, network operating system. It was developed in early 1970s at bell laboratories. Many version of

this operating system are available. It uses command driven interface.

iv) LINUX

Linux is free, multitasking and network operating system. It was developed in 1991. Some version of Linux use command-line interface and other GUI.

v) SOLARIS

Solaris is version of UNIX operating system. It was developed by Sun Microsystems. It is network operating system designed for e-commerce applications.

DISCUSS THE FOLLOWING.

1-SCHEDULING 2- DEADLOCK 3-DEADLOCK HANDLING

SCHEDULING.

The Allocation of CPU (Resources) to different jobs to be process on the computer is called scheduling and the module of operating system which handle this task is called scheduler. The Scheduler arrange jobs in the sequences base in the priority. In the time sharing system all the resources of computer system are share among the different user, as CPU is one of the primary computer resource so the sharing of CPU time among different user (Jobs) is term as scheduling.

The Scheduler has to make decision that which process should be given CPU time when and how much.

1-Scheduler Algorithm.

The following are well know scheduler algorithm .

a) Non-Preemptive Algorithm.

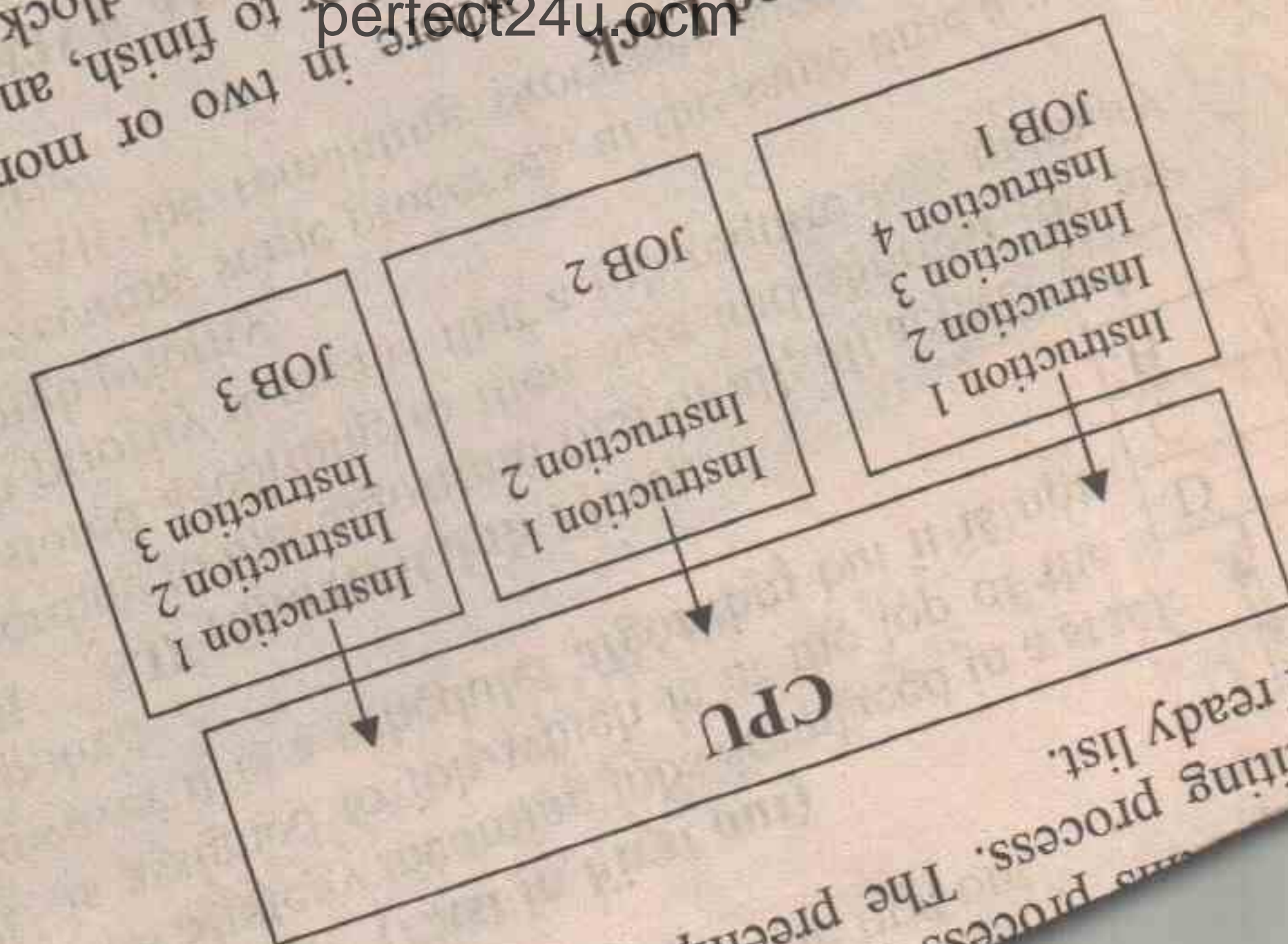
- i. FIFO ii. LIFO. iii. SJF

b) Preemptive Algorithm.

- i. SJN ii. RR

Deadlock is a common problem in multiprocessing systems, where software and hardware locks are used to handle process synchronization.

Deadlock is a situation where two or more competing actions are each waiting for the other to finish, and thus neither ever does. In an operating system, a waiting state because a resource, which is requested by it is waiting for another resource. If a process is requested by it are being state held by another resource. If a process, then the system is said to be in a deadlock.



next waiting process. The preempted process is placed at the back of ready list.

PRE-EMPTIVE ALGORITHM.

PRE-EMPTIVE ALGORITHM.

Khalid Series

Operating System DIT Part-I

Page # 10

b.ii

RR (Round Robbins algorithm)

In this scheduling method the process are dispatched FIFO and no priority is assigned to any job, all the active job are given a limited amount of CPU time called a time slice or quantum's. If a process doesn't complete before its time slice expires, then this process is moved to the end of the ready queue.

RR (Round Robbins algorithm)
scheduling method the proce
riority is assigned to any
amount of CPU
process doesn't

Necessary conditions

A deadlock situation can arise only if all of the following conditions hold simultaneously in a system:

- 1. Mutual Exclusion:** At least one resource must be non-shareable. Only one process can use the resource at any given instant of time.
- 2. Hold and Wait or Resource Holding:** A process is currently holding at least one resource and requesting additional resources which are being held by other processes.
- 3. No Preemption:** The operating system must not de-allocate resources once they have been allocated; they must be released by the holding process voluntarily.
- 4. Circular Wait:** A process is waiting for a resource which is being held by another process, which in turn is waiting for the first process to release the resource. In general, there is a set of waiting processes, $P = \{P_1, P_2, \dots, P_N\}$, such that P_1 is waiting for a resource held by P_2 , P_2 is waiting for a resource held by P_3 and so on till P_N is waiting for a resource held by P_1 .

3-DEADLOCK HANDLING

Most current operating systems cannot prevent a deadlock from occurring. When a deadlock occurs, different operating systems respond to them in different non-standard manners. Major approaches are as follows.

1. Ignoring deadlock

In this approach, it is assumed that a deadlock will never occur. This is also called the Ostrich algorithm. This approach was initially used by MINIX and UNIX. This is used when the time intervals between occurrences of deadlocks is large and the data loss incurred each time is tolerable. It is avoided in very critical systems.

2. Detection

Under deadlock detection, deadlocks are allowed to occur. Then the state of the system is examined to detect that a deadlock has occurred and subsequently it is corrected. An algorithm is employed that tracks resource allocation and process states, it rolls back and restarts one or more of the processes in order to remove the detected deadlock. Detecting a deadlock that has already occurred is easily possible since the resources that each process has locked and/or currently requested are known to the resource scheduler of the operating system

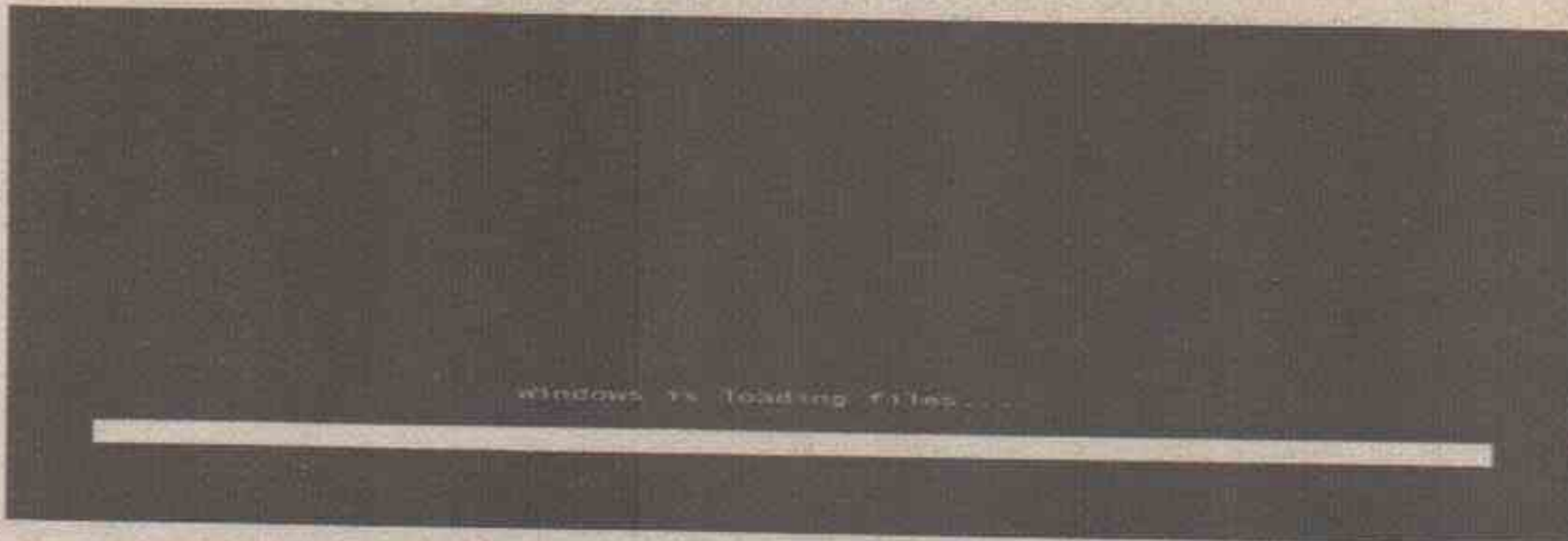
3. Avoidance

Deadlock can be avoided if certain information about processes are available to the operating system before allocation of resources, such as which resources a process will consume in its lifetime. For every resource request, the system sees if granting the request will mean that the system will enter an unsafe state, meaning a state that could result in deadlock. The system then only grants requests that will lead to safe states. In order for the system to be able to determine whether the next state will be safe or unsafe, it must know in advance at any time :

- resources currently available
- resources currently allocated to each process
- resources that will be required and released by these processes in the future

INSTALLING WINDOWS 7

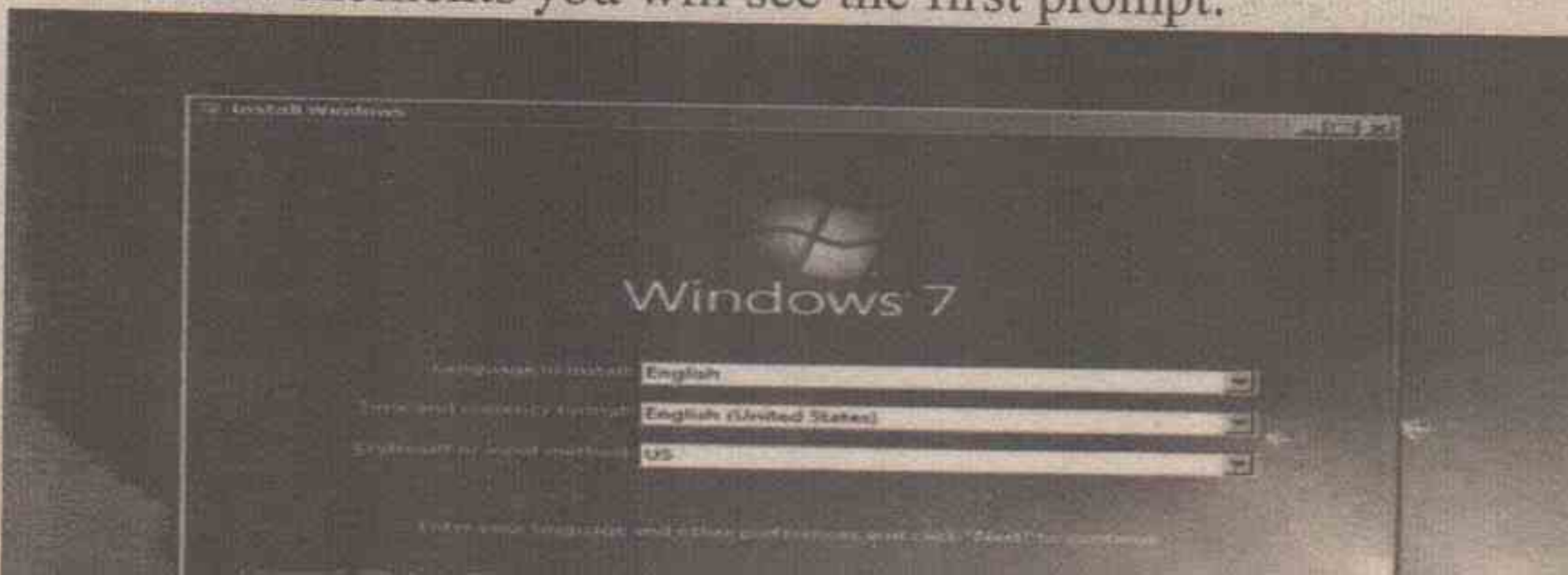
When installing on a physical computer insert your Windows 7 DVD media into your DVD drive and reboot your computer. If you're asked to press a key to boot from DVD or CD, press any key. A black window will appear momentarily while the DVD content is read.



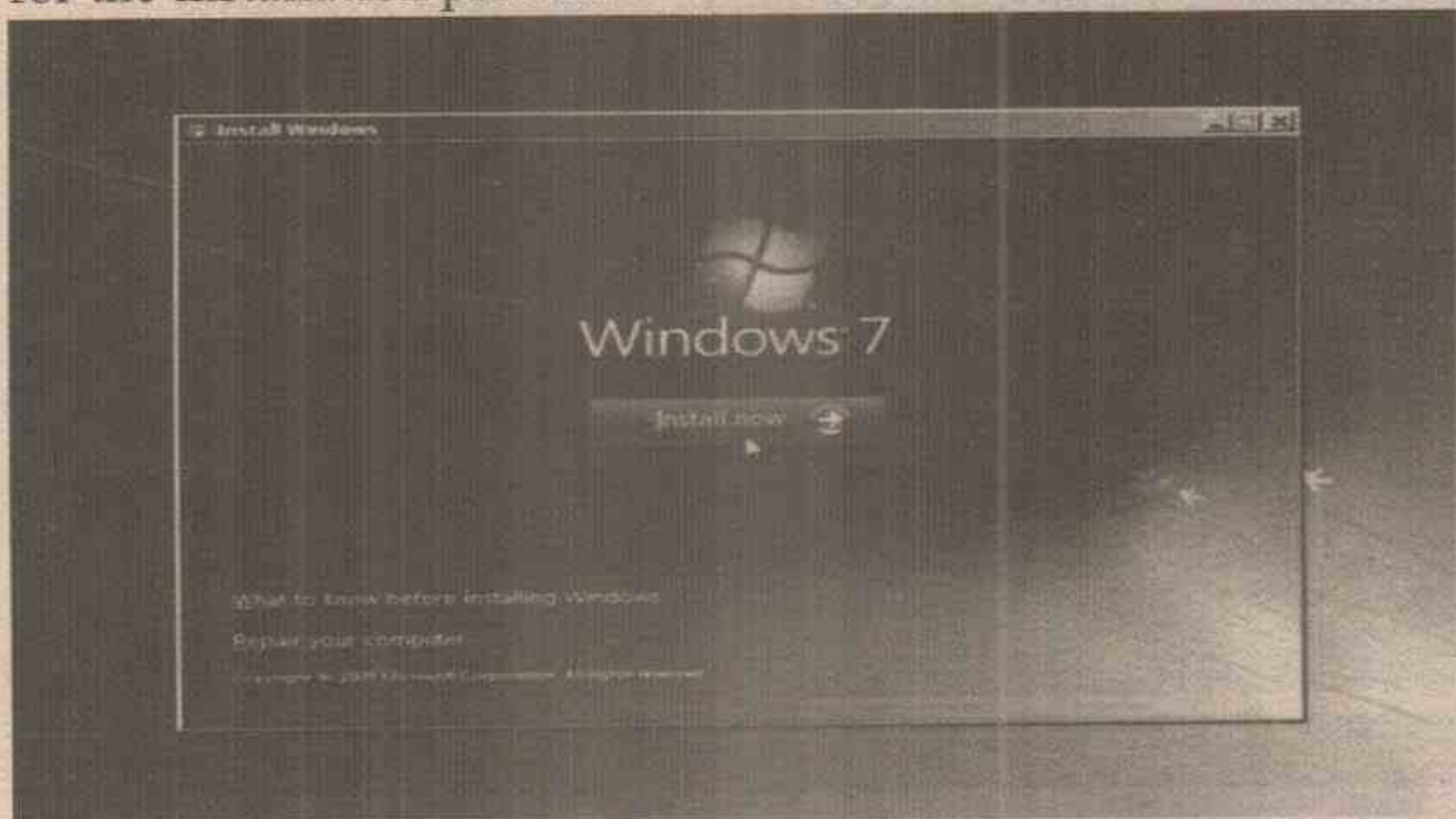
perfect24u.ocm

Next, a Starting Windows screen will appear. Like in Windows Vista and Windows Server 2008, and unlike previous versions of Windows, Windows 7 does not have a noticeable text phase of the setup process, and it will boot directly into the Graphical User Interface (GUI) mode.

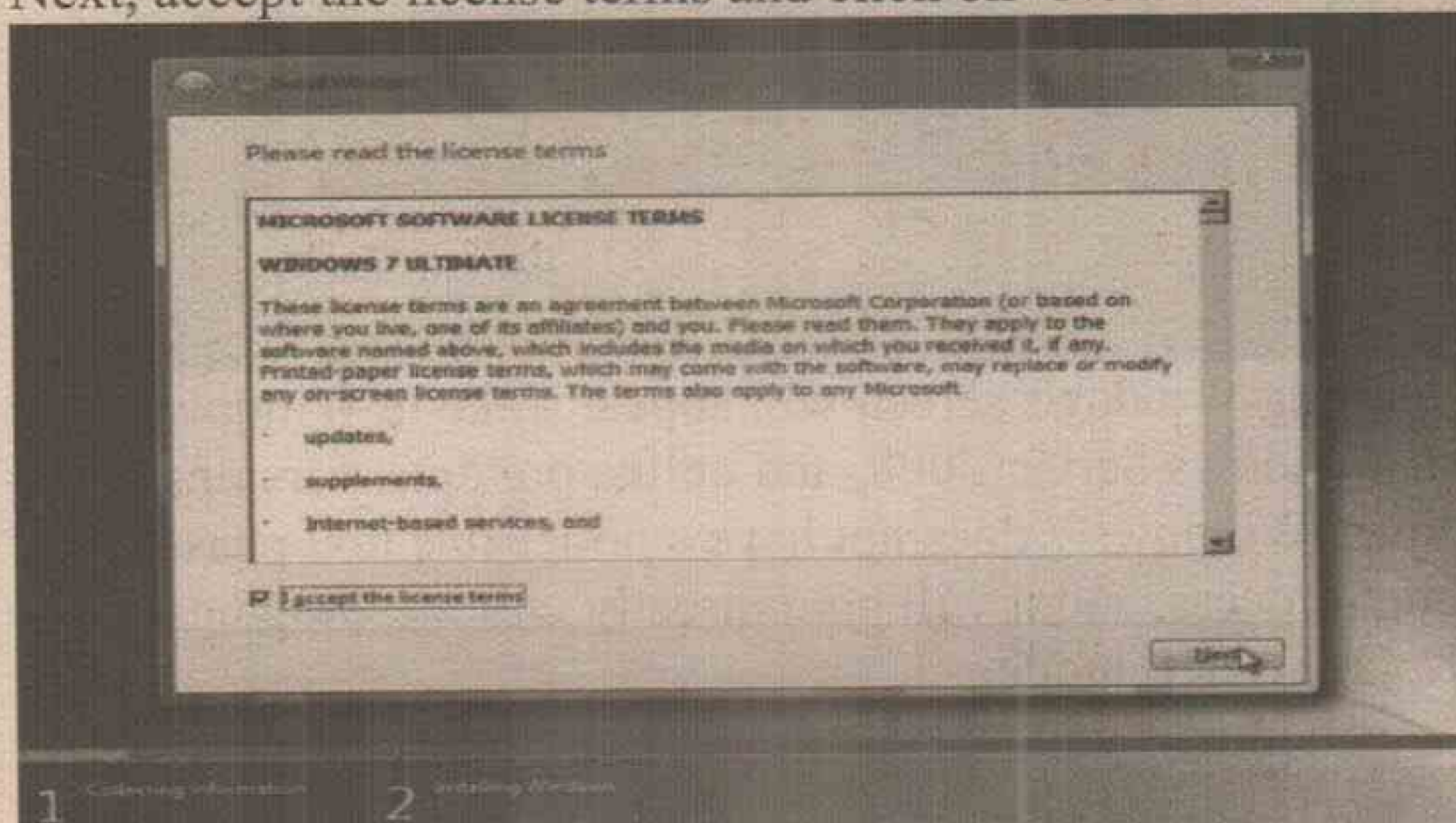
After a few moments you will see the first prompt:



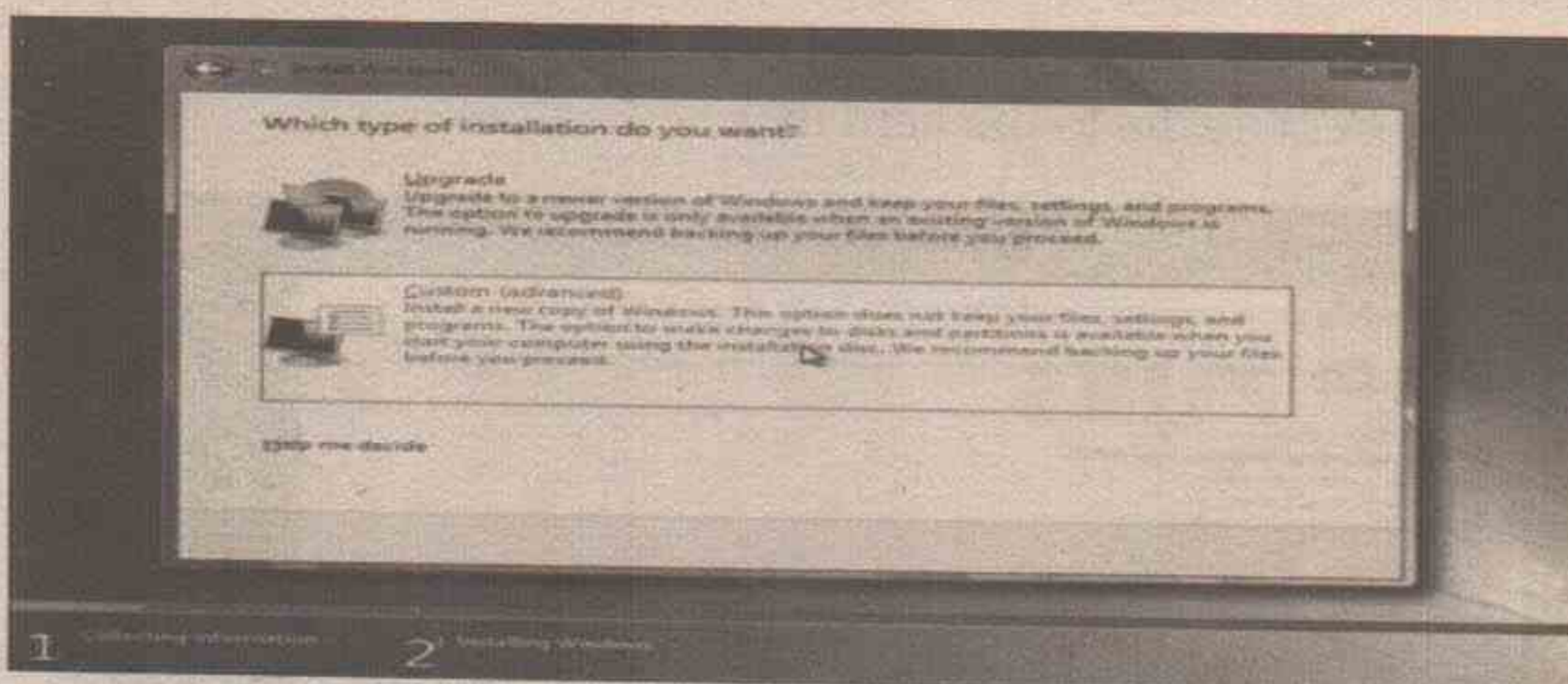
Click "Next" unless you want to change some regional settings for the installation process



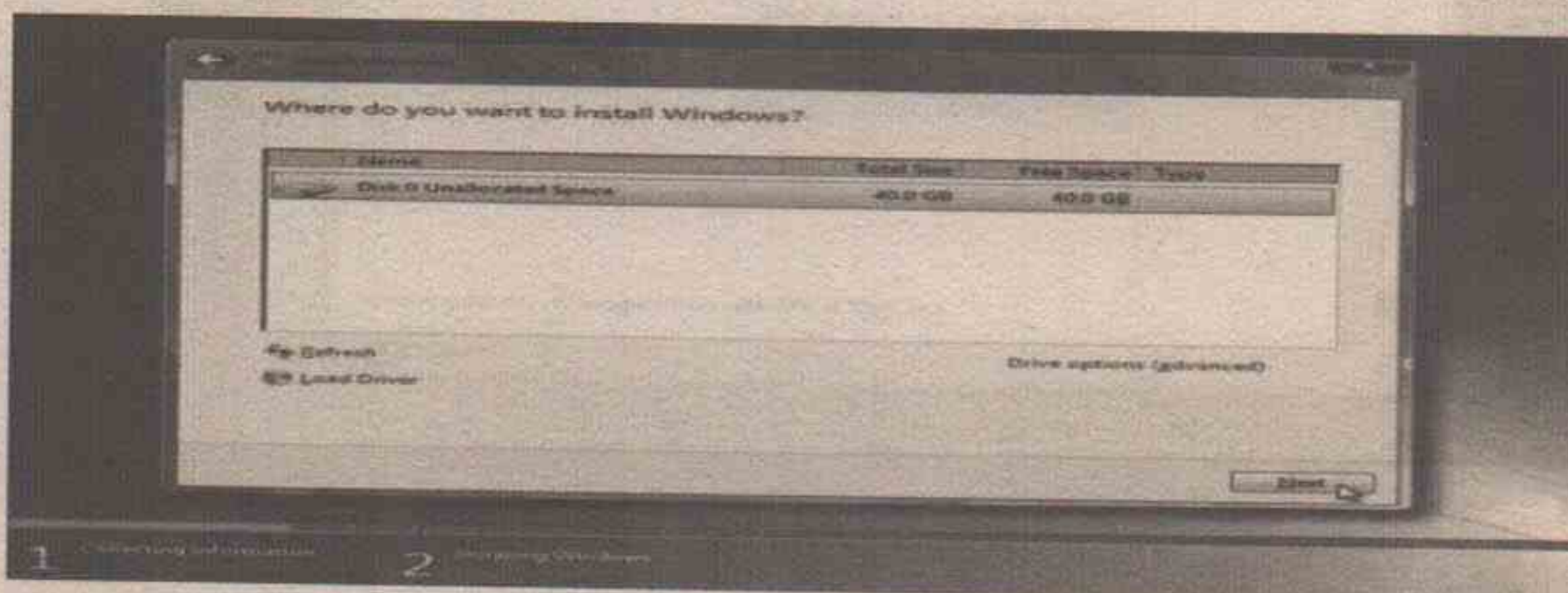
Click on the "Install now" button.
Next, accept the license terms and click on "Next".



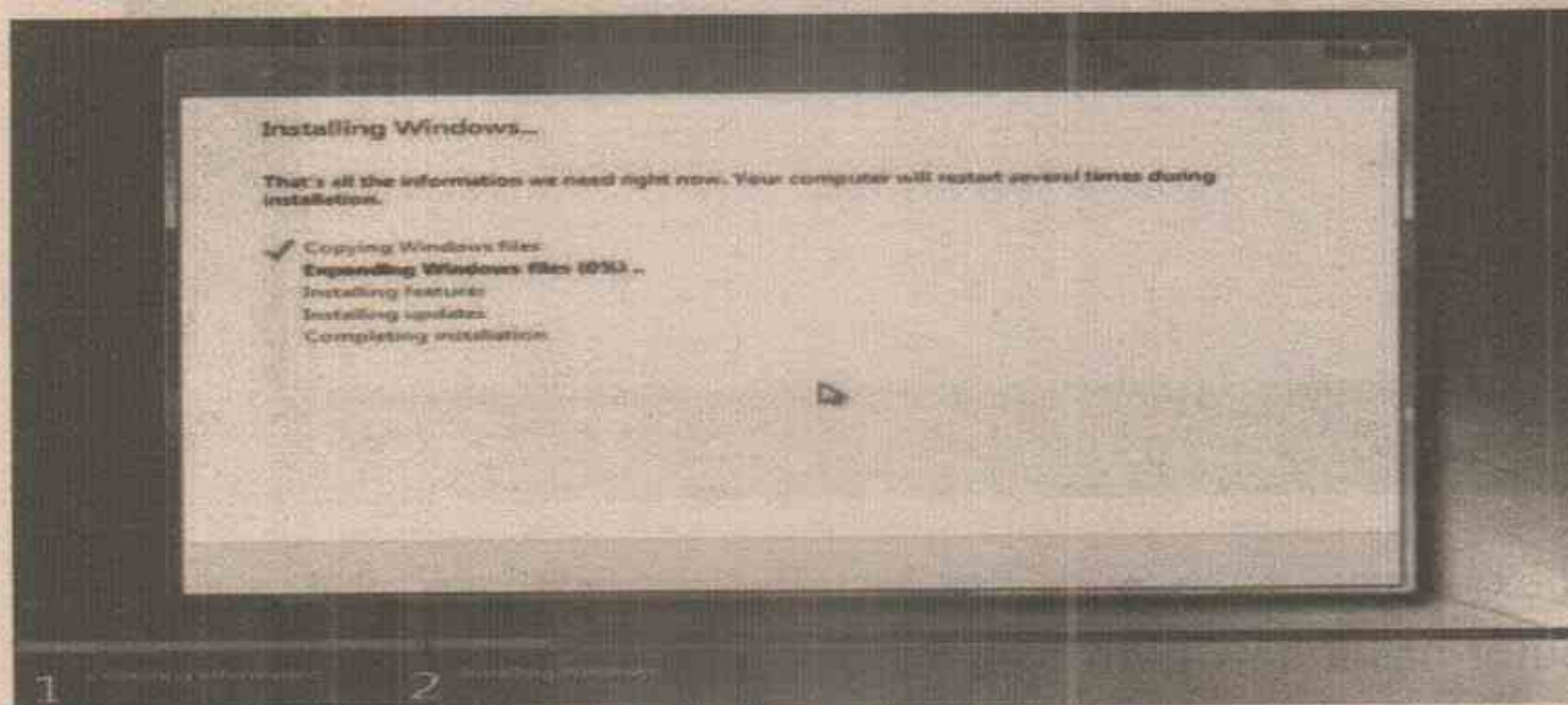
Next, unless you're upgrading an existing Windows installation, press the Custom (Advanced) installation type button. Note that in this case, the Upgrade button is disabled because this specific installation is performed on a new computer without any previous operating system on it.



The next phase is to pick the installation partition. Since this computer has a new hard disk that hasn't been formatted before, you will only have the option to create a new partition on it. If you don't want to specify a specific partition to install Windows on, or create partitions on your hard disk, click Next to begin the installation. If you select another existing partition with enough free space and want to install the Windows 7 on that partition to create a multiboot configuration, select the partition you want to use, and then click Next to begin the installation. If you want to create, extend, delete, or format a partition, click Drive options (advanced), click the option you want, and then follow the instructions. Since I don't need to perform any additional task I will just click on the "Next" button. The installation process will then create a partition on all the available disk space, and format it.

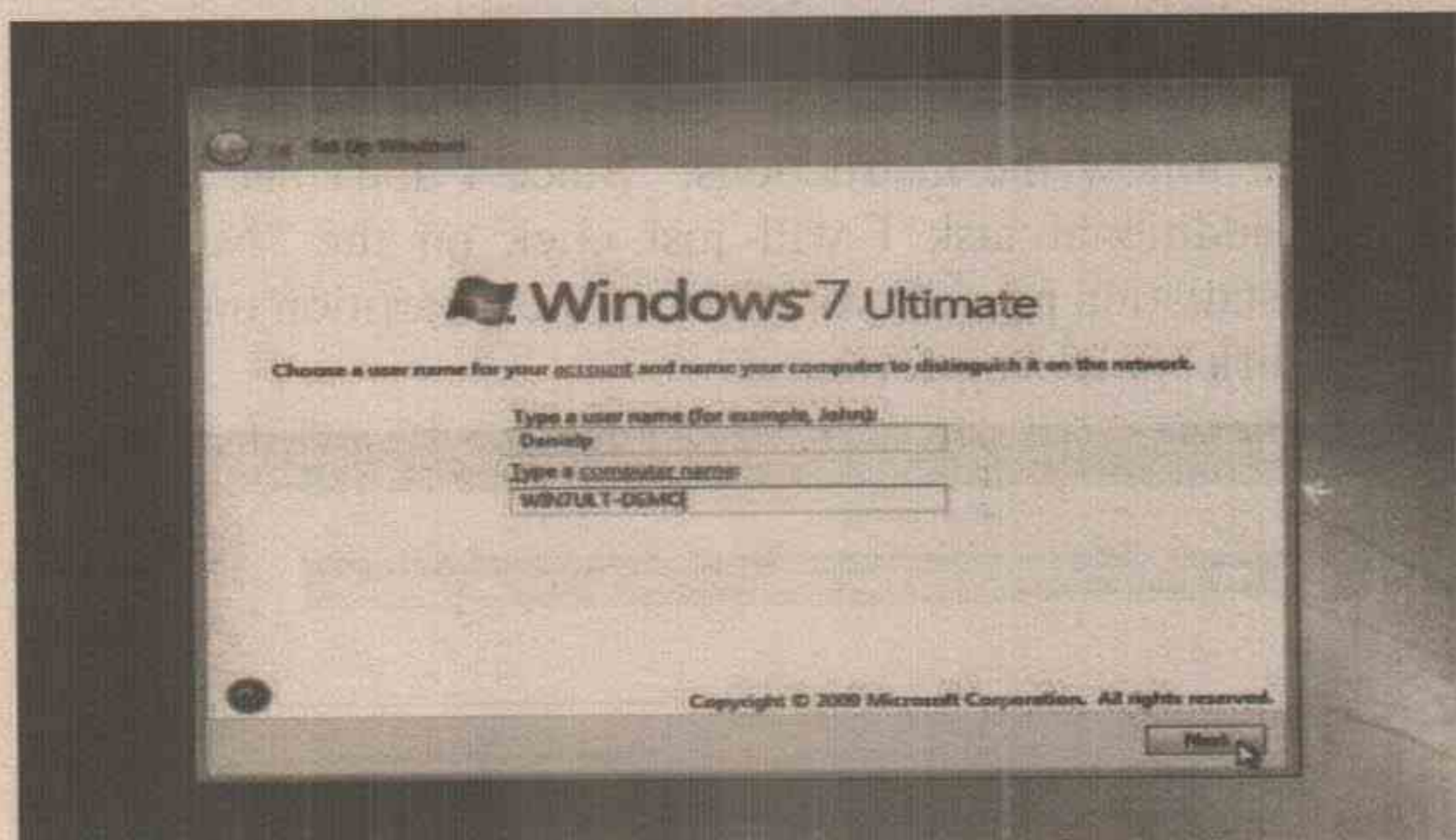


The setup process will now begin to copy files from the installation DVD media to the hard disk



The computer will reboot, and the next thing you'll see is the prompt to set the user's and computer's name. By default, the computer's name will be perfect24u.com where username is the username you've entered.

Click on "Next".



Configuring Disks and Drives Using Disk Management

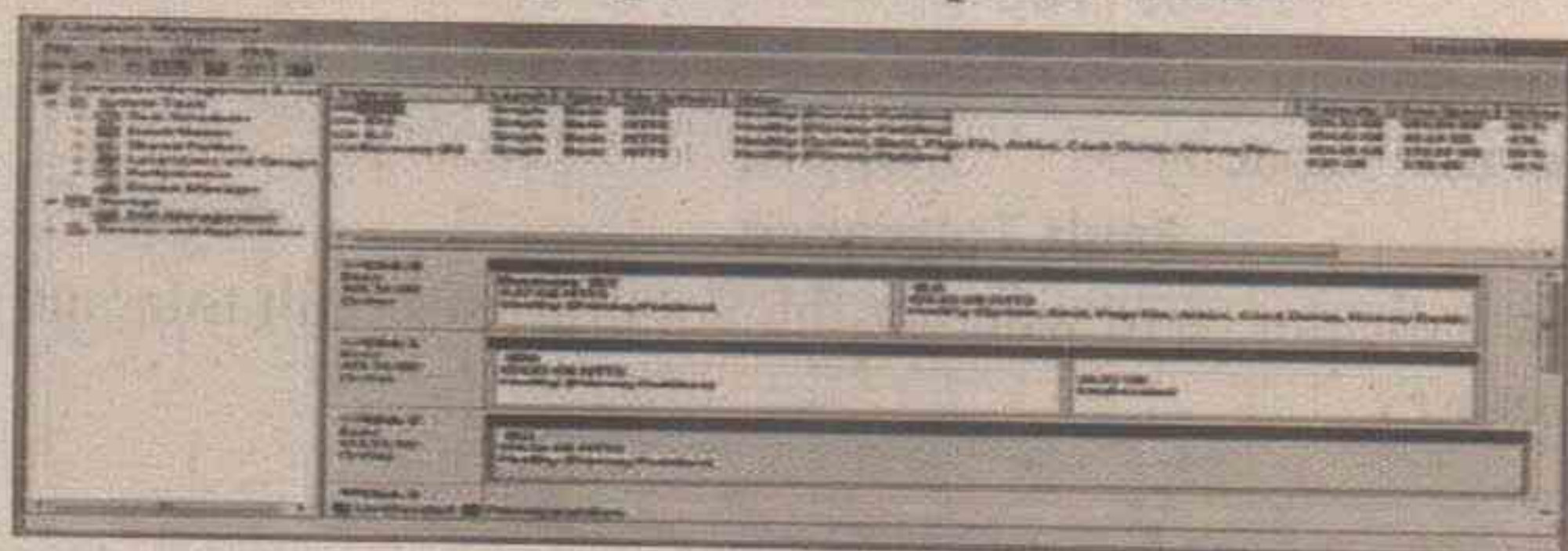
Your primary tool for working with your computer's disks is Disk Management. You will use Disk Management to partition disks, format disk volumes with file systems, and mount disk volumes. You can also use Disk Management to convert a disk from the basic disk type to the dynamic disk type and vice versa. However, while you can convert from a basic disk type to the dynamic disk type without losing data, you must remove disk volumes on a dynamic disk before you can convert the disk to the basic disk type.

Using an Administrator account, you can start and work with Disk Management by completing the following steps:

1. Right-click Computer on the Start menu.
2. On the shortcut menu, choose Manage to start Computer Management.
3. In the left pane of the Computer Management window, select Disk Management under Storage.

As Figure shows, Disk Management provides an overview of the storage devices configure within or attached to your computer. By default, Disk Management's main windows show the Volume list view in the upper panel and the Graphical view in the lower panel. The third view available but not displayed is the Disk List view.

Figure: Managing your computer's disks



You can set the view for the top or bottom pane using options from the View menu. To change the top view, select View, choose Top, and then select the view you want to use. To change the bottom view, select View, choose Bottom, and then select the view you want to use.

Volume list view provides a detailed summary of internal drives and external devices with removable storage. Devices with removable media, such as CD-ROM and DVD-ROM drives, are listed only if you've inserted a CD or DVD. The volume details provide the following information:

Volume

The drive letter or the volume name and drive letter, such as C:

Layout

The layout type of the volume, such as simple

Type

The drive type, such as basic or dynamic

File System

The file system type, such as FAT or NTFS

Status

The status of the volume, as well as any relevant volume designations, such as Healthy (Active, Primary Partition)

Capacity

The amount of data the volume can store

Free Space

The amount of free space in megabytes or gigabytes.

% Free

The amount of free space as a percentage of total volume capacity

Fault Tolerance

An indicator as to whether the volume uses fault tolerant features

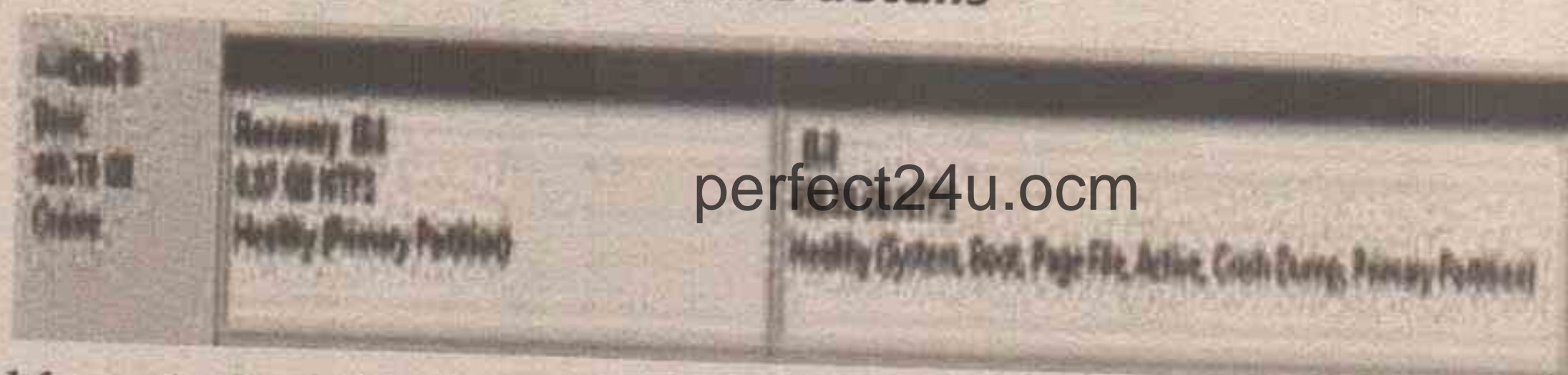
Overhead

The total additional disk space required because of the fault tolerant feature used (if applicable)

The Graphical view provides a graphical overview of internal drives, external drives with removable storage, and devices with removable media. This is the view you use to partition, format, and mount disks.

In the Graphical view, you can see the individual areas of allocated and unallocated space on internal disks and disks with removable storage. An allocated area of a disk has a volume. An unallocated area of a disk is free space that's not being used. As Figure shows.

Figure Viewing disk and volume details



Although Disk Management can show only two view panes at a time, you can display the Disk List view in either the upper or the lower pane of the main window. As Figure 3 shows, the Disk List view provides summary information about physical drives. This information includes:

Disk

The disk designator and number, such as Disk 0 or CD-ROM 1.

Type

The drive or media type, such as basic, dynamic, removable, CD, or DVD. Also displays the drive letter if one is assigned.

Capacity

The amount of data the drive, device, or media can store.

Unallocated Space

The amount of space that hasn't been allocated (if any).

Status

The drive or device status, such as online, online (errors), no media, or offline.

Device Type

The device interface type, such as Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI), USB, or FireWire (1394).

Partition Style

The partition style of the disk or device. Windows 7 supports both Master Boot Record (MBR) and GUID Partition Table (GPT) partition styles. For the most part, the partition style used is determined by your computer's processor architecture and the type of device.

Figure Viewing a list of disks

Disk	Type	Capacity	Unallocated Space	Status	Device Type	Partition Style
Disk 0	Basic	465.76 GB	2 MB	Online	UNKNOWN	MBR
Disk 1	Basic	465.76 GB	10.93 GB	Online	UNKNOWN	MBR
Disk 2	Basic	931.51 GB	2 MB	Online	UNKNOWN	MBR
Disk 3	Removable (H:)	0 MB	0 MB	No Media	USB	MBR
Disk 4	Removable (I:)	0 MB	0 MB	No Media	USB	MBR
Disk 5	Removable (J:)	0 MB	0 MB	No Media	USB	MBR
Disk 6	Removable (K:)	0 MB	0 MB	No Media	USB	MBR
CD-ROM 0	DVD (F:)	0 MB	0 MB	No Media	IDE	MBR
CD-ROM 1	DVD (G:)	0 MB	0 MB	No Media	IDE	MBR

When you are working with basic or dynamic disks, you should note the special designations assigned to drive sections. Drive sections can have one or more of the following designations:

Active

The drive section used for system cache and startup. Some devices with removable storage may be listed as having the active partition, such as when you use Ready Boost.

System

The drive section containing the boot manager files needed to load the operating system. A drive section with this designation can't be part of a striped or spanned volume.

Boot

The drive section containing the operating system and its related files.

Page File

A drive section containing a paging file used by the operating system.

Crash Dump

The drive section to which the computer attempts to write dump files in the event of a system crash.

Your computer has one active, one system, one boot, and one crash dump drive section. The page file designation is the only drive designation you might see on multiple drive sections.

Depending on the disk type and status, you might also see the following designations:

At Risk

A drive section with this designation is at risk of failing, and probably also has an error status, such as Online (Errors).

Primary Partition

A drive section that is designated as a primary partition. Although this designation is usually displayed only for fixed disks, you may see this designation on devices with removable storage and on devices with removable media.

Create a New Partition on a Windows 7 Hard Disk

The Windows 7 Disk Management tool provides a simple interface for managing partitions and volumes. Here's an easy way to create a new partition on your disk.

1. Open the Disk Management console by typing `diskmgmt.msc` at an elevated command prompt. In Disk Management's Graphical view, right-click an unallocated or free area, and then click New Simple Volume. This starts the New Simple Volume Wizard. (Note: If you need to create unallocated space, see the Tip Easily Shrink a Volume on a Windows 7 Disk for information on how to do this.)
2. Read the Welcome page and then click Next.
3. The Specify Volume Size page specifies the minimum and maximum size for the volume in megabytes and lets

you size the volume within these limits. Size the partition in megabytes using the Simple Volume Size field and then click Next.

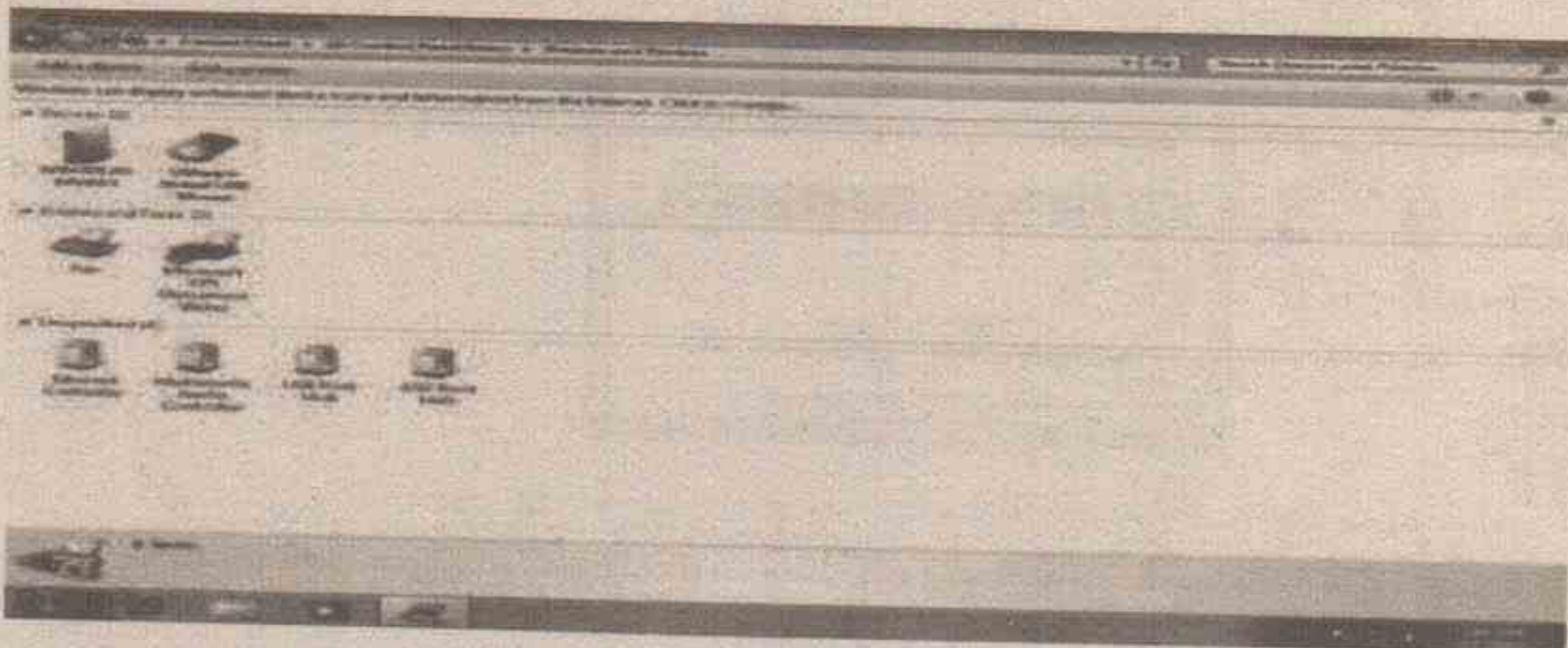
4. On the Assign Drive Letter Or Path page, specify whether you want to assign a drive letter or path and then click Next. The available options are as follows:
Assign The Following Drive Letter Select an available drive letter in the selection list provided. By default, Windows 7 selects the lowest available drive letter and excludes reserved drive letters as well as those assigned to local disks or network drives.
5. Mount In The Following Empty NTFS Folder Choose this option to mount the partition in an empty NTFS folder. You must then type the path to an existing folder or click Browse to search for or create a folder to use.
Do Not Assign A Drive Letter Or Drive Path Choose this option if you want to create the partition without assigning a drive letter or path. Later, if you want the partition to be available for storage, you can assign a drive letter or path at that time.
6. Use the Format Partition page to determine whether and how the volume should be formatted. If you want to format the volume, choose Format This Volume With The Following Settings, and then configure the following options:
File System Sets the file system type as FAT, FAT32, or NTFS. NTFS is selected by default in most cases. If you create a file system as FAT or FAT32, you can later convert it to NTFS by using the Convert utility. You can't, however, convert NTFS partitions to FAT or FAT32.
Allocation Unit Size Sets the cluster size for the file

system. This is the basic unit in which disk space is allocated. The default allocation unit size is based on the size of the volume and, by default, is set dynamically prior to formatting. To override this feature, you can set the allocation unit size to a specific value. If you use many small files, you might want to use a smaller cluster size, such as 512 or 1,024 bytes. With these settings, small files use less disk space. Volume Label Sets a text label for the partition. This label is the partition's volume name and by default is set to New Volume. You can change the volume label at any time by right-clicking the volume in Windows Explorer, choosing Properties, and typing a new value in the Label field provided on the General tab.

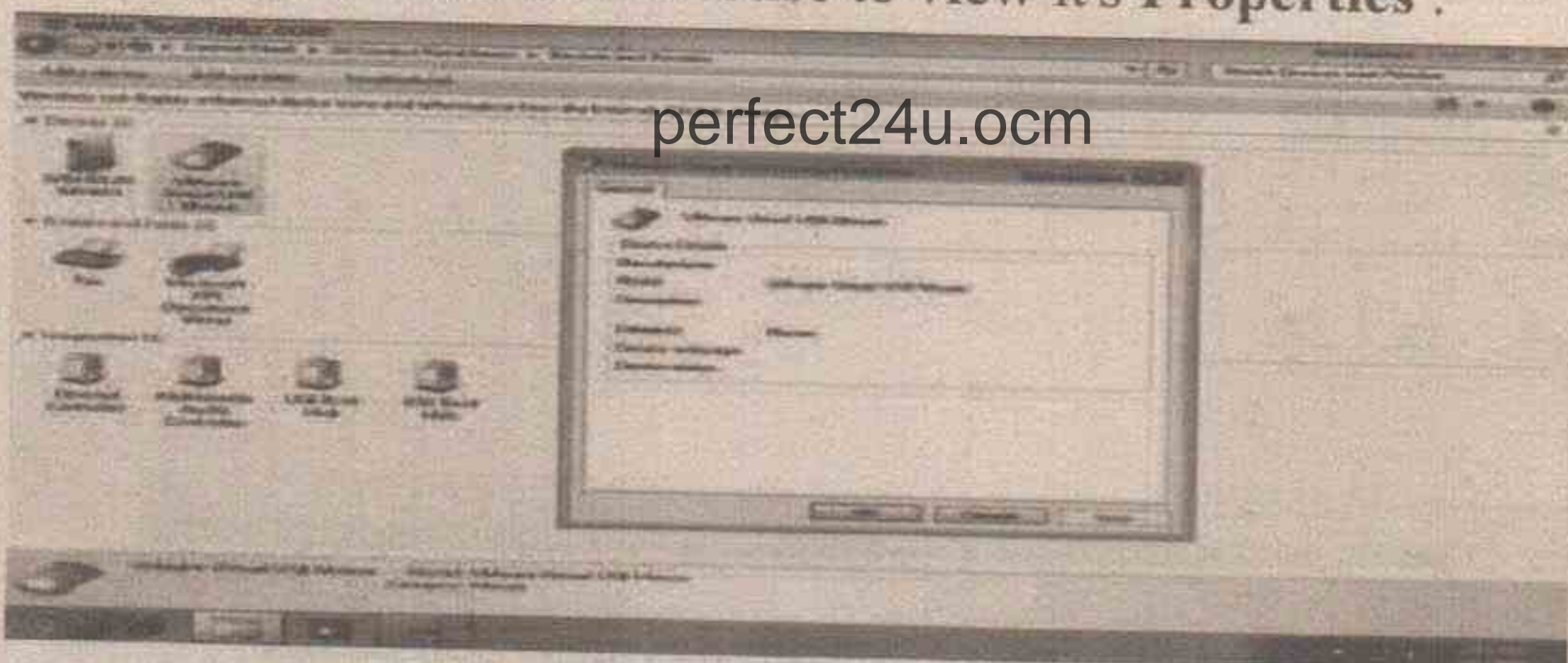
7. Perform A Quick Format Tells Windows 7 to format without checking the partition for errors. With large partitions, this option can save you a few minutes. However, it's usually better to check for errors, which enables Disk Management to mark bad sectors on the disk and lock the mount.
8. Enable File And Folder Compression Turns on compression for the disk. Built-in compression is available only for NTFS. Under NTFS, compression is transparent to users and compressed files can be accessed just like regular files. If you select this option, files and directories on this drive are compressed automatically.

Click Next, confirm your options, and then click Finish.

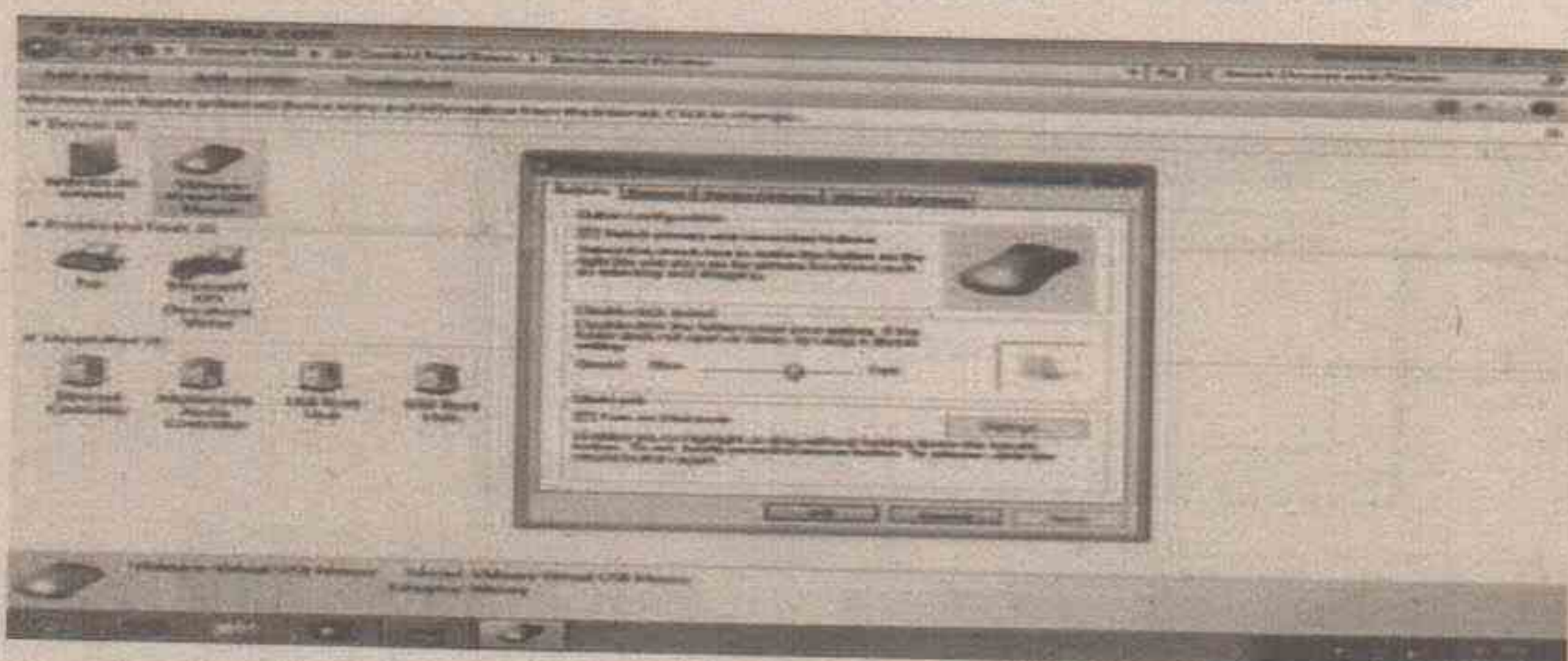
3. The **Device and Printer** window opens up with the list of all external devices and printer.



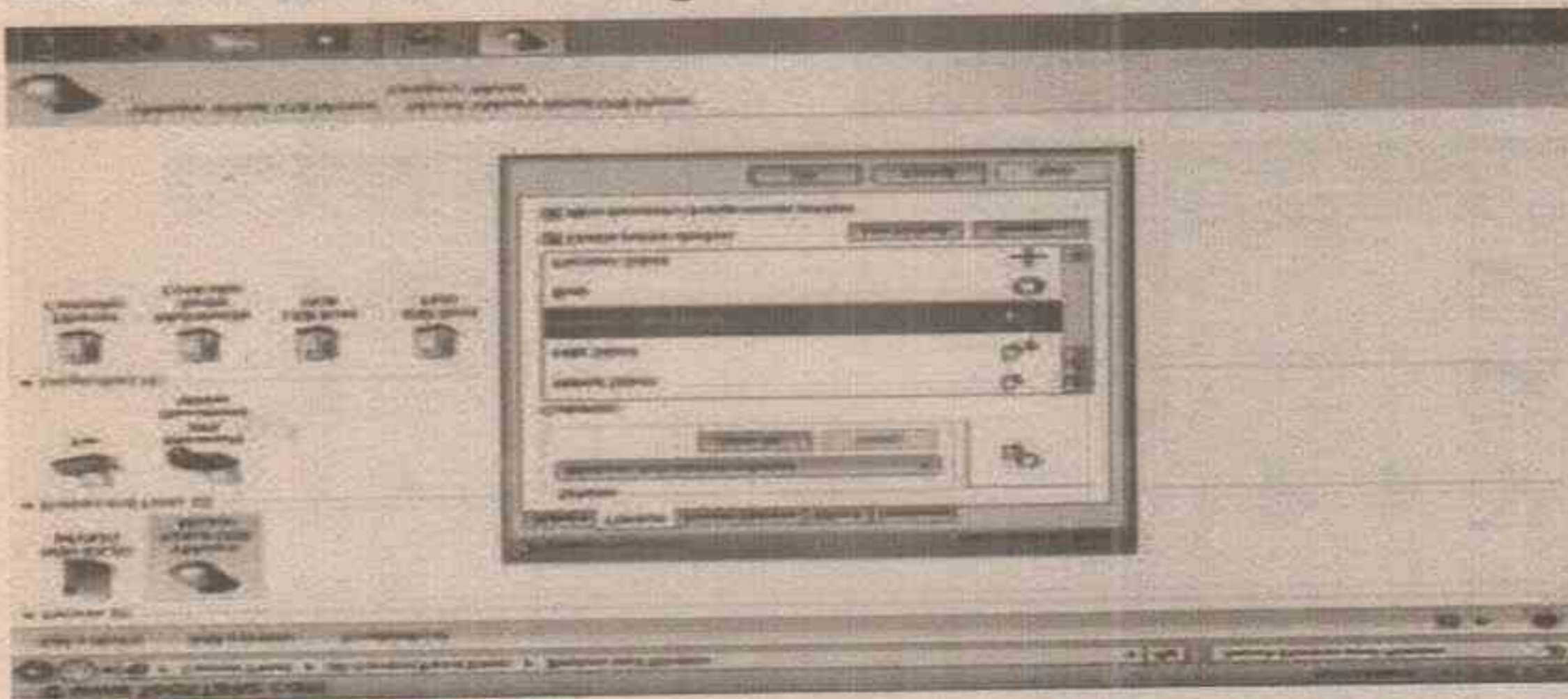
4. Click on **Virtual USB Mouse** to view its **Properties**.



5. Right-click on the **Mouse** icon and click **Mouse Settings**.



Click **Pointers** tab to change the Pointer settings.

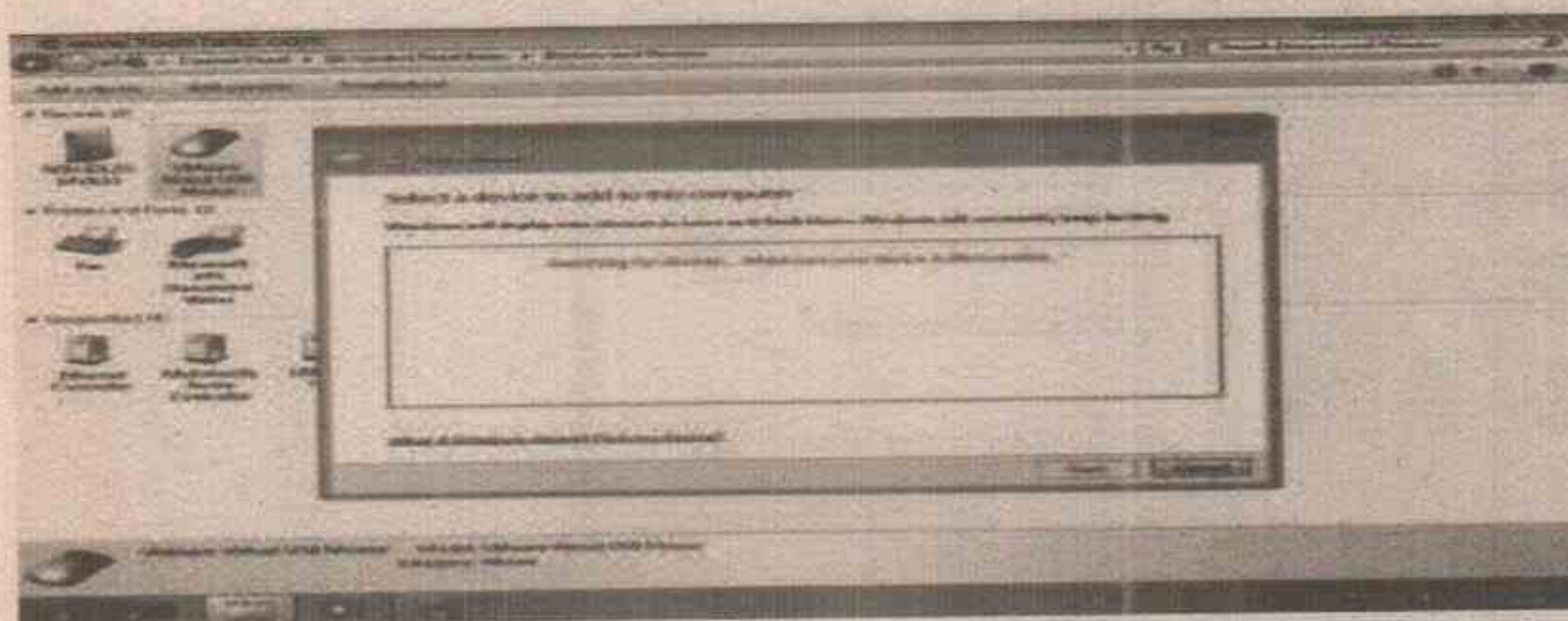


Click **Apply** and **Ok**.

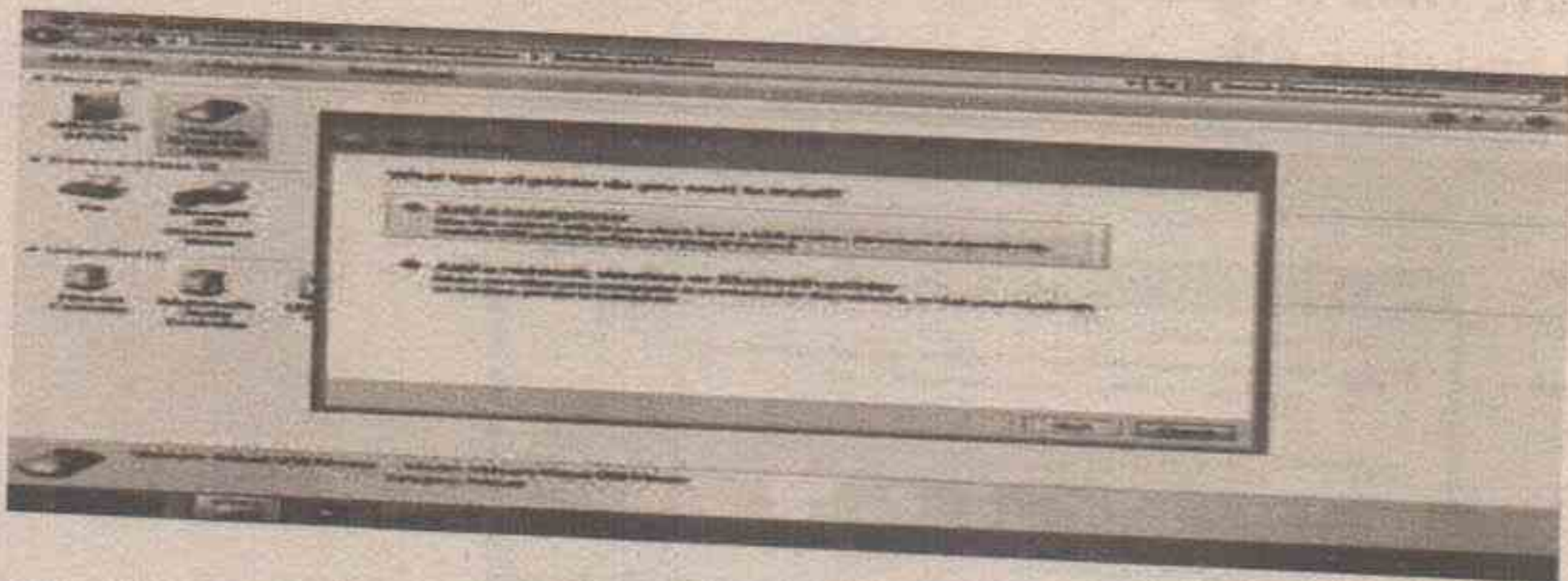
6. To Add a **Wireless** or network device click **Add a device**.



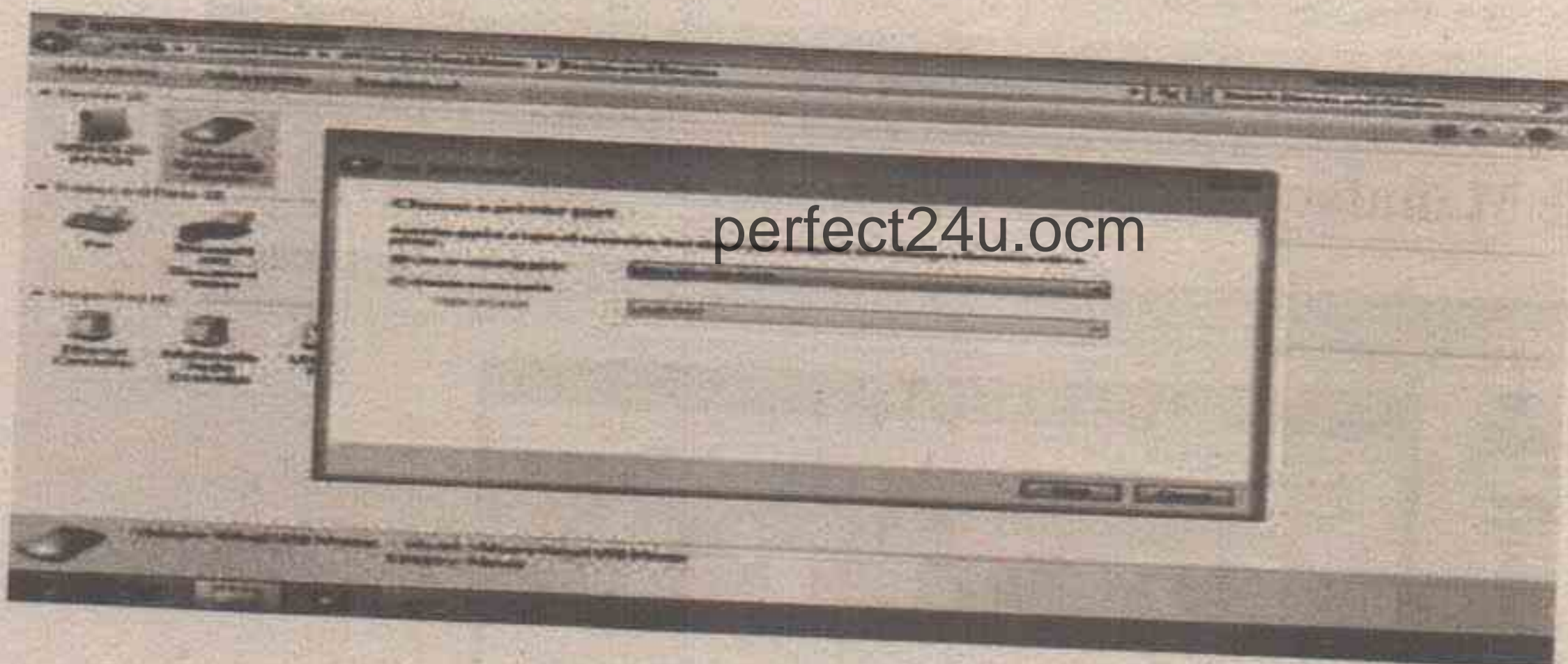
It may take **some time** to search for the devices. **Select the device** and **follow the instructions**.



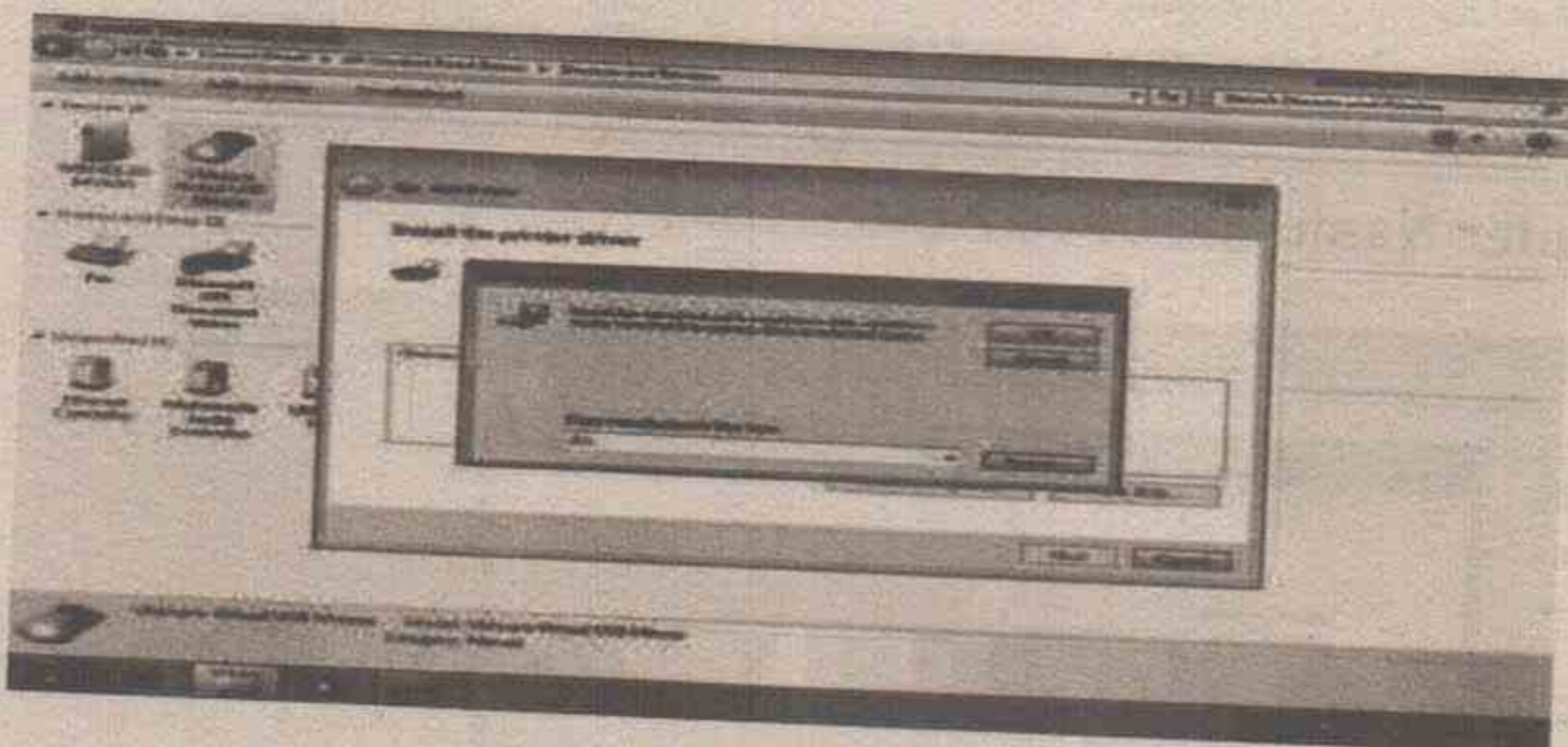
7. Click **Add a printer** to add new printer.



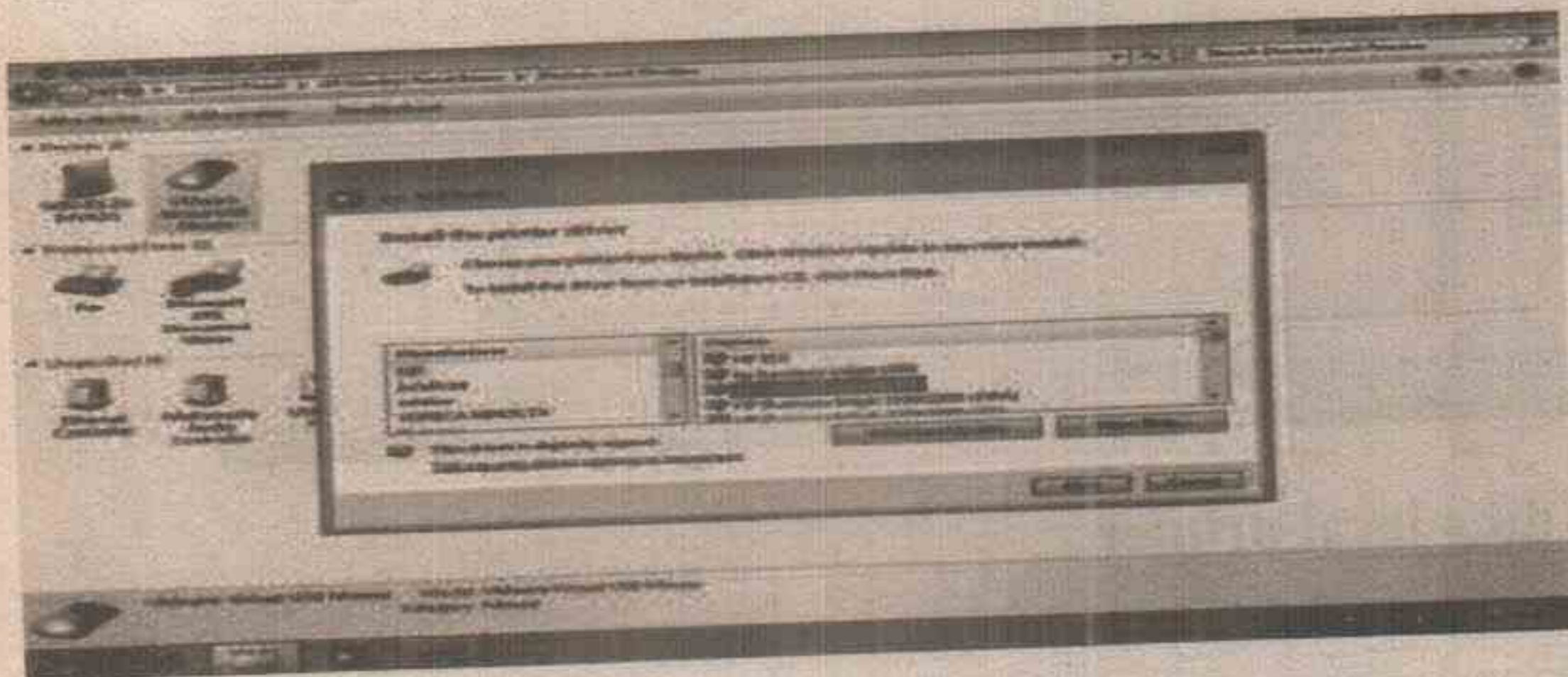
Click **Add a local printer**.



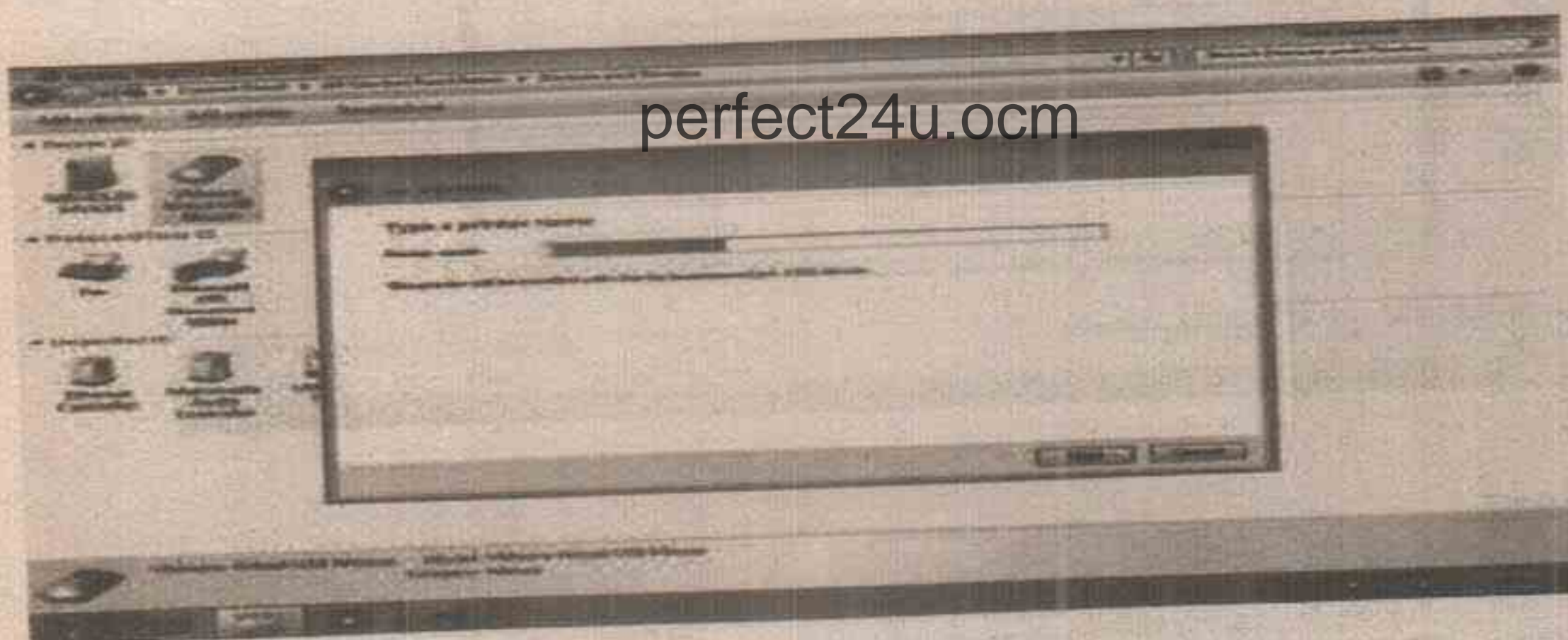
Click **Next**.



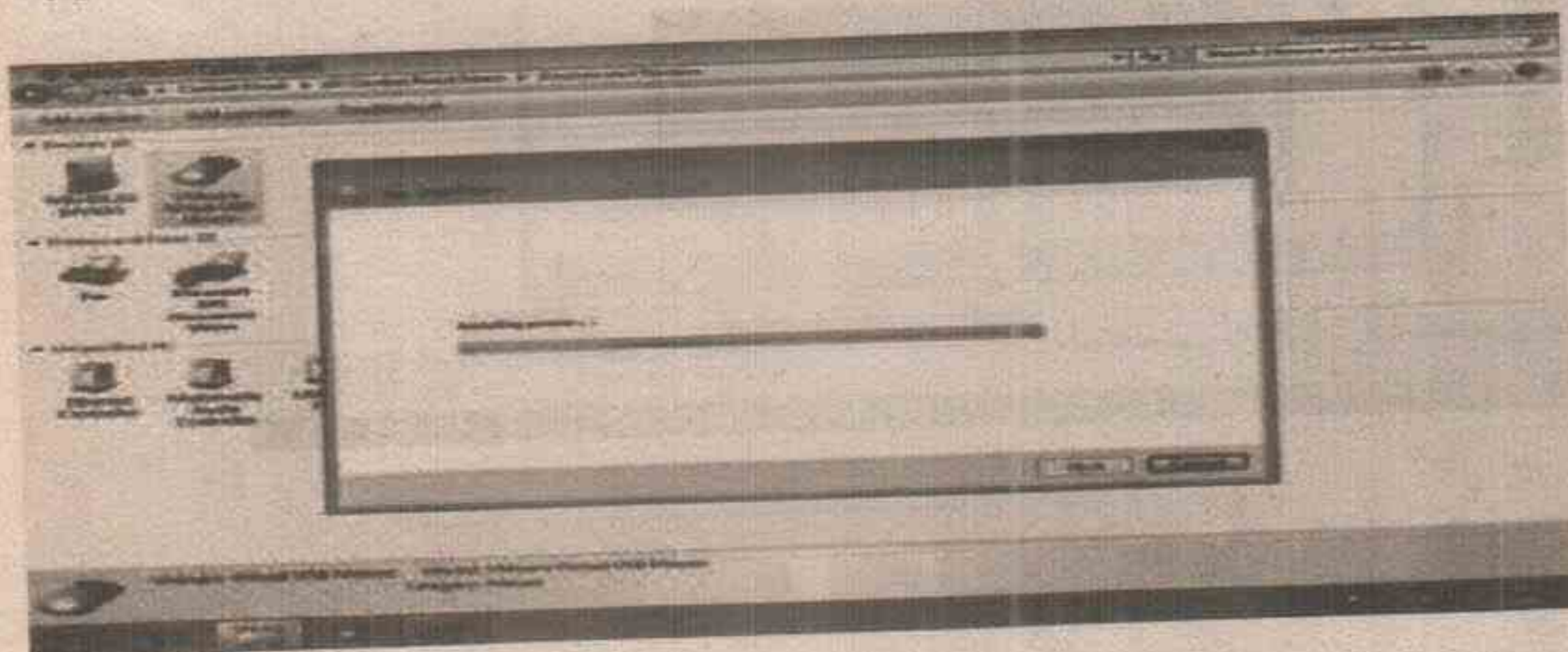
Click **Have Disk** to install **Printer Driver**. Browse driver location and click **Ok**.



Choose **Manufacturer** and **Printer**. Click **Next**.



Type **Printer Name** and Click **Next**.



A screenshot of a Windows XP desktop environment. A security warning dialog box is open in the center, displaying a message about a file named "C:\Program Files\Internet Explorer\Internet Explorer.exe" that has been modified by a program named "Internet Explorer". The dialog box has a yellow border and a "Details" button. The desktop background is a light blue gradient. The taskbar at the bottom shows the Start button and several open applications, including Internet Explorer and the Windows Explorer. The system tray in the bottom right corner shows the date and time as "12/27/2007 12:00 PM".

Step 2 Enter the IP address or domain name of the server to which you want to connect. If you're connecting to a work network, your IT administrator can provide the best address.

Step 3 If you want to set up the connection, but not connect, select *Don't connect now*; otherwise, leave it blank and click *Next*.

Step 4 On this next screen, you can either put in your username and password, or leave it blank. You'll be prompted for it again on the actual connection. Click *Connect*.

Step 5 To connect, click on the Windows network logo on the lower-right part of your screen; then select *Connect* under VPN Connection.

Step 6 In the Connect VPN Connection box, enter the appropriate domain and your log-in credentials; then click *Connect*.



Step 7 If you can't connect, the problem could be due to the server configuration. (There are different types of VPN.) Check with your network administrator to see what kind is in use--such as PPTP--then, on the Connect VPN Connection screen, select *Properties*.

Step 8 Navigate to the Security tab and select the specific Type of VPN from the drop-down list. You may also have to unselect *Include Windows logon domain* under the Options tab. Then click *OK* and *Connect*.

Step by Step: Building a VPN (Incoming)

Step 1 Click the *Start* button, and, in the search bar, type **Network and Sharing**.

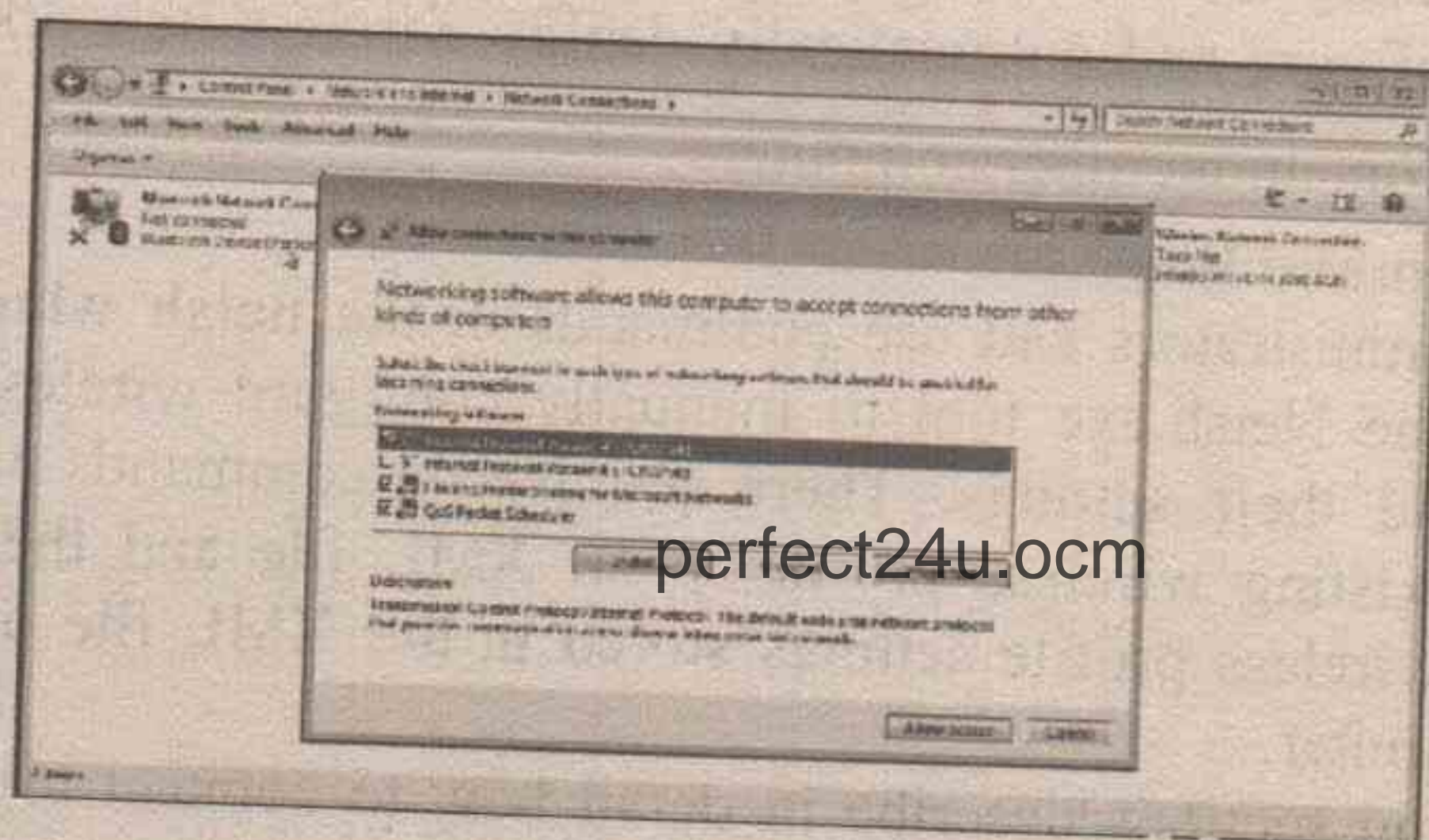
Step 2 Click *Change Adapter Settings* in the left-hand menu.

Step 3 Click *File*, and then *New Incoming Connection*.

Step 4 Select the users you'd like to give access to and click *Next*.

Step 5 Click *Through the Internet* and select *Next*.

Step 6 Select the Internet Protocol you'd like to use. (The default TCP/IPv4--the line highlighted in the screenshot below--will work fine.)



Step 7 Finally, click *Allow access*; you've now set up an incoming VPN connection.

COMPUTER NETWORK CONNECTING TO WIRELESS NETWORKS WITH WINDOWS 7

Wireless network configuration methods

You can configure connections to wireless networks, known as wireless profiles, for a computer running Windows 7 with the following methods

- **Network notification area icon**
This is the primary method by which users connect to available wireless networks.
- **Set up a connection or network dialog box**

This is a method by which users can manually create wireless network profiles

- **Manage Wireless Networks** dialog box

This is another method to manually configure wireless networks

- **Group Policy**

Network administrators can use Group Policy settings in an Active Directory Domain Services (AD DS) environment to centrally configure and automatically deploy wireless network settings for domain member computers

- **Command line**

Network administrators can use commands in the **netsh wlan** context of the Netsh.exe tool to manually configure wireless networks and their settings. There are Netsh commands to export an existing wireless profile to an XML file and then import the wireless profile settings stored in the XML file on another computer.

The following sections describe in detail how to connect to a wireless network using the Network notification area icon and the **Set up a connection or network** dialog box in Windows 7, how to manage your wireless networks, and how to connect to non-broadcasting wireless networks.

The Network notification area icon

To connect to an available wireless network, click the Network icon in the notification area of your desktop. The resulting pane contains a list of detected wireless networks and, for domain-joined computers, the names of wireless networks configured through Group Policy. Figure shows an example.

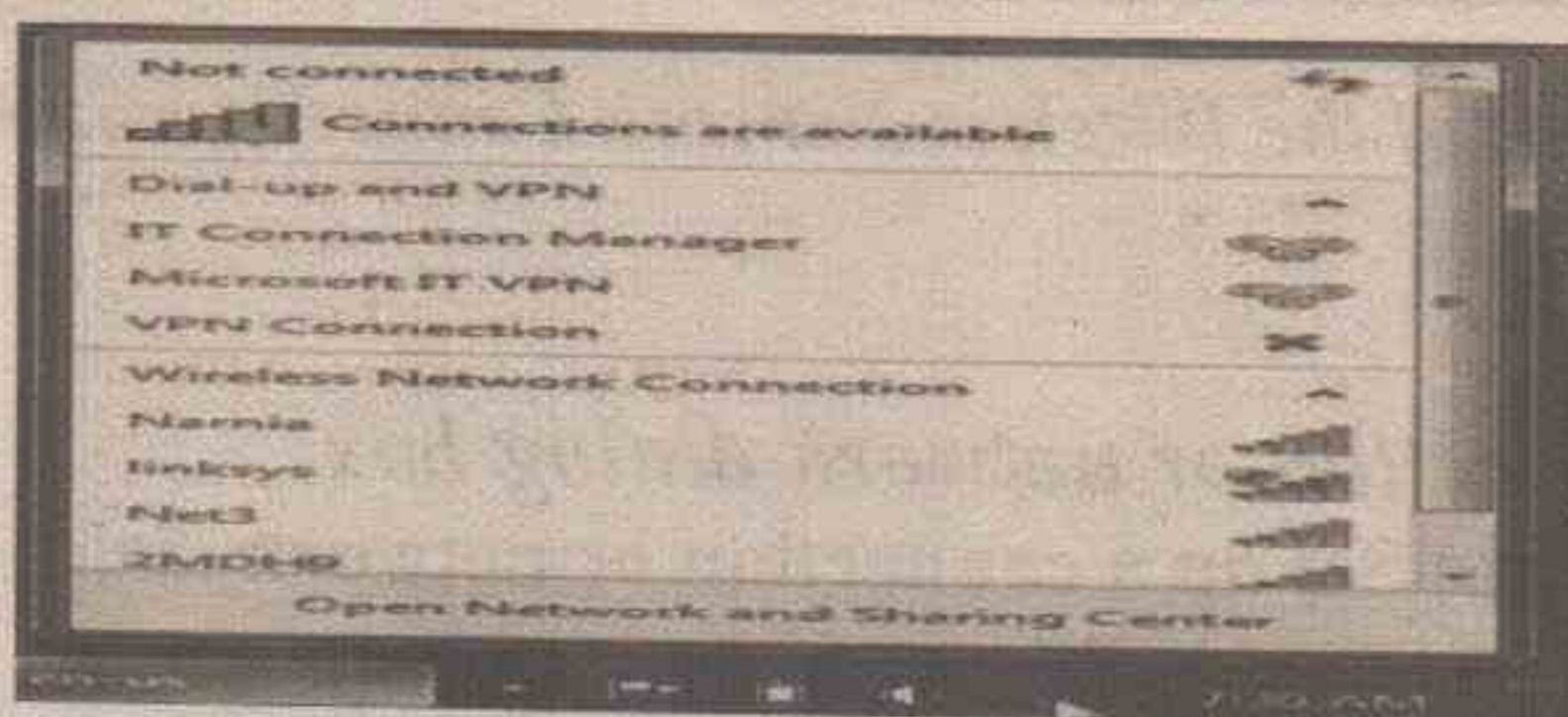


Figure Example of the list of available networks

From this pane you can connect to a listed wireless network by double-clicking it, clicking the network and then clicking **Connect**, or by right-clicking the network and clicking **Connect**. To view information for a listed wireless network, place the mouse pointer over the network name. The information includes the wireless network's name, signal strength, security type, radio type (802.11b/g/n), and Service Set Identifier (SSID). To refresh the list of wireless networks, click the up/down arrow icon in the upper right of the pane. To disconnect from a connected wireless network, right-click the network and then click **Disconnect**.

You can obtain status of a connected network and properties of a connected network or a network that has been configured through Group Policy through the wireless network's context menu. Figure shows an example of the **Wireless Network Connection Status** dialog box.

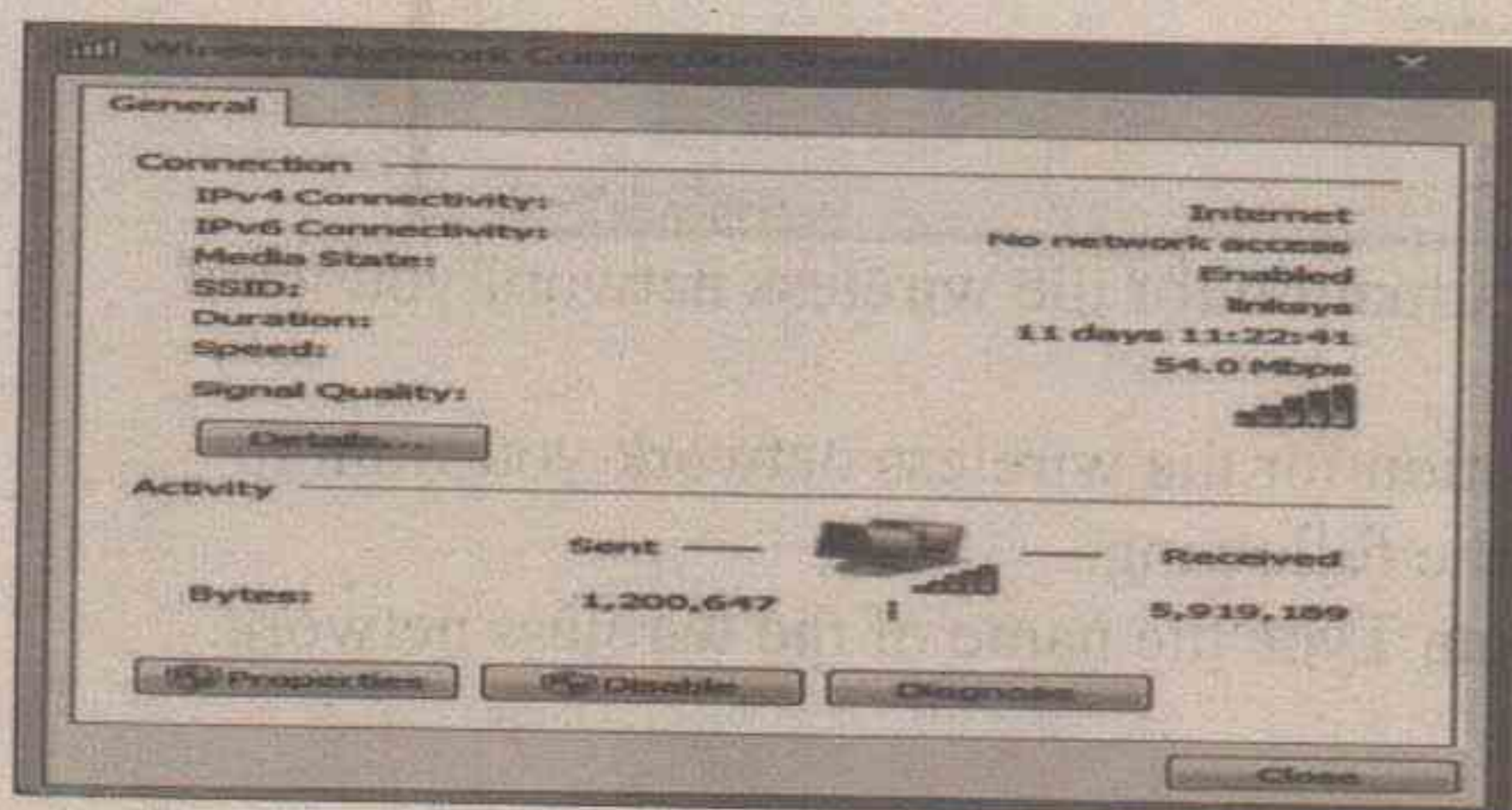


Figure Example of the Wireless Network Connection Status dialog box

Set up a connection or network dialog box

You can access the **Set up a connection or network** dialog box in Windows 7, as shown in Figure, from the **Set up a new connection or network** link in the Network and Sharing center.

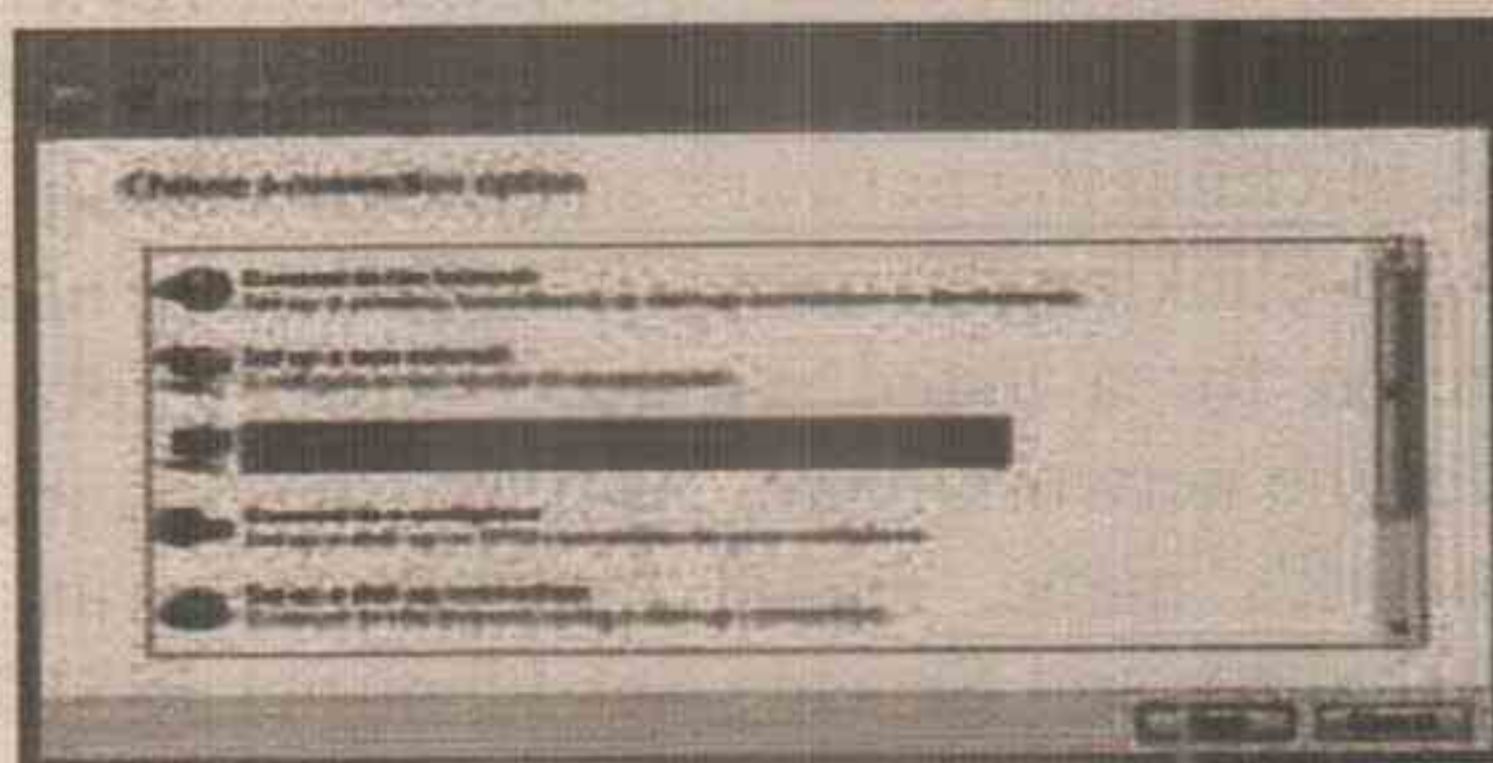


Figure The Set up a connection or network dialog box

To manually create a wireless network profile, click manually connects to a wireless network, and then clicks Next. You should see Figure.

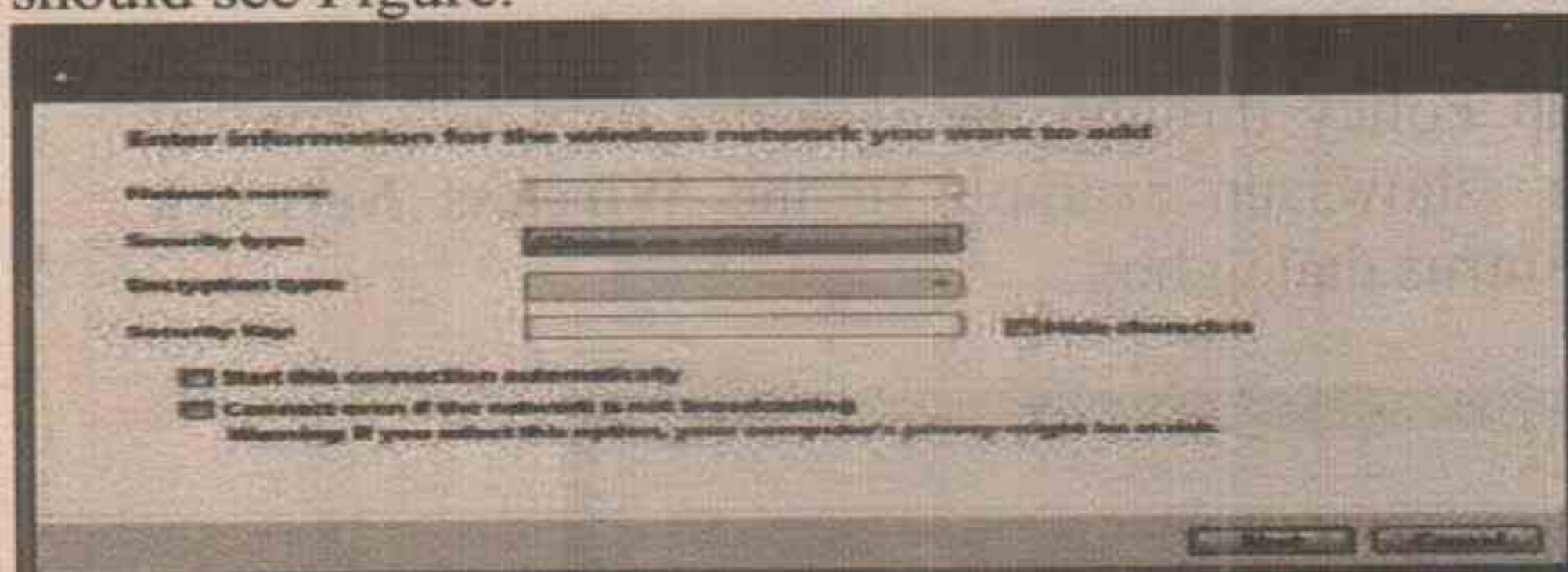


Figure The Enter information for the wireless network you want to add page

On the Enter information for the wireless network you want to add page, configure the following:

- **Network name** Type the name of the wireless network.

- **Security type** Select the method used to authenticate a connection to the wireless network. The choices are the following:
 - **No authentication (Open)** Open system authentication with no encryption.
 - **WEP** Open system authentication with Wired Equivalent Privacy.
 - **WPA2-Personal** Wi-Fi Protected Access 2 (WPA2) with a preshared key (also known as a passphrase).
 - **WPA-Personal** Wi-Fi Protected Access (WPA) with a preshared key.
 - **WPA2-Enterprise** WPA2 with IEEE 802.1X authentication.
 - **WPA-Enterprise** WPA with IEEE 802.1X authentication.
 - **802.1x** IEEE 802.1X authentication with WEP (also known ...)

The choices listed depend on the capabilities of your wireless network adapter that are reported to Windows. If an authentication type does not appear in the list, ensure that your wireless adapter supports the type and that you have installed the latest driver for your adapter that is compatible with Windows 7.

The shared key authentication method is not listed. Microsoft strongly discourages its use because it provides weak security for your wireless network. To configure shared key authentication, select **No authentication (Open)** here and then select **Shared** from the **Security** tab in the properties of the wireless network (described later in this article).

- **Encryption type** Select the method used to encrypt data sent over the wireless network. The choices depend on the selected security type.

- When you select the **No authentication (Open)** security type, **None** is selected for you.
- When you select the **WEP** security type, **WEP** is selected for you.
- When you select the **802.1x** security type, **WEP** is selected for you.
- When you select the **WPA2-Personal**, **WPA2-Enterprise**, **WPA-Personal**, **WPA-Enterprise** security types, you can select **AES**.

The encryption type choices listed depend on the capabilities of your wireless network adapter that it reports to Windows.

- **Security Key Type** the WEP key (if you selected the **WEP** security type), the WPA preshared key (if you selected the **WPA-Personal** security type), or the WPA2 preshared key (if you selected the **WPA2-Personal** security type). For the **WPA2-Enterprise**, **WPA-Enterprise**, and **802.1x** security types, Windows 7 automatically determines the security key when performing 802.1 X-based authentications.
- **Hide characters** Specifies whether you want to view the value typed in **Security Key**.
- **Starts this connection automatically** Specifies whether Windows 7 will automatically connect to this wireless network. If you clear this checkbox, you must manually connect to the wireless network from the list of networks available from the Network notification area icon.
- **Connect even if the network is not broadcasting** Specifies whether Windows should attempt to connect even if the wireless network is not broadcasting its name. This will cause Windows to send Probe Request frames to locate the wireless network. These probe request frames can be used by malicious users to determine the name of the non-broadcast network.

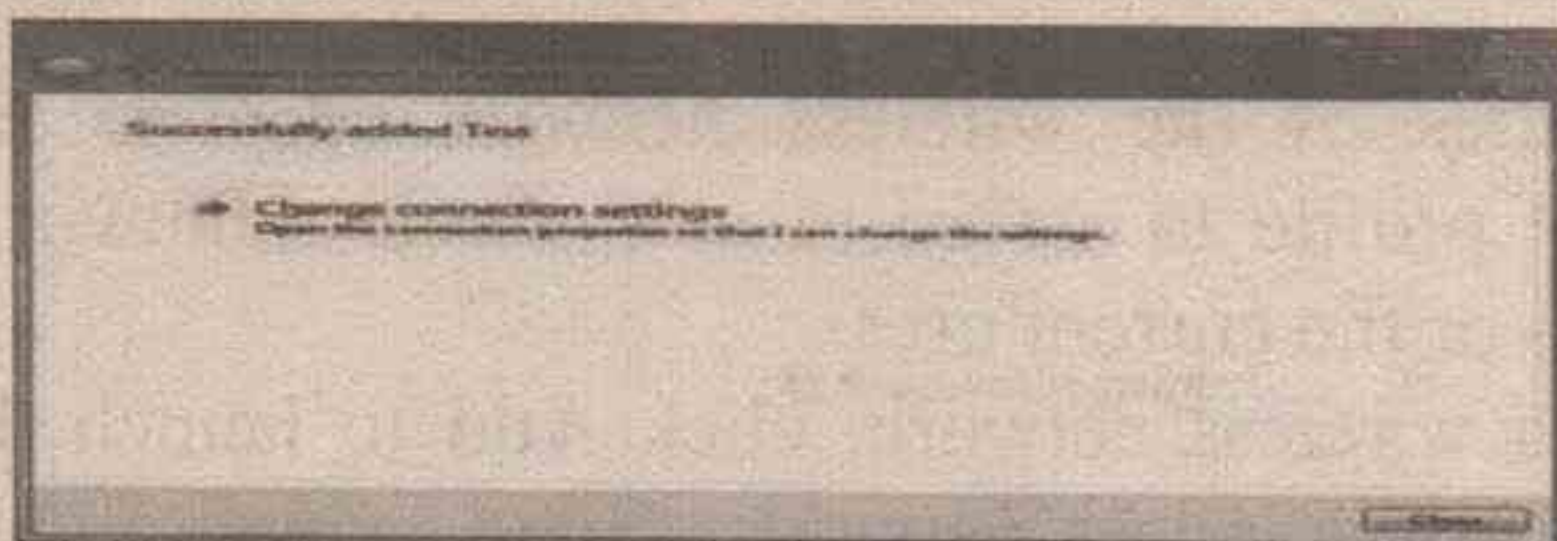


Figure The Successfully added page

You can click **Change connection settings** to access the properties of the wireless network, as described later in this article, or click **Close**.

The Manage Wireless Networks dialog box

You can access the **Manage Wireless Networks** dialog box from the **Manage wireless networks** link in the Network and Sharing Center. Figure shows an example

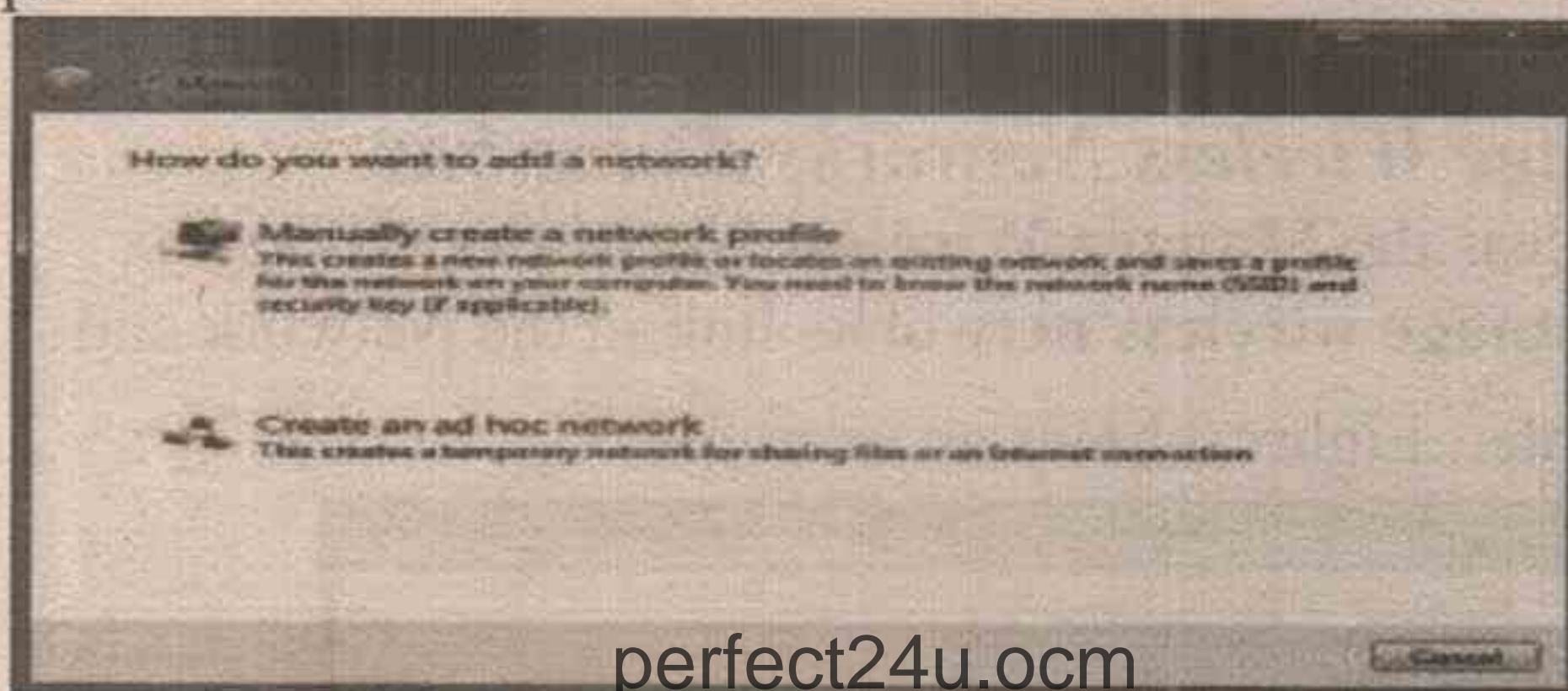


- **Note** If the **Manage wireless networks** link is not present from the Network and Sharing Center, click the **Change adapter settings** link and ensure that your wireless network adapter is enabled on your laptop or notebook computer, appears in the Network Connections folder as a wireless connection, and is enabled. If your wireless network adapter appears in the Network Connections folder as a wired connection, ensure that you have installed the latest driver that is compatible with Windows 7.

From the **Manage Wireless Networks** dialog box, you can add a new wireless network, remove a selected wireless network,

obtain the properties of the wireless network adapter, and choose the type of profile to assign to new wireless networks (applies to all users or the current user).

To manually add a wireless network, click **Add** to launch the Manually connect to a wireless network wizard, which allows you to create a wireless network profile for either an infrastructure or ad hoc wireless network. Figure shows an example.



To create a wireless profile for an infrastructure wireless network, click **Manually create a network profile**. To create a wireless profile for an ad hoc wireless network, click **Create an ad hoc network**.

To view or modify the properties of a wireless network in the list, double-click the name in the **Manage wireless networks** dialog box. Windows 7 displays the dialog box in Figure

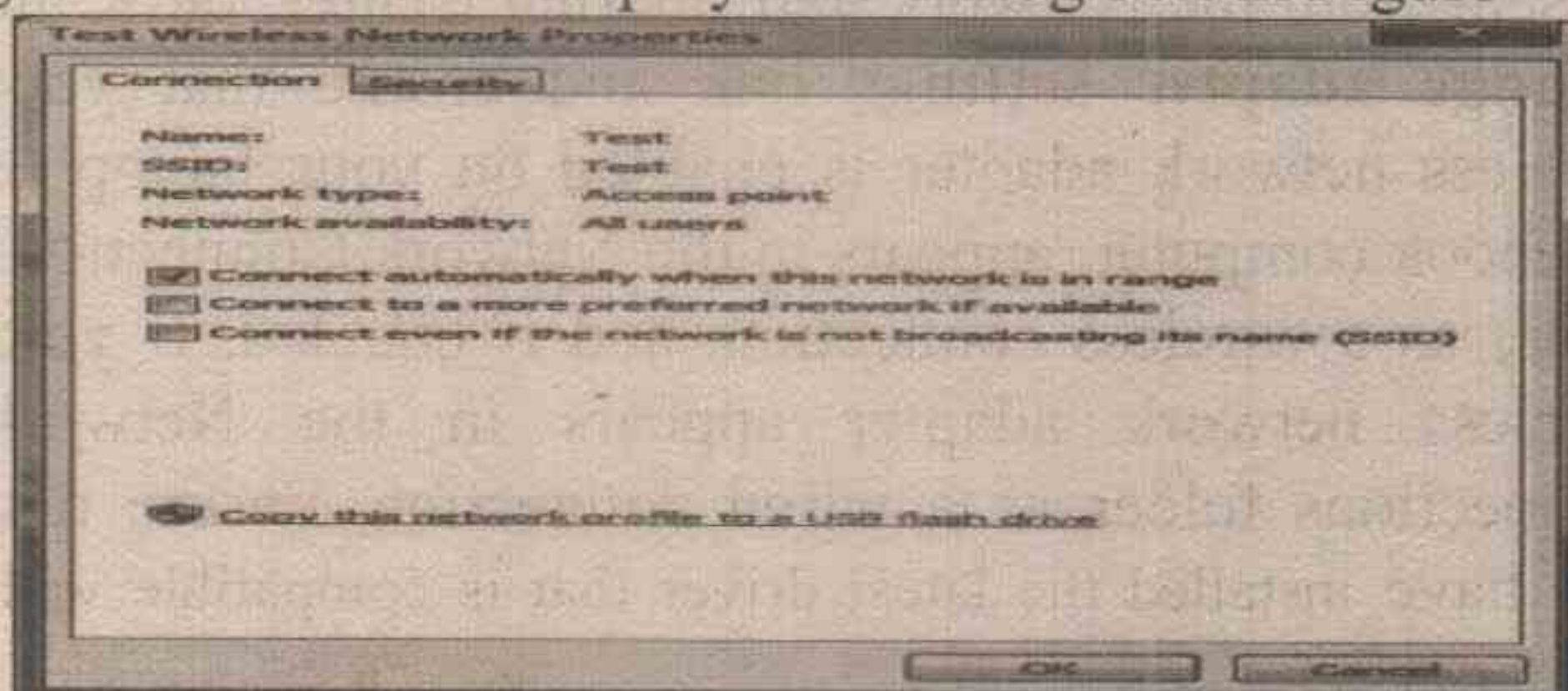


Figure The Wireless Network Properties dialog box

From the Connection tab, you can view the wireless network's name, SSID, network type (either Access point for infrastructure mode networks or Computer-to-computer for ad hoc mode networks), and availability. You can also configure the following:

- Connect automatically when the network is in range
- Connect to a more preferred network if available
- Specifies whether Windows 7 will automatically disconnect from this wireless network if a more preferred wireless network comes within range.
- Connect even if the network is not broadcasting its name (SSID)
- The **Copy this network profile to a USB flash drive** link launches the Copy Network Settings wizard, which writes the wireless network profile settings to a USB flash drive. You can then use this flash drive to automate the wireless network profile configuration of other computers.

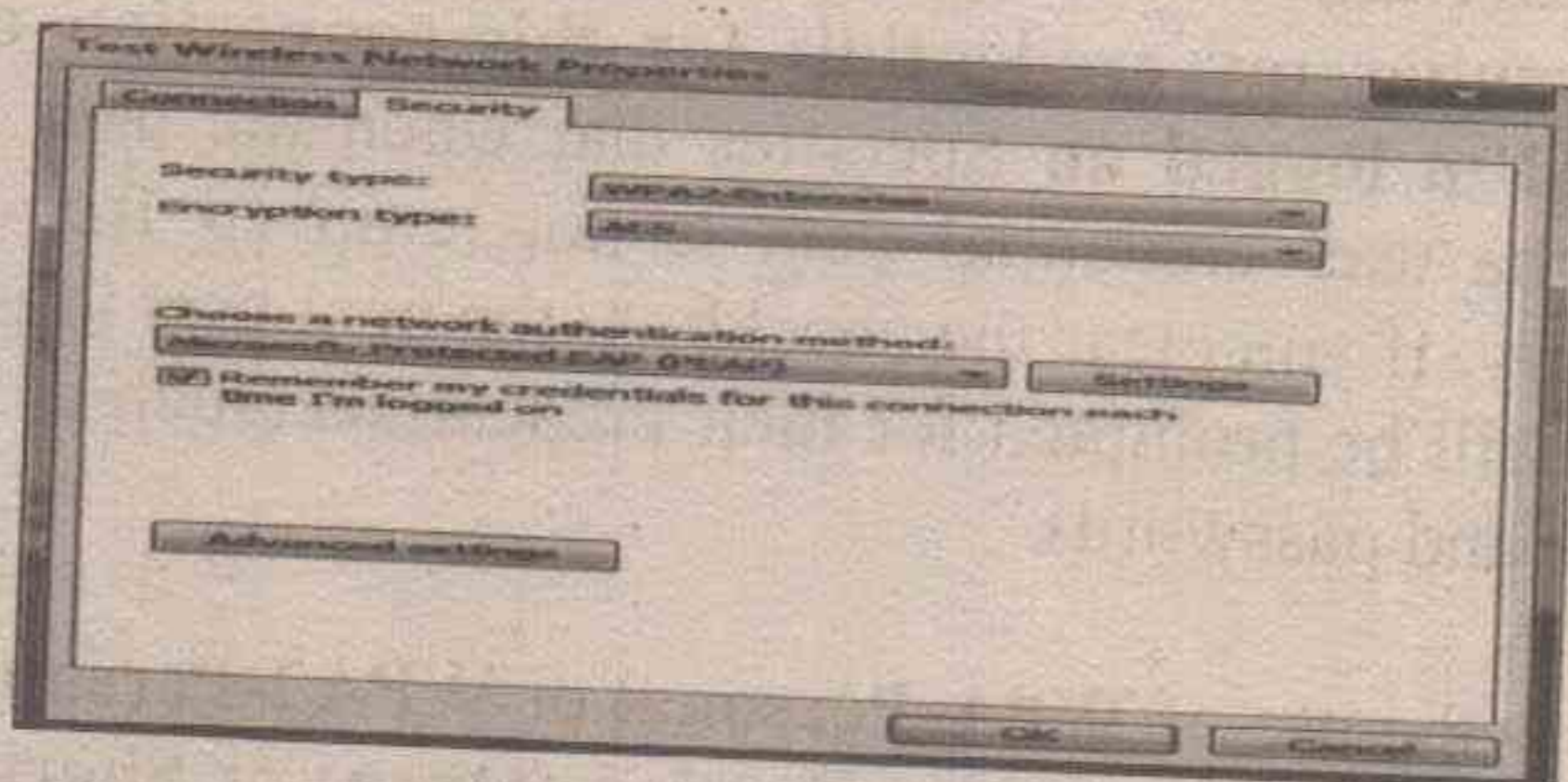


Figure The Security tab of the Wireless Network Properties dialog box

On the **Security** tab, you can specify the following security types:

- No authentication (Open)
- Shared

Shared key authentication. The **Security** tab is the only location where you can configure shared key authentication because its use is highly discouraged

- WPA2-Personal
- WPA-Personal
- WPA2-Enterprise
- WPA-Enterprise
- 802.1x

Based on the selected security type, you can configure either a network security key or specify and configure a network authentication method. If you specify **WPA-Enterprise**, **WPA2-Enterprise**, or **802.1x** as your security type, you must configure the following (as shown in the Figure 9):

- **Choose a network authentication method** Select an Extensible Authentication Protocol (EAP) method and click **Settings** to configure the EAP type as needed.
- **Remember my credentials for this connection each time I'm logged on** Specifies that when the user logs off, the user credential data is not removed from the registry. If you clear the checkbox, the next user logs on, they will be prompted for their credentials (such as user name and password).

If you specify the use of **WPA-Personal** or **WPA2-Personal** as your security type or **No authentication (Open)** or **Shared** as your security type with WEP as your encryption type, you must configure a network security key, as shown in Figure.

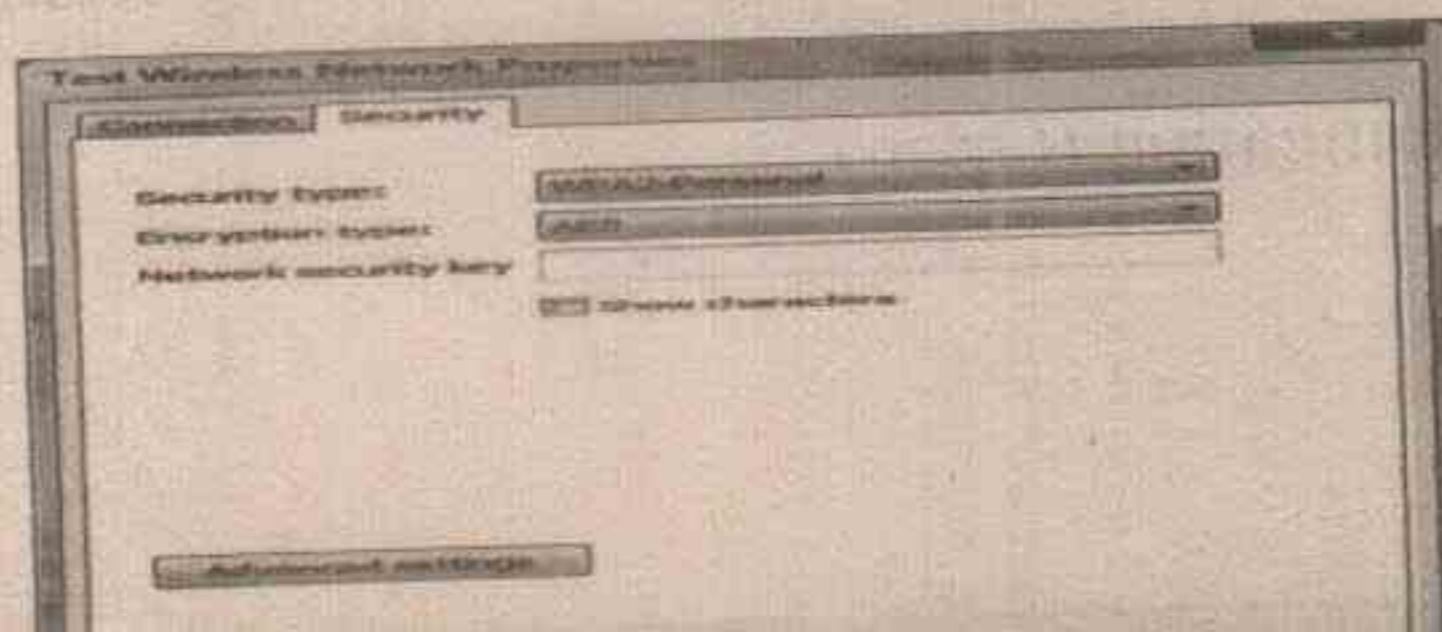
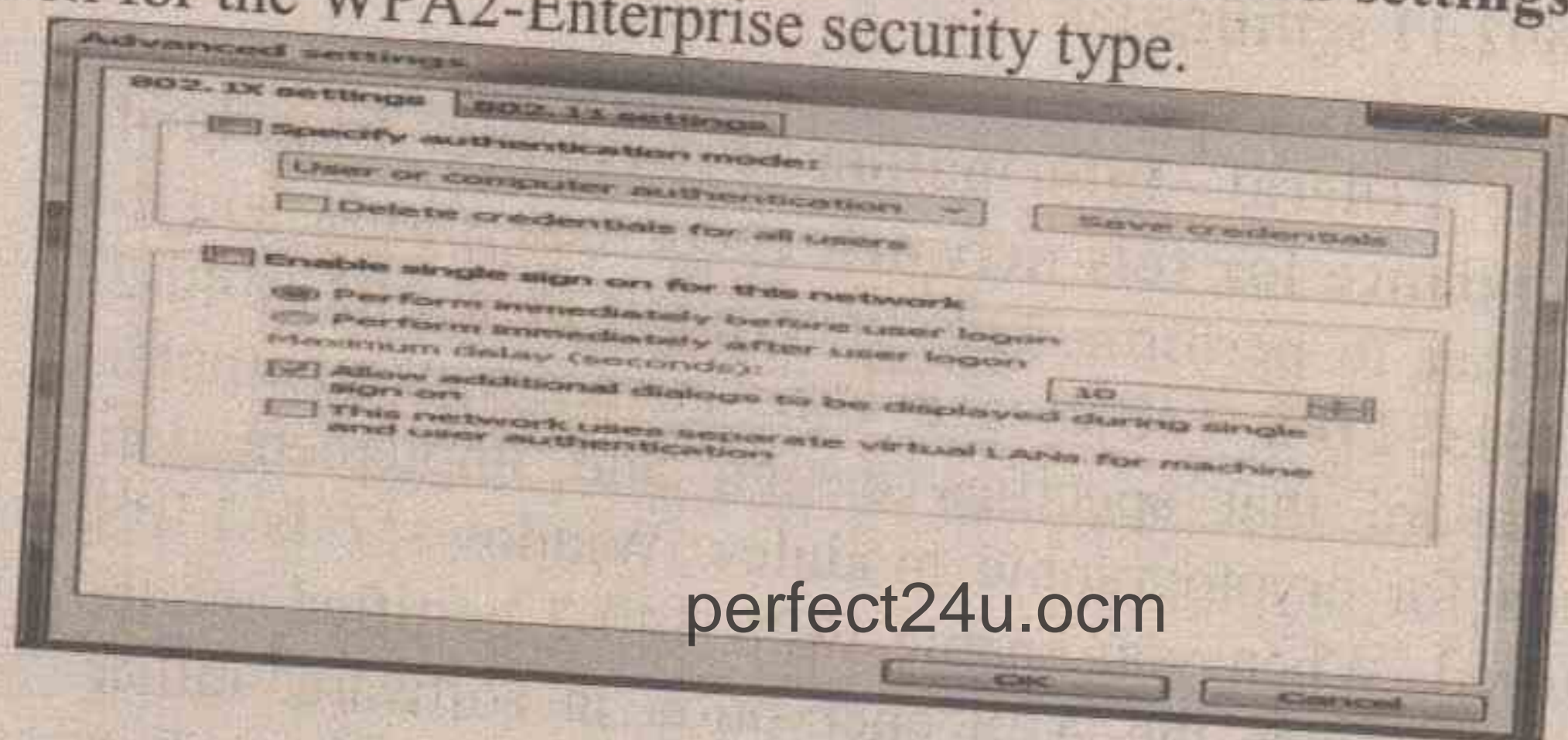
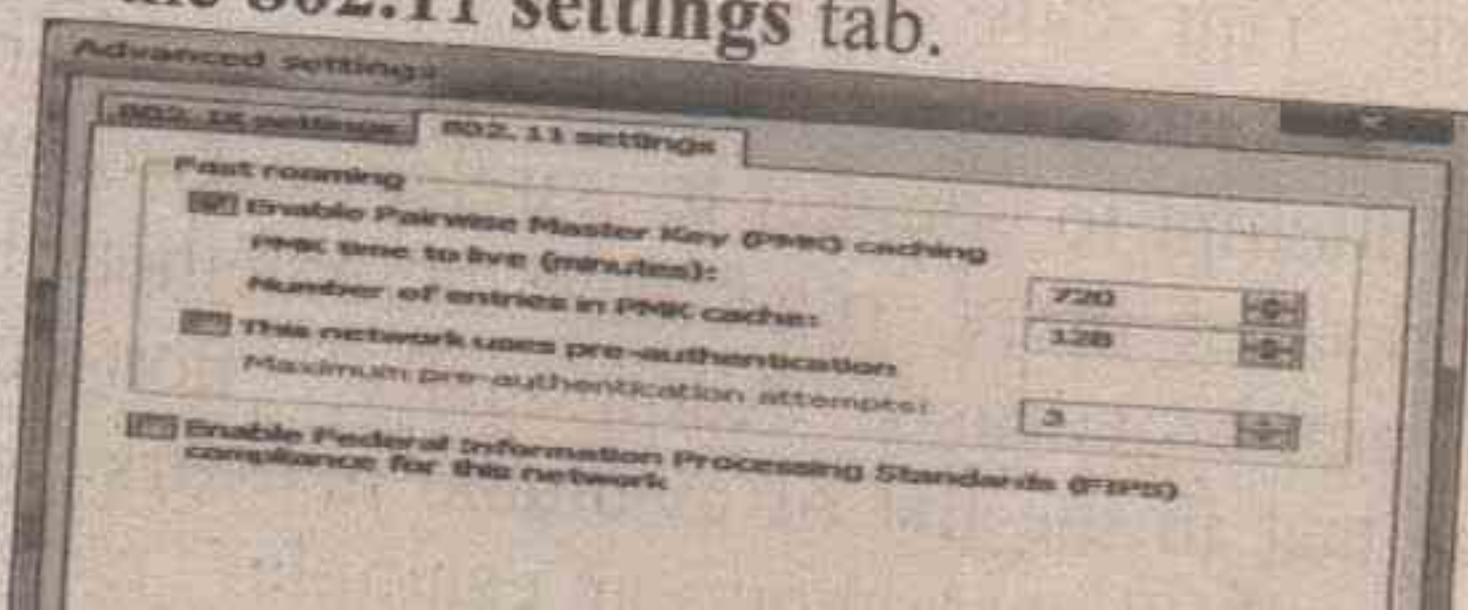


Figure Example of configuring a network security key
 If you choose the WPA-Enterprise, WPA2-Enterprise, or WPA2-Personal security types, you can also configure advanced settings. Figure shows the **Advanced settings** dialog box for the WPA2-Enterprise security type.



perfect24u.ocm

On the **802.1X settings** tab, you can specify the authentication mode (User or computer authentication, Computer authentication, User authentication, or Guest authentication), save a set credentials for user authentication, and delete credentials for all users. Single sign-on (SSO) allows you to configure when 802.1X authentication occurs relative to the user logon and to integrate user logon and 802.1X authentication credentials on the Windows logon screen. Figure shows the **802.11 settings** tab.



In the **Fast roaming** section, you can configure Pair wise Master Key (PMK) caching and pre-authentication options.

- **Note** When you select the **WPA-Enterprise** security type, the **Advanced settings** dialog box does not contain the **802.11 settings** tab.

The **Enable Federal Information Processing Standard (FIPS) compliance for this network** check box allows you to specify whether to perform AES encryption in a FIPS 140-2 certified mode. FIPS 140-2 is a U.S. government computer security standard that specifies design and implementation requirements for cryptographic modules. Windows 7 is FIPS 140-2 certified. When you enable FIPS 140-2 certified mode, Windows 7 performs the AES encryption in software, rather than relying on the wireless network adapter. This check box only appears when you select WPA2-Enterprise or WPA2-Personal as the authentication method on the **Security** tab.

Non-broadcasting wireless networks

A non-broadcasting wireless network does not advertise its network name, also known as its SSID. A wireless access point of a non-broadcasting wireless network can be configured to send Beacon frames with an SSID set to NULL. A non-broadcasting wireless network is also known as a hidden wireless network. You can configure wireless networks in Windows 7 as broadcast or non-broadcast. A computer running Windows 7 will attempt to connect to wireless networks in the preferred networks list order, regardless of whether they are broadcast or non-broadcast. Additionally, non-broadcast networks appear last in the list of available networks with the name **Other Network**. Figure shows an example.

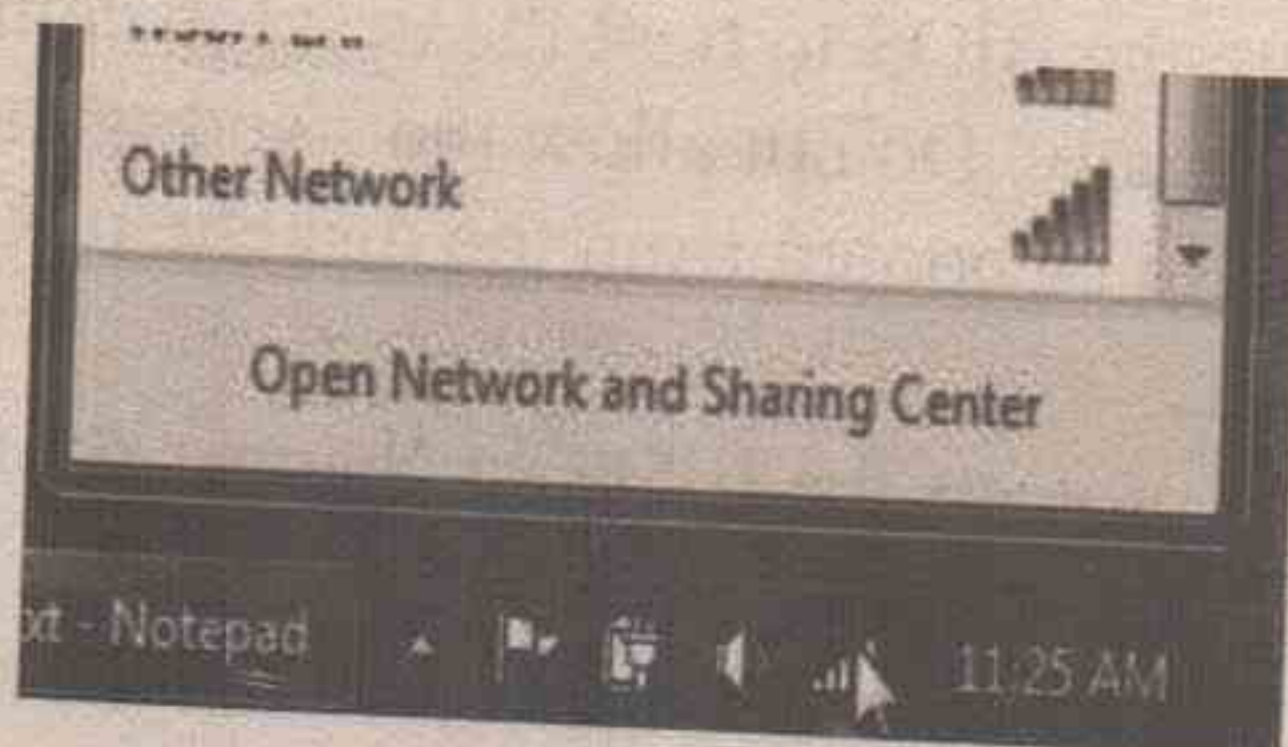


Figure Example of a non-broadcast wireless network

When you connect to the **Other Network**, Windows 7 prompts you to specify the wireless network name (SSID). Figure 14 shows an example.



Figure Typing the name of a non-broadcast wireless network

SECURE WINDOWS 7 CLIENT DESKTOP COMPUTER

A stand-alone desktop computer is one that is in no way connected to another computer or networked device, such as a switch, hub, or router (with the possible exception of a printer), or to the Internet or a local area network (LAN). The stand-alone desktop computer can be running Windows 7/8 client or server, Linux, or Mac OS X. Because the stand-alone desktop computer is not connected to the Internet or a local or wide area network, the emphasis for securing the data is placed on physical security of the computer and controlling access to the data.

Physical Security of a Stand-Alone Computer

1. Configure the BIOS to boot the desktop computer from the hard drive only. Do not allow the stand-alone desktop computer to be booted from the diskette or CD-ROM drive.
2. Password protects the BIOS so changes cannot be made to the BIOS without authorization.
3. Secure the desktop computer on which the Add Health data resides in a locked room, or secure the desktop computer to a table with a lock and cable (locking the case so the battery cannot be disconnected, which would disable the BIOS password).
4. Remove or disable the network interface card (NIC) so it cannot be used.
5. Store the data on a desktop computer only. Laptops may not be used to store the Add Health data.

Controlling Access to the Data

1. Restrict access to the Add Health data to project personnel using the security features available via the operating system (e.g., login via userid/password and NTFS permissions in Windows 7/8, ACLs in Linux and OS X).
2. Require strong passwords.
 - You can run L0phtcrack to look for bad passwords.
 - You can enable password complexity.
3. Password protect screen saver and activate after three minutes of inactivity.
4. Enable whole disk encryption (e.g., *Bitlocker*, *PGP Whole Disk Encryption*, *FileVault2*, *Veracrypt*) or directory-based encryption (e.g., *Windows Encrypting File System* or *Veracrypt*) for directories containing secure data.

5. Configure your analysis software to point temporary work files to the encrypted Add Health data directory.
6. Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. (*Heidi is free and works well* .SDELETE also works well and can be scripted.)
7. Do not copy or move the Add Health data out of the secured directory for any reason.

Optimize and maintain the performance and reliability of windows-7 client computer

1. Automatically Optimize and Maintain Windows 7

Microsoft has created a pair of built-in automated troubleshooting packs to optimize and maintain Windows 7 performance.

Dell Recommended: To ~~attempt to fix~~ this problem automatically, click the **Fix it** link below. Then, click **Run** in the **File Download** dialog box and follow the steps in the wizard.

Or follow the steps below to run the troubleshooters built into your computer:

1. Open the Performance troubleshooter by clicking the **Start** button , and then clicking **Control Panel** .
2. In the search box, type **troubleshooter**, and then click **Troubleshooting** .
3. Click **View All** and then click the checkbox to show online troubleshooters.

2. Basic Maintenance of Windows 7

There are a few key housekeeping tasks that should be routinely performed on a computer to keep it running smoothly

- **Run Windows Update** - Make sure that all key operating system updates are installed. Visit Microsoft KB article "Updating Your Computer" to learn more.
- **Defragment Your Hard Drive.** Files on your hard drive can sometimes become spread out, or fragmented, across different sectors of the drive. Defragmenting the hard drive aligns the pieces of those files in one sector, which increases the efficiency of the operating system to open the files. To learn more, see Microsoft KB article:
- "Improve performance by defragmenting your hard disk"
- **Update the Drivers on the Computer.** Old drivers may cause certain applications to not run correctly, or may have bugs that have been fixed in later releases. Drivers should be checked for updates at least twice a year. Click the button below to visit the Dell Drivers and Downloads website to update your drivers!

CONFIGURE REMOTE DESKTOP ACCESS ON WINDOWS 7 SYSTEMS

Remote Desktop is not enabled by default. You must specifically enable it to allow remote access to the workstation. When it is enabled, any member of the Administrators group can connect to the workstation. Other users must be placed on a remote access list to gain access to the workstation. To configure remote access, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box to the Remote tab.
3. To disable Remote Desktop, select Don't Allow Connections

to This Computer, and then click OK. Skip the remaining steps.

4. To enable Remote Desktop, you have two options. You can:

- Select Allow Connections from Computers Running Any Version of Remote Desktop to allow connections from any version of Windows.
- Select Allow Connections Only from Computers Running Remote Desktop with Network Level Authentication to allow connections only from Windows 7 or later computers (and computers with secure network authentication).

5. Click Select Users. This displays the Remote Desktop Users dialog box.

6. To grant Remote Desktop access to a user, click Add. This opens the Select Users dialog box. In the Select Users dialog box, click Locations to select the computer or domain in which the users you want to work with are located. Type the name of a user you want to work with in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.

7. To revoke remote access permissions for a user account, select the account and then click Remove.

8. Click OK twice when you have finished. Windows Firewall must be configured to allow inbound Remote Desktop exceptions. You can configure this on a per-computer basis in Windows Firewall for the domain profile and the standard profile.

STEP BY STEP INSTALLATION OF WINDOWS SERVER 2008

To use Windows Server 2008 you need to meet the following hardware requirements:

Component Requirement

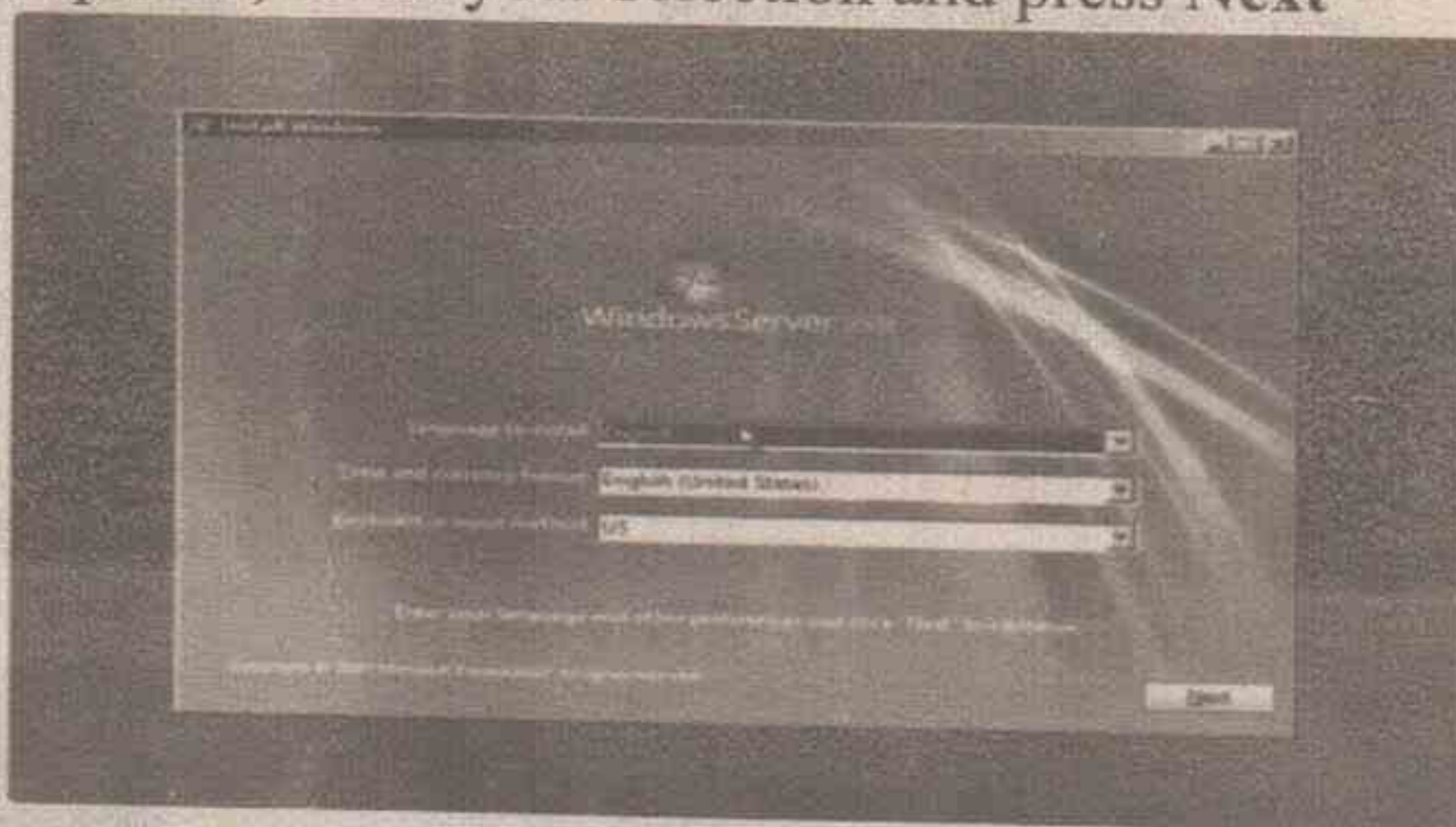
Processor	<ul style="list-style-type: none"> • Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor) • Recommended: 2GHz or faster <p>Note: An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-based Systems</p>
Memory	<ul style="list-style-type: none"> • Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum (32-bit systems): 4GB (Standard) or 64GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32GB (Standard) or 2TB (Enterprise, Datacenter and Itanium-based Systems)
Available Disk Space	<ul style="list-style-type: none"> • Minimum: 10GB • Recommended: 40GB or greater <p>Note: Computers with more than 16GB of RAM will require more space for paging, hibernation, and dump files</p>
Drive	DVD-ROM drive
Display	and • Super VGA (800 x 600) or higher-resolution monitor
Peripherals	<ul style="list-style-type: none"> • Keyboard • Microsoft Mouse or compatible pointing device

Follow this procedure to install Windows Server 2008:

1. Insert the appropriate **Windows Server 2008 installation media** into your DVD drive. If you don't have an installation DVD for Windows Server 2008,
2. **Reboot** the computer



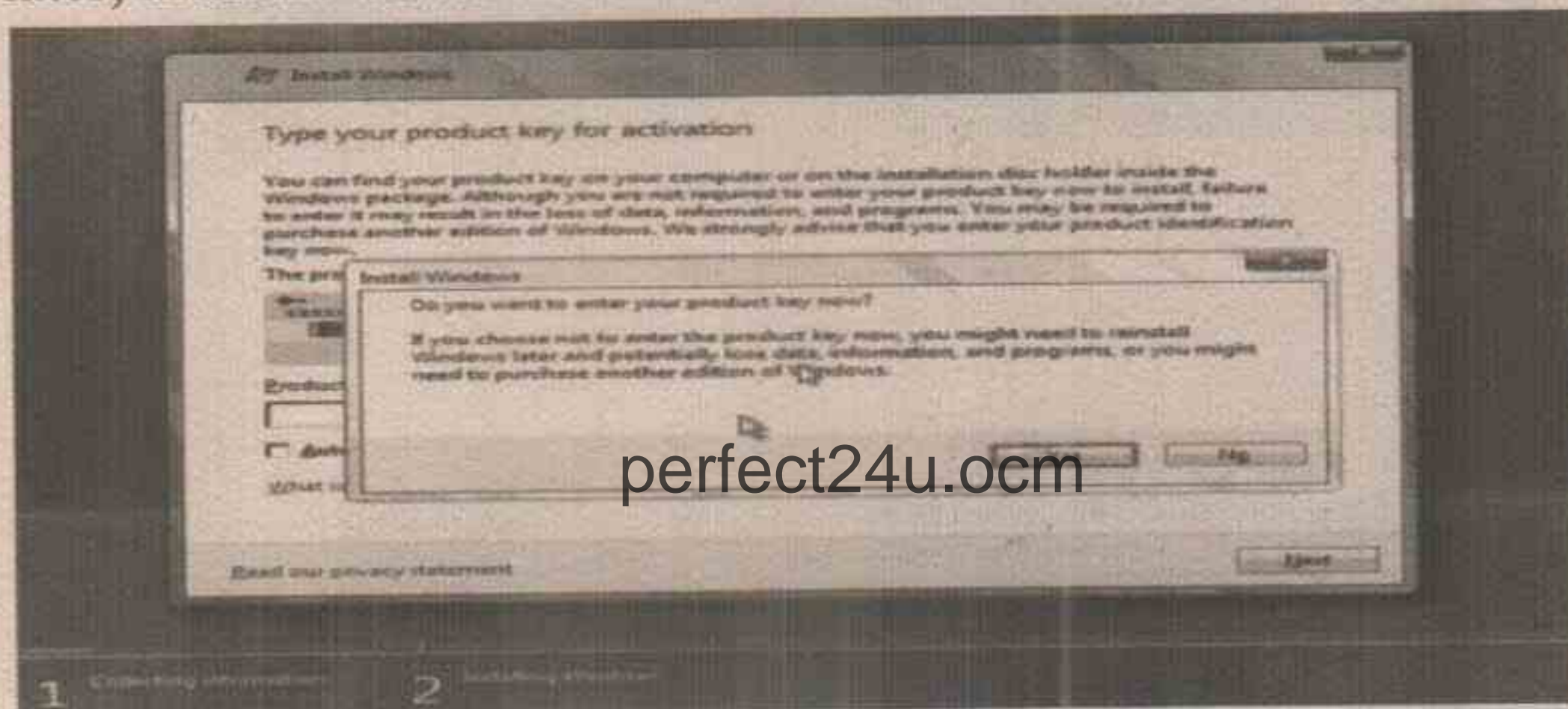
When prompted for an **installation language** and other regional options, make your selection and press **Next**



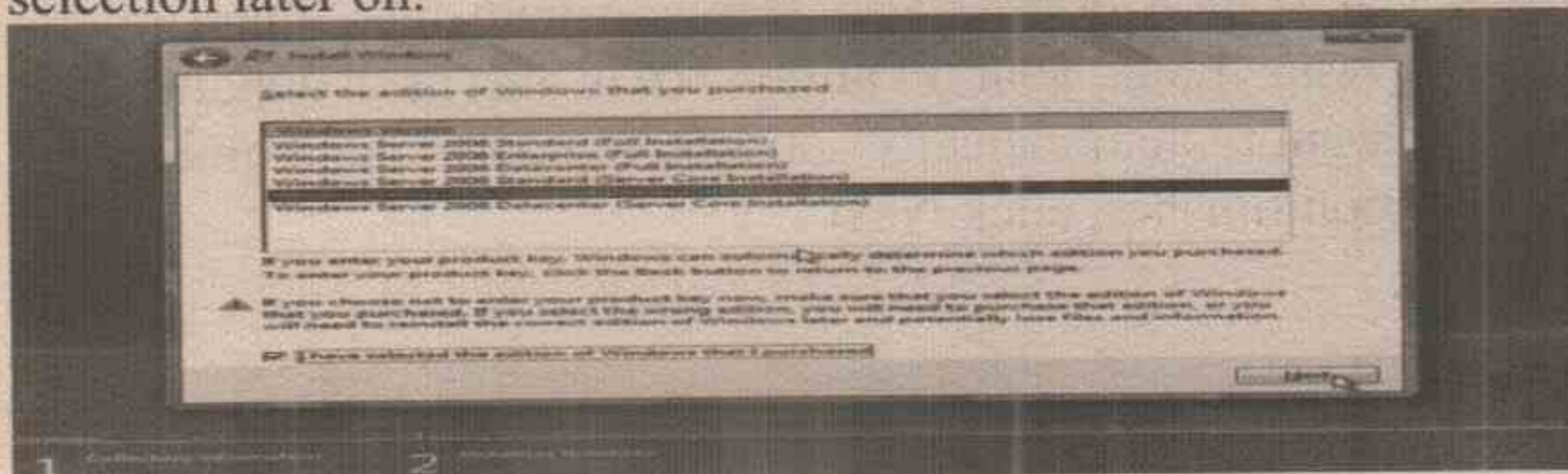
5. Product activation is now also identical with that found in Windows Vista. Enter your **Product ID** in the next window, and if you want to automatically activate Windows the moment the installation finishes, click **Next**.



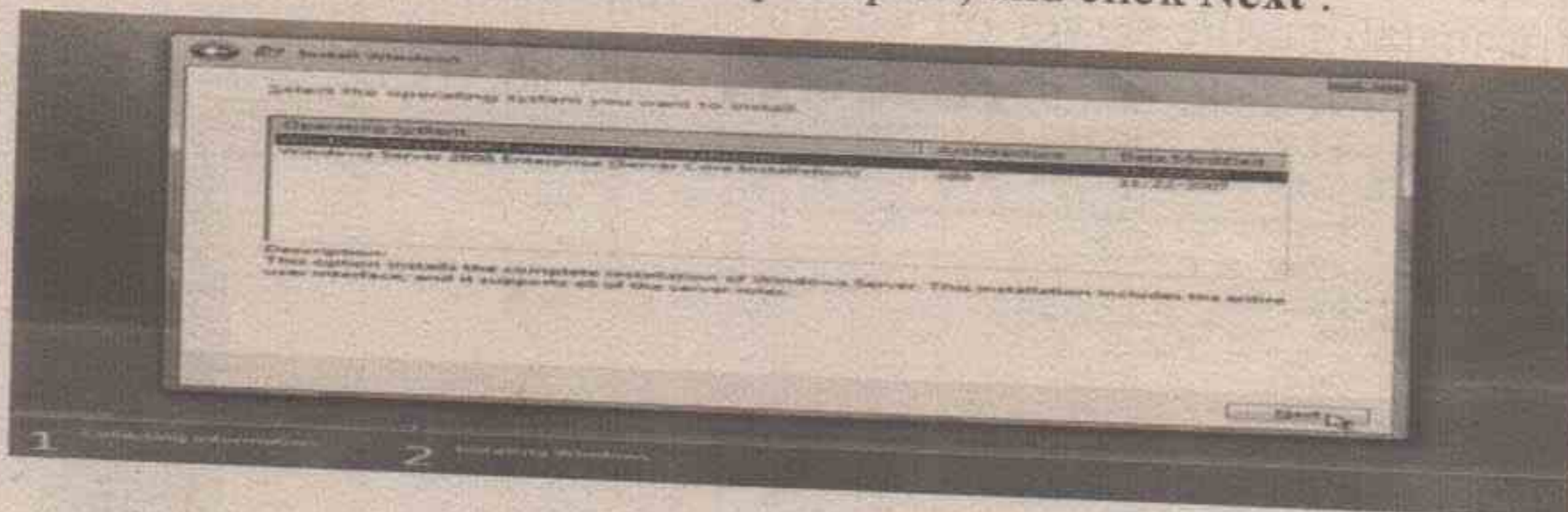
If you do not have the Product ID available right now, you can leave the box empty, and click Next. You will need to provide the Product ID later, after the server installation is over. Press No.



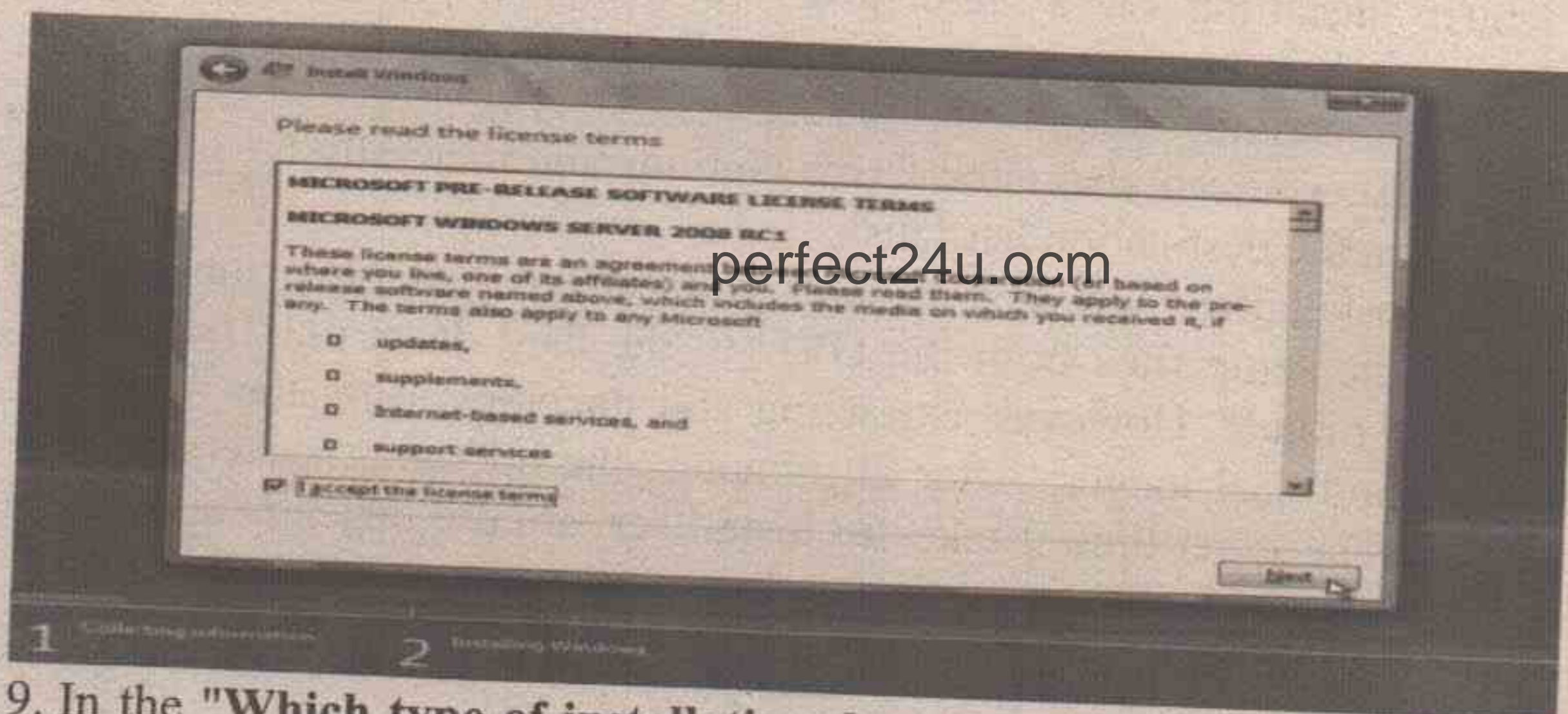
Because you did not provide the correct ID, the installation process cannot determine what kind of Windows Server 2008 license you own, and therefore you will be prompted to **select your correct version** in the next screen, assuming you are telling the truth and will provide the correct ID to prove your selection later on.



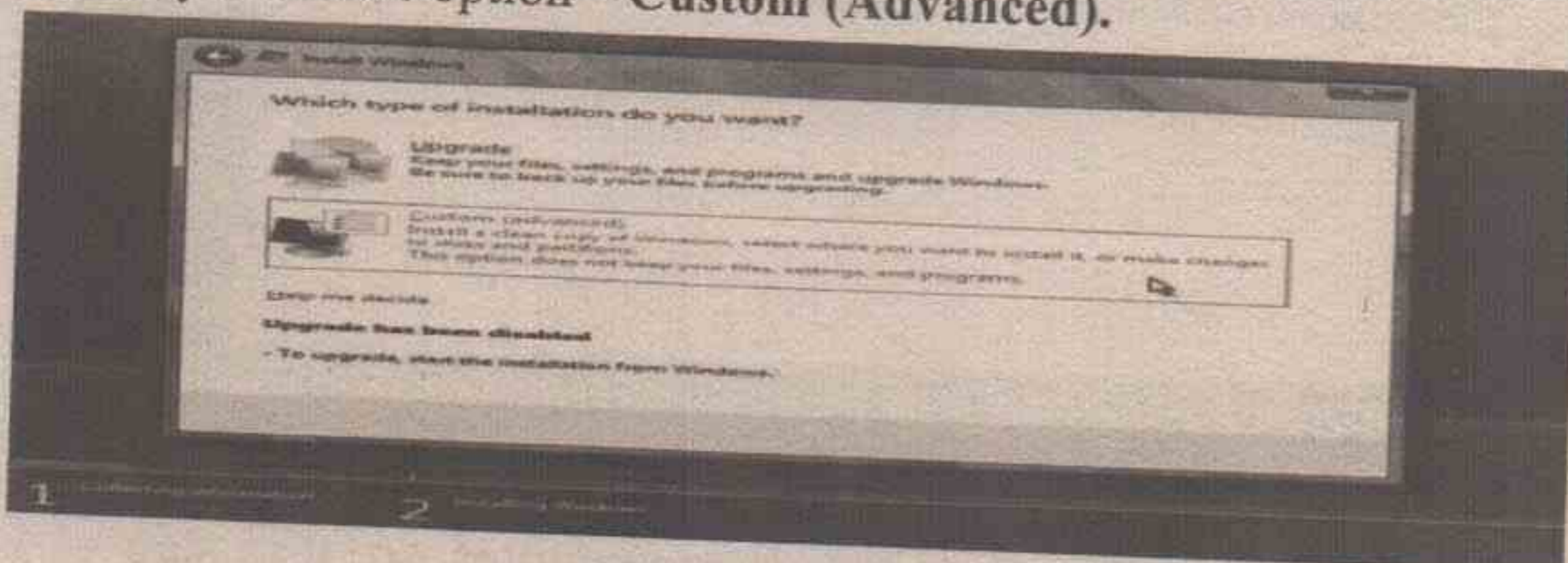
7. If you did provide the right Product ID, select the **Full version** of the right Windows version you're prompted, and click **Next**.



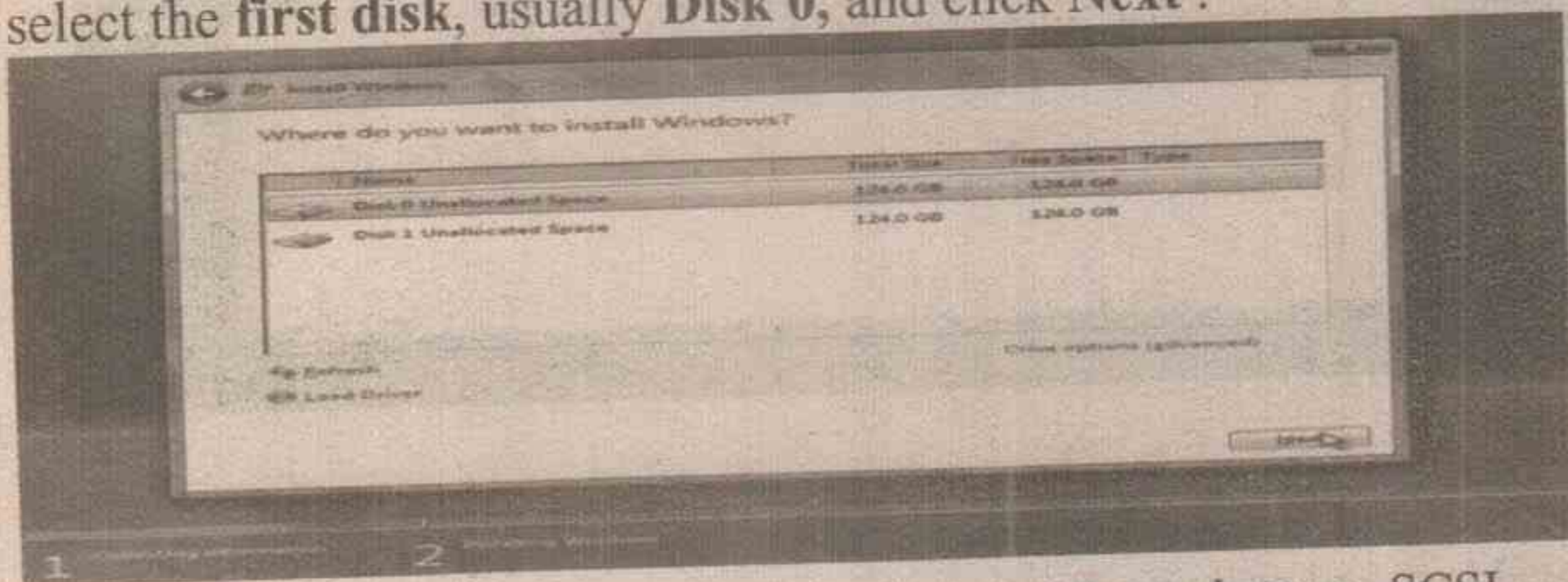
8. Read and accept the license terms by clicking to select the **checkbox** and pressing **Next**.



9. In the "Which type of installation do you want?" window, click the only available option – **Custom (Advanced)**.



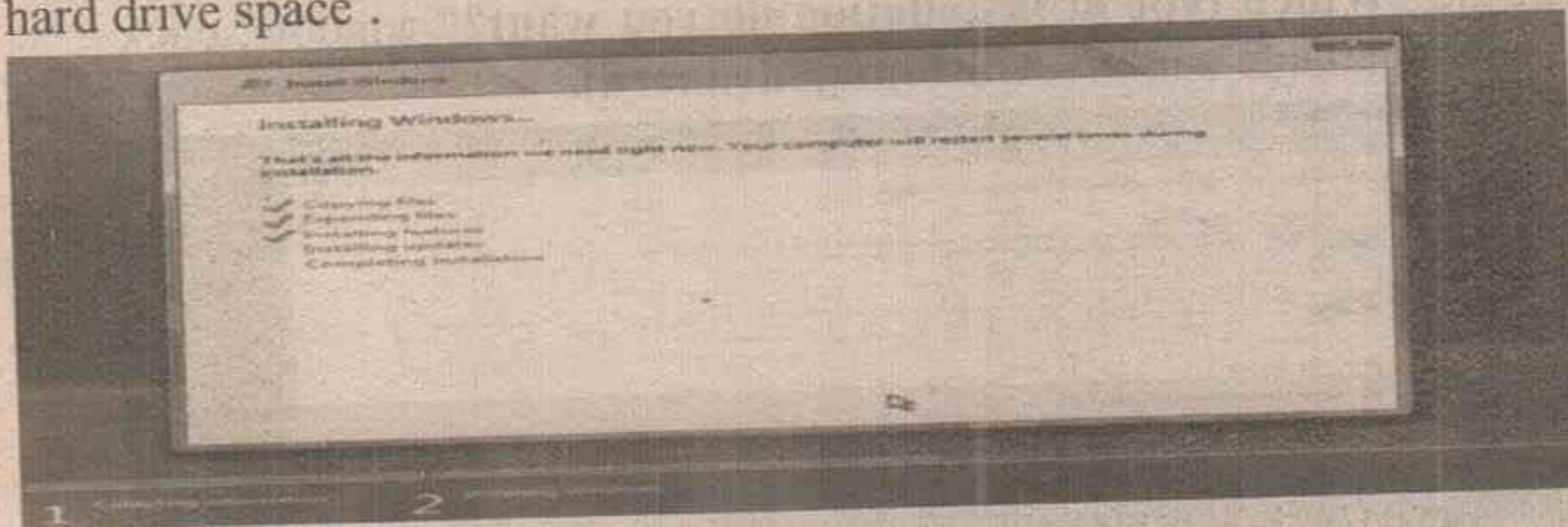
10. In the "Where do you want to install Windows?", if you're installing the server on a regular IDE hard disk, click to select the **first disk**, usually **Disk 0**, and click **Next**.



If you're installing on a hard disk that's connected to a SCSI controller, click **Load Driver** and insert the media provided by the controller's manufacturer.

If you must, you can also click **Drive Options** and manually create a partition on the destination hard disk.

11. The installation now begins, and you can go and have lunch. Copying the setup files from the DVD to the hard drive only takes about one minute. However, extracting and uncompressing the files takes a good deal longer. After 20 minutes, the operating system is installed. The exact time it takes to install server core depends upon your hardware specifications. Faster disks will perform much faster installs... Windows Server 2008 takes up approximately 10 GB of hard drive space.



The installation process will reboot your computer, so, if in step #10 you inserted a floppy disk (either real or virtual), make sure you remove it before going to lunch, as you'll find the server

hanged without the ability to boot (you can bypass this by configuring the server to boot from a CD/DVD and then from the hard disk in the booting order on the server's BIOS)

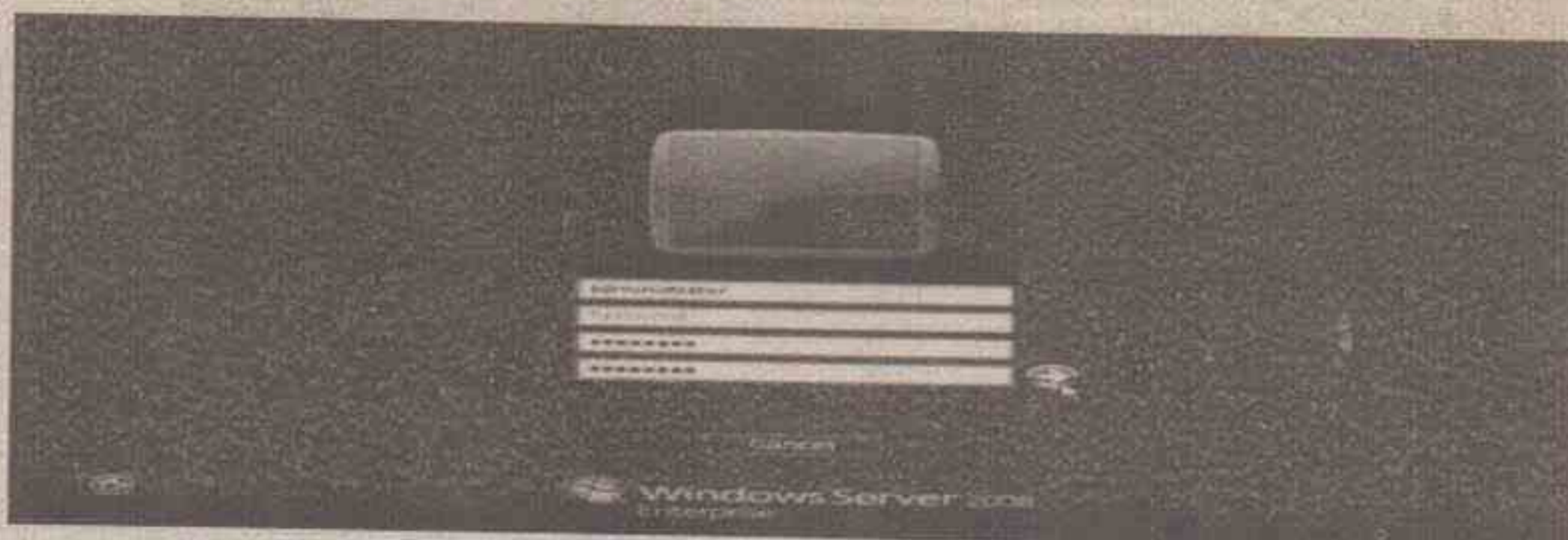
12. Then the server reboots you'll be prompted with the new Windows Server 2008 type of login screen. Press **CTRL+ALT+DEL** to log in.



perfect24u.ocm



14. The default Administrator is blank, so just type Administrator and press Enter .



15. You will be prompted to change the user's password. You have no choice but to press **Ok**.



16. In the password changing dialog box, leave the **default password blank** and enter a new, complex, at-least-7-characters-long new password twice. A password like "topsecret" is not valid (it's not complex), but one like "T0pSecreT!" sure is. Make sure you remember it.



17. Someone thought it would be cool to nag you once more, so now you'll be prompted to accept the fact that the password had been changed. Press **Ok**





18. Finally, the desktop appears and that's it, you're logged on and can begin working. You will be greeted by an assistant for the **initial server configuration**, and after performing some initial configuration tasks, you will be able to start working.

Managing Server Roles and Features

Windows Server® 2008 R2 eases managing and securing multiple server roles in an enterprise with the Server Manager console. Server Manager in Windows Server 2008 R2 provides a single source for managing server identity and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on server.

Add roles or features by using the Windows interface

- In the **Roles Summary** or **Features Summary** areas of the Server Manager main window, click either **Add Roles** or **Add Features**, depending on the software that you want to install.
-- or --

In the **Customize this server** area of the **Initial Configuration Tasks** window, click either **Add Roles** or **Add Features**.

The **Initial Configuration Tasks** window opens by default when a member of the Administrators group logs on to the computer.

Server Manager opens when the **Initial Configuration Tasks** window is closed. You can also open Server Manager by using shortcuts on the **Start** menu, on the Windows taskbar, or in Administrative Tools.

Administrative Tools

Administrative Tools is the collective name for several advanced tools in Windows that are used mainly by system administrators. Administrative Tools is available in Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, and Windows Server operating systems.

The programs available in Administrative Tools can be used to schedule a test of your computer's memory, manage advanced aspects of users and groups, format hard drives, configure Windows services, change how the operating system starts, and much, much more.

Access Administrative Tools

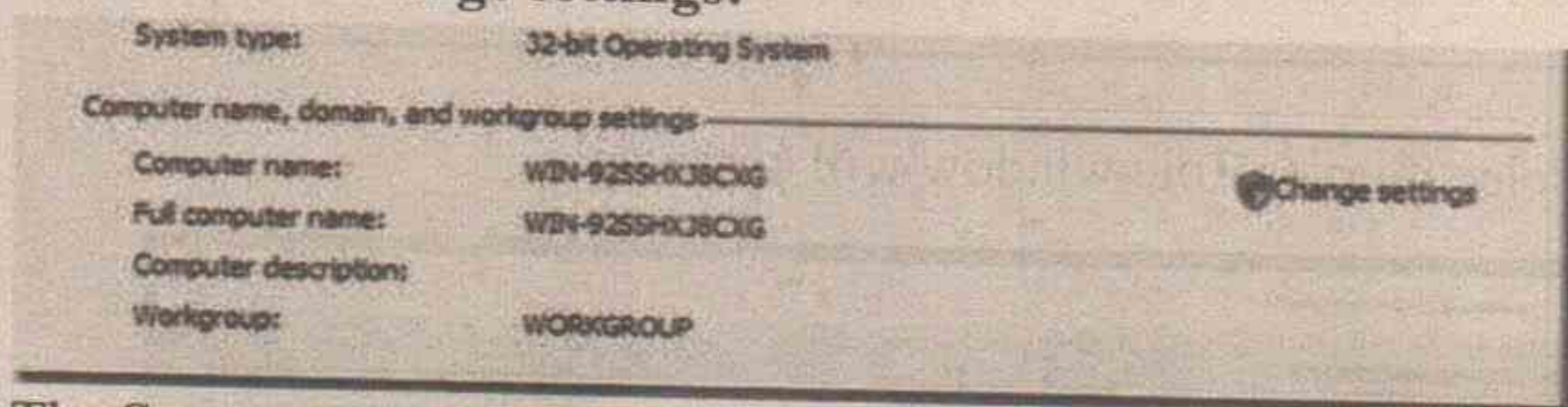
Administrative Tools is a Control Panel applet and so can be accessed via Control Panel. To open Administrative Tools, first, open Control Panel and then tap or click on the Administrative Tools icon.

Overview of Active Directory

Active Directory Domain Services is Microsoft's Directory Server. It provides authentication and authorization mechanisms as well as a framework within which other related services can be deployed (AD Certificate Services, AD Federated Services, etc). It is an LDAP compliant database that contains objects

ACTIVE DIRECTORY INSTALLATION ON WINDOWS SERVER 2008

To start the installation of active directory is to change the name of the computer to reflect the new status. To do that, login to the server and click on the **Start** button and **right-click** on **Computer** and go to **Properties**. At the bottom under **computer name, domain, and workgroup settings**, click on the **Change settings**:



The **System Property** window will come up. Click on the **change tab**, and change the computer name to whatever you want.

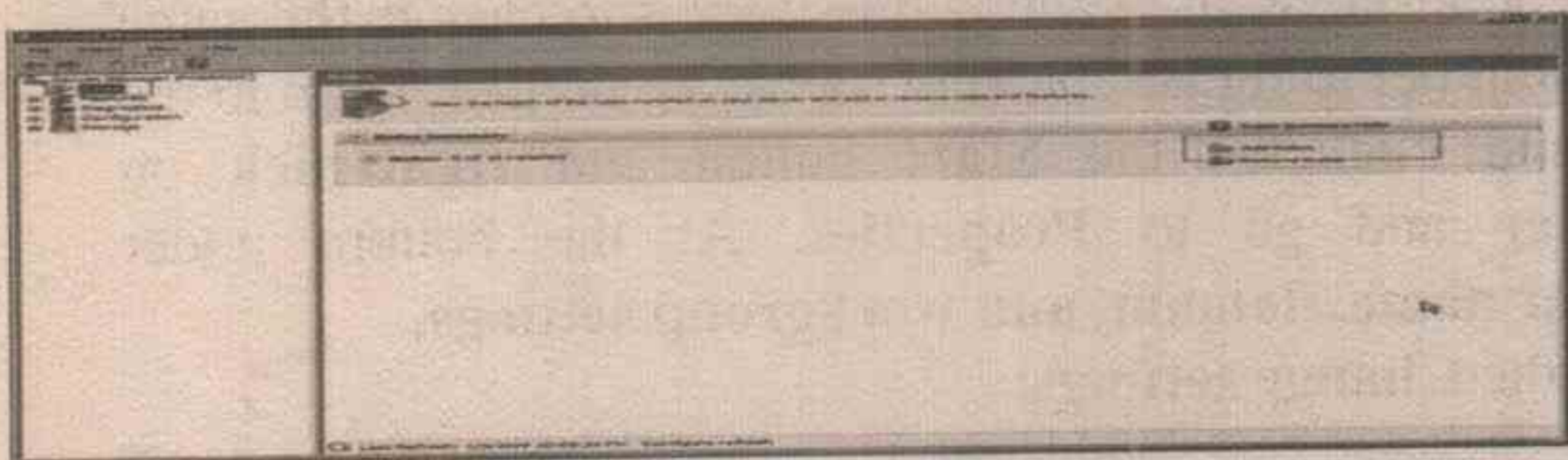


Click on the **OK** button. Windows Server 2008 will now reboot.

Creating/Installing Active Directory Domain Services

Now that we have renamed the computer to something that reflects the new role on windows server 2008, we will proceed with the installation of active directory. To install active directory domain services, go to **Start** and click on **Server Manager**.

The server manager window will come up:



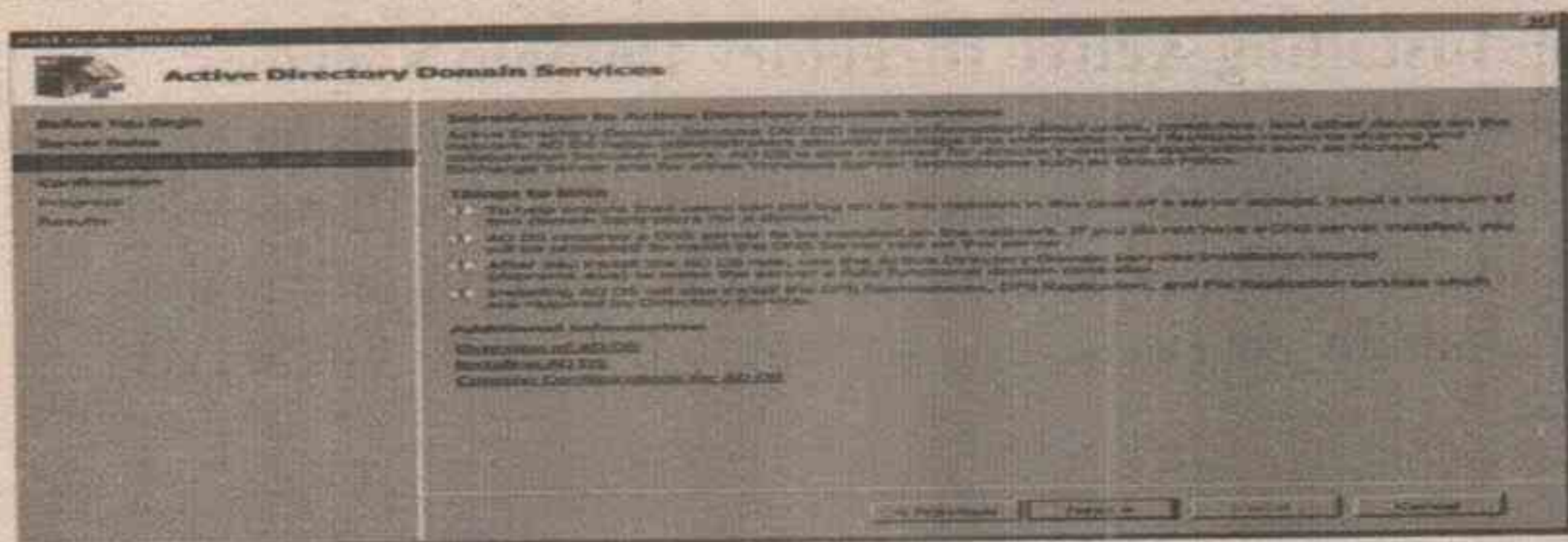
The Select Server Role window will come up:



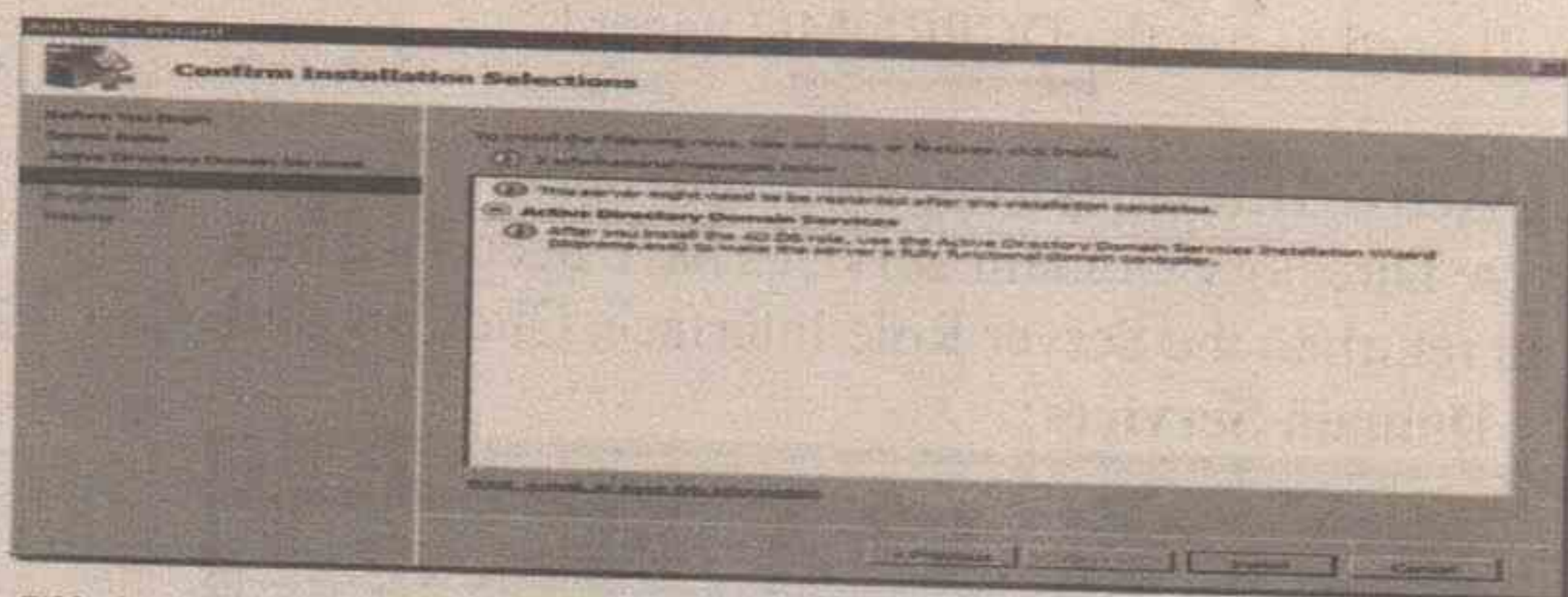
Make sure the Active Directory Domain Services option is checked.

Click on **Next** after checking the option.

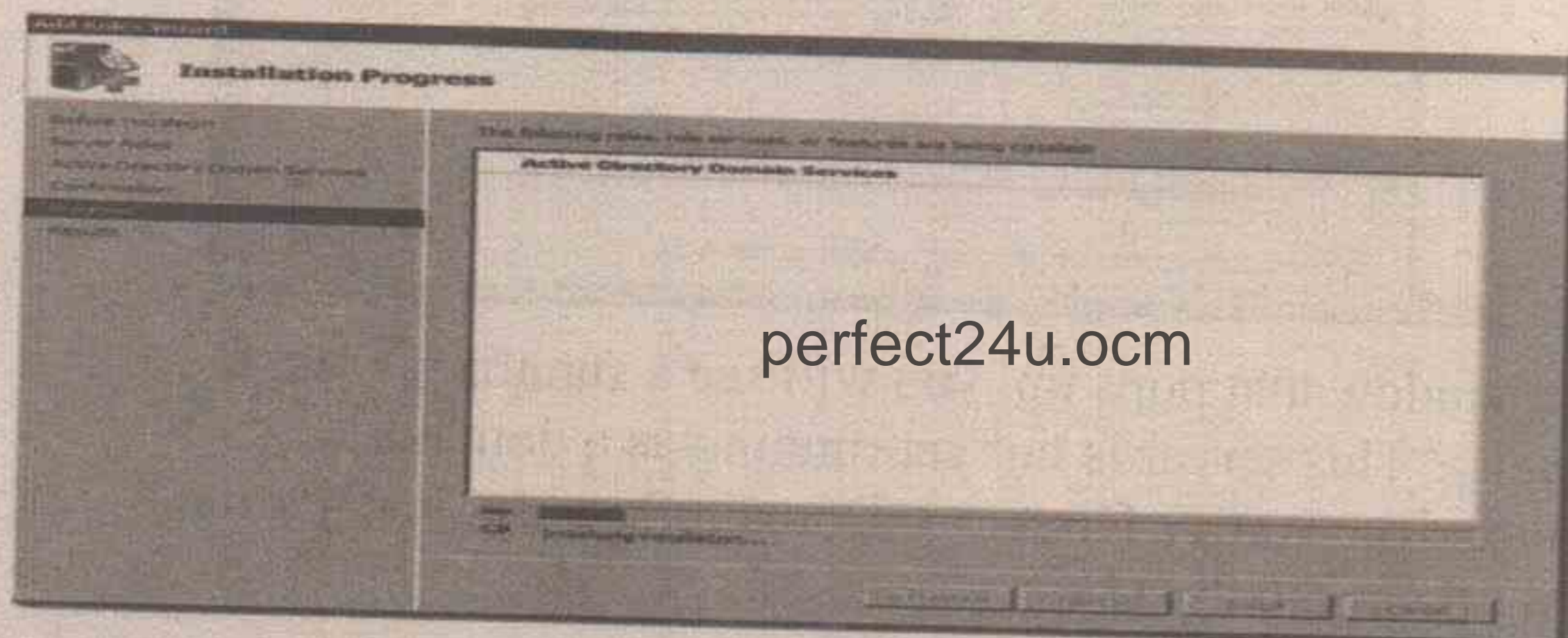
Active directory domain services (AD DS) is something new on Windows Server 2008. On the following window you can read a small introduction about it. Click next when you finish reading.



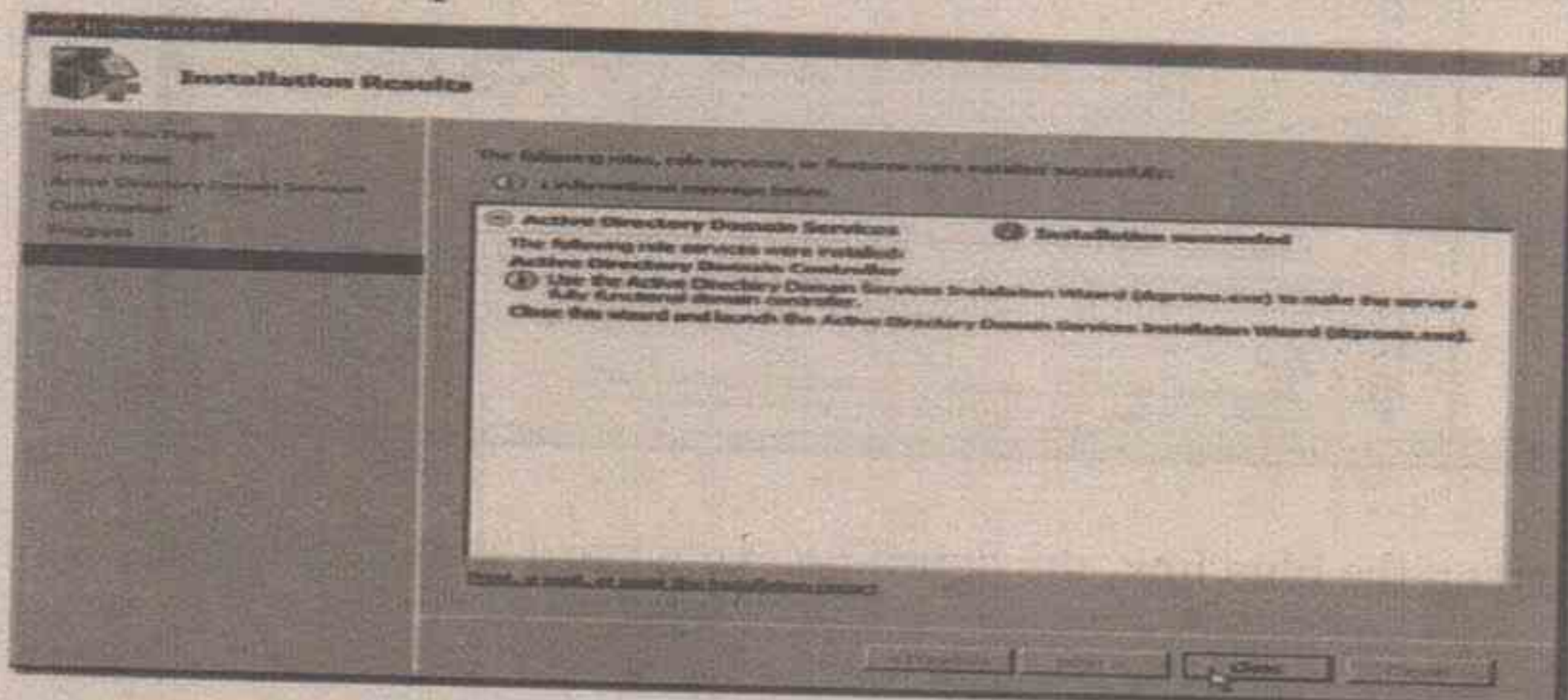
On the following window, you will be asked to confirm the installation of domain services:



Click on Install to start the installation.



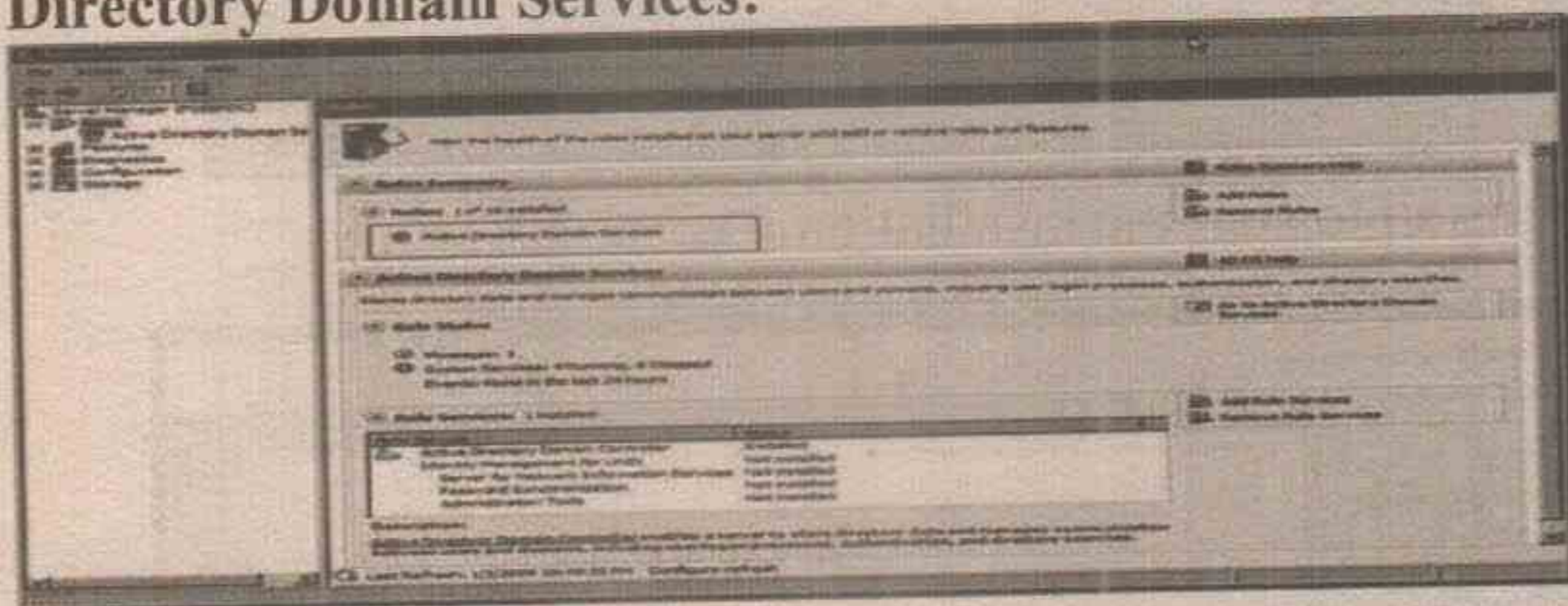
You should receive the Installation Results window after the installation completes.



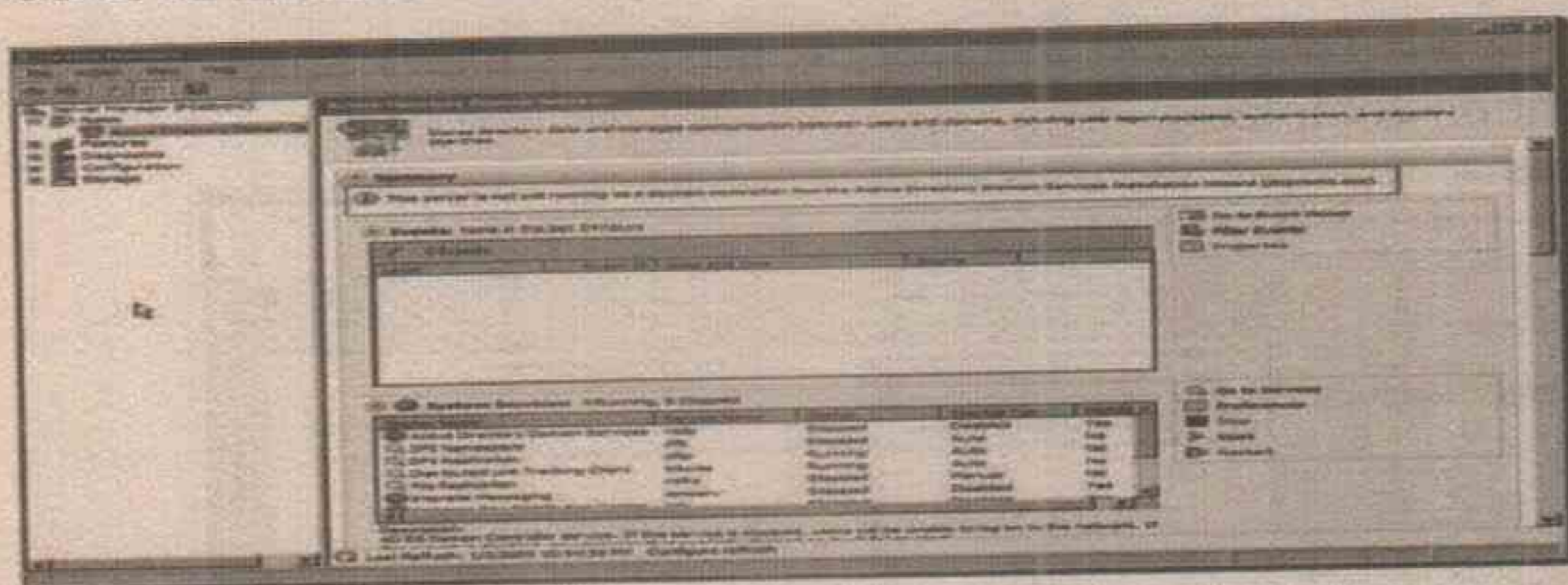
Note: this only installs Active Directory domain services, it does not make Windows server 2008 a domain controller. For that we will need to run the DCPROMO wizard.

Installing Active Directory Domain Controller

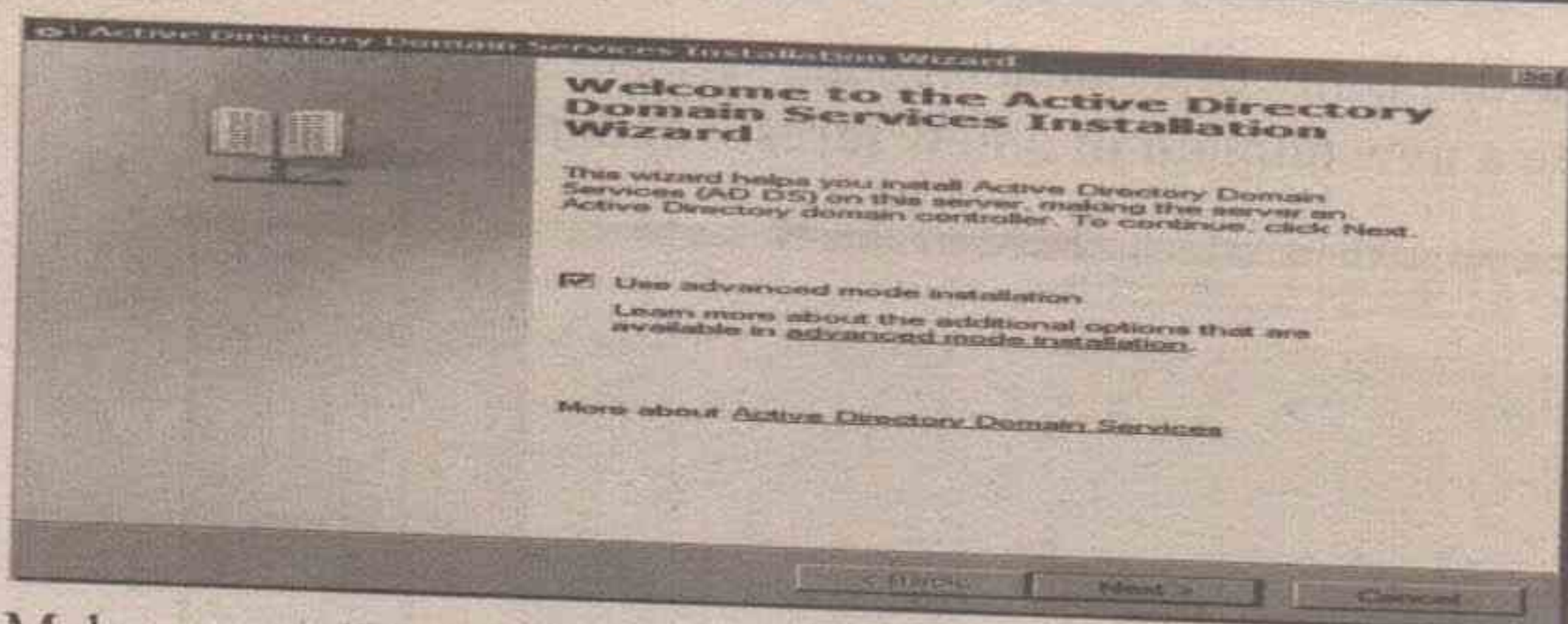
After Active Directory Domain Services have been installed, you should return to the Server Role Interface. Click on **Active Directory Domain Services**:



On the window that pops up, you will see a summary message that reads, "This server is not yet running as a domain controller: Run Active Directory Domain Services Installation Wizard (dcpromo.exe) Click on the blue link.

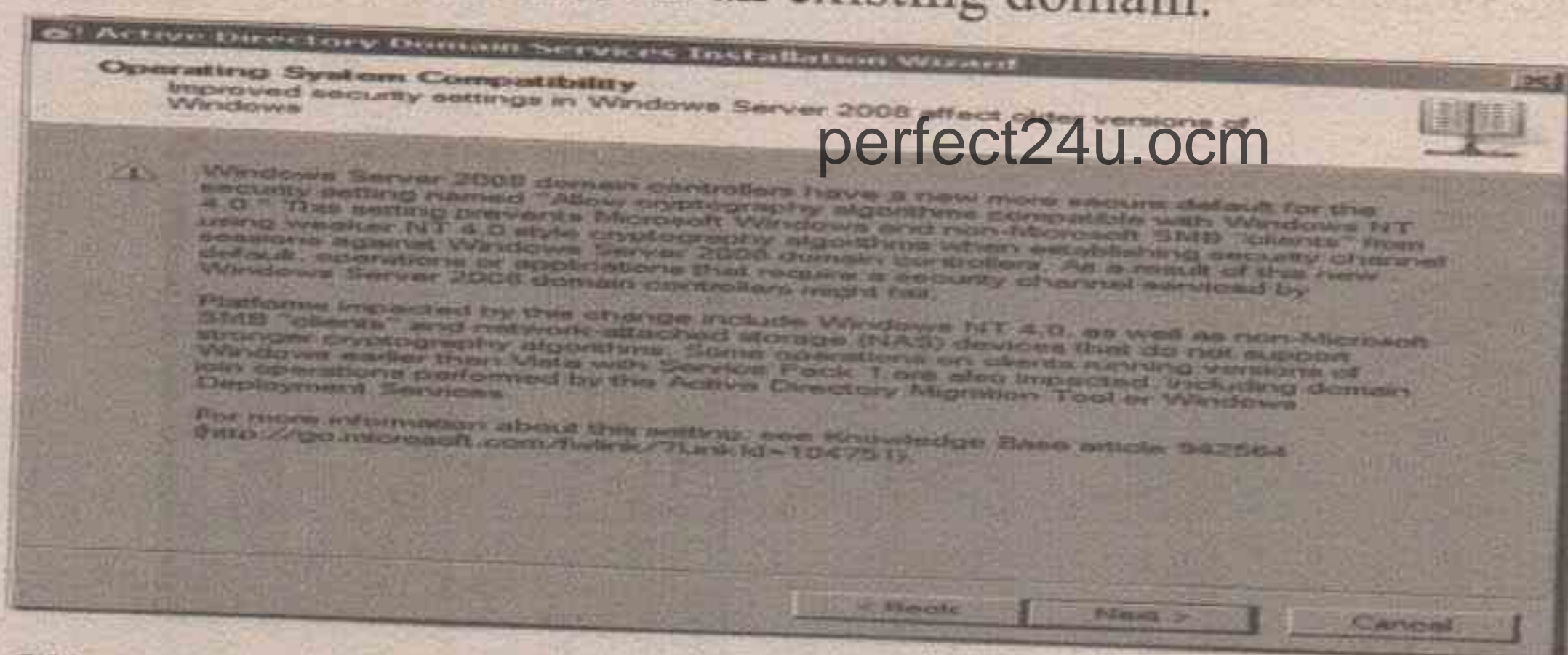


By clicking on the blue link, the dcpromo.exe wizard should come up

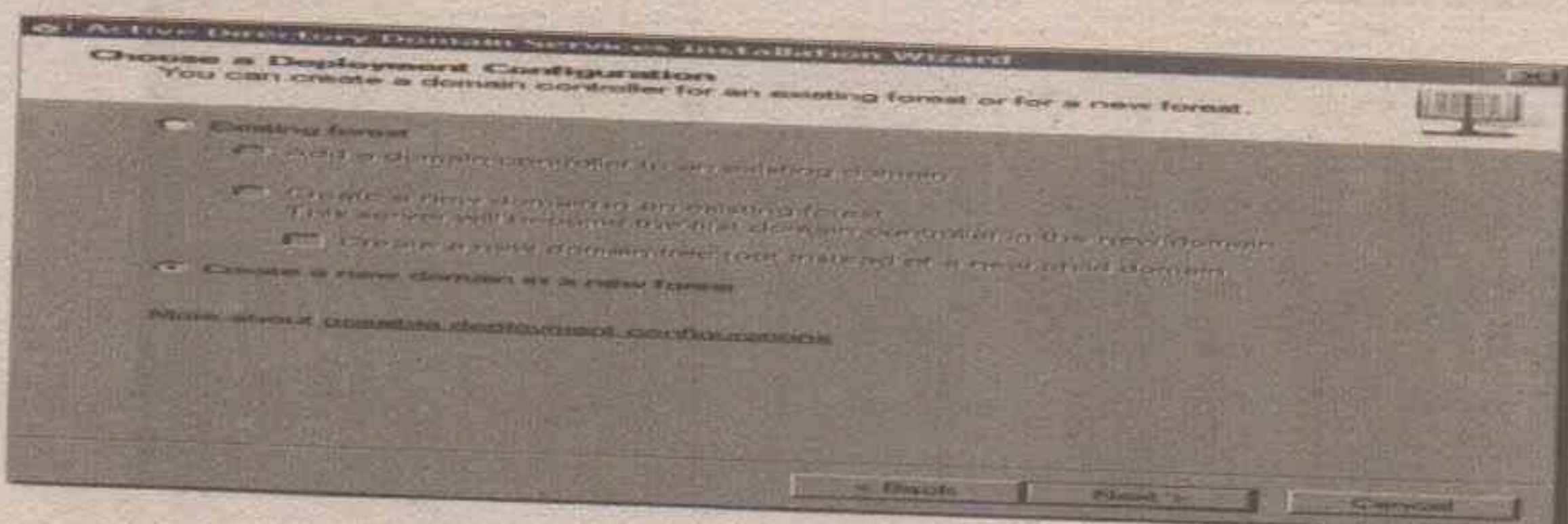


Make sure "Use advanced mode installation" option is checked and click Next .

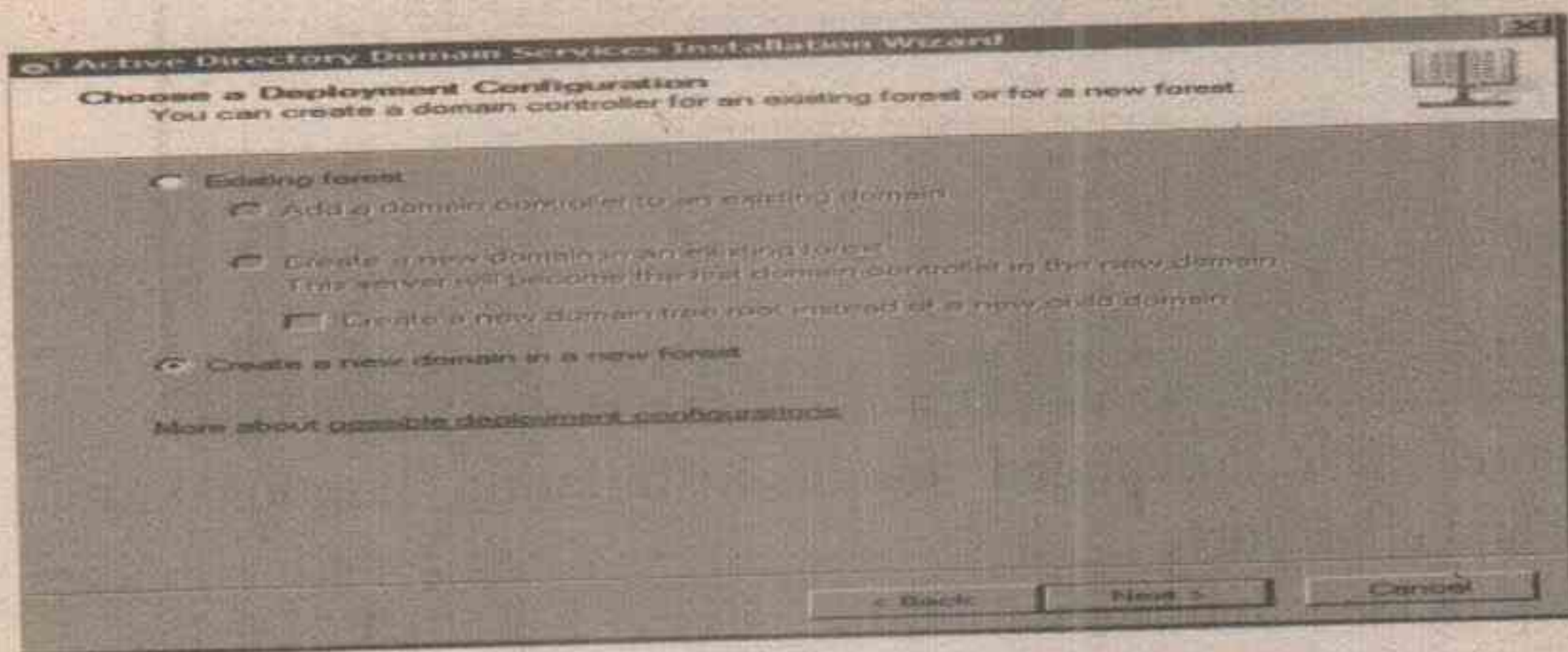
read the provided information on the next screen. that explains some new features on windows server 2008 domain services that might affect older Windows operating systems and non Microsoft SMB clients on an existing domain.



Click Next after you read the above warning.
On the following screen, choose your deployment configuration.



Because this is my first domain controller, I will choose the “Create a new domain in a new forest” option.



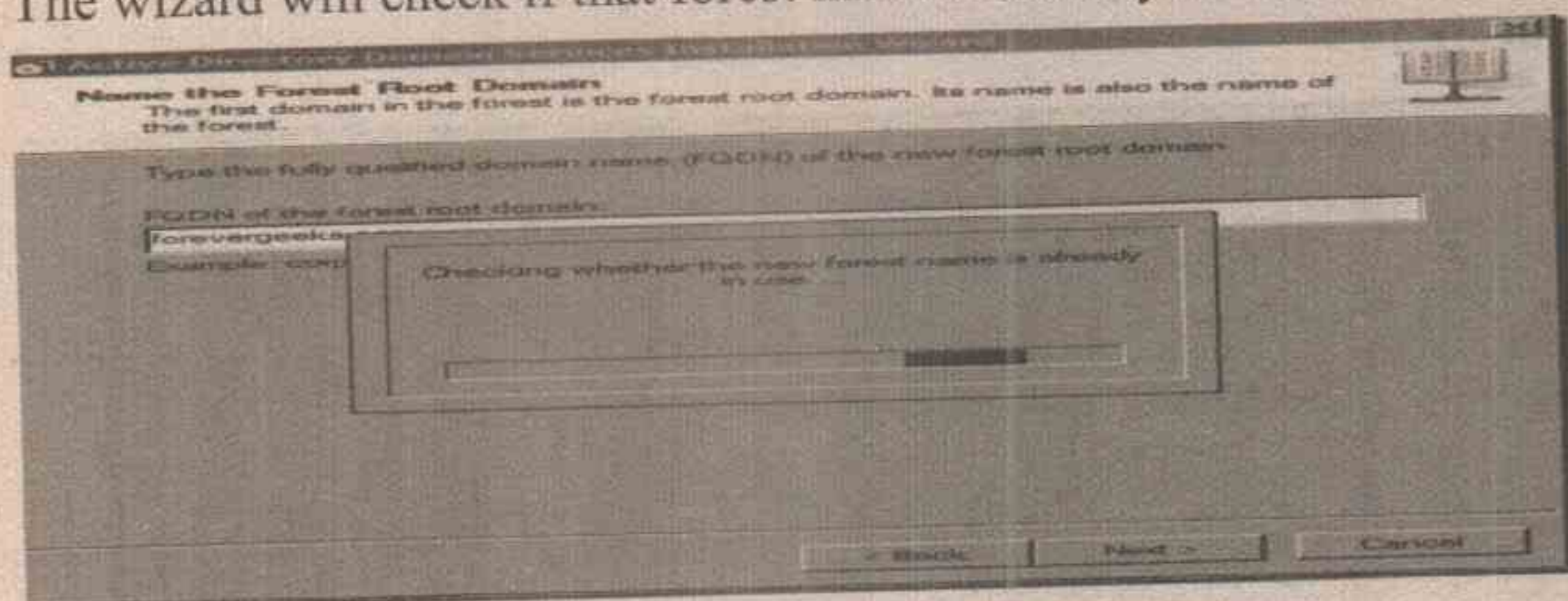
click on Next .

Choose the name for your forest root domain on the following window.

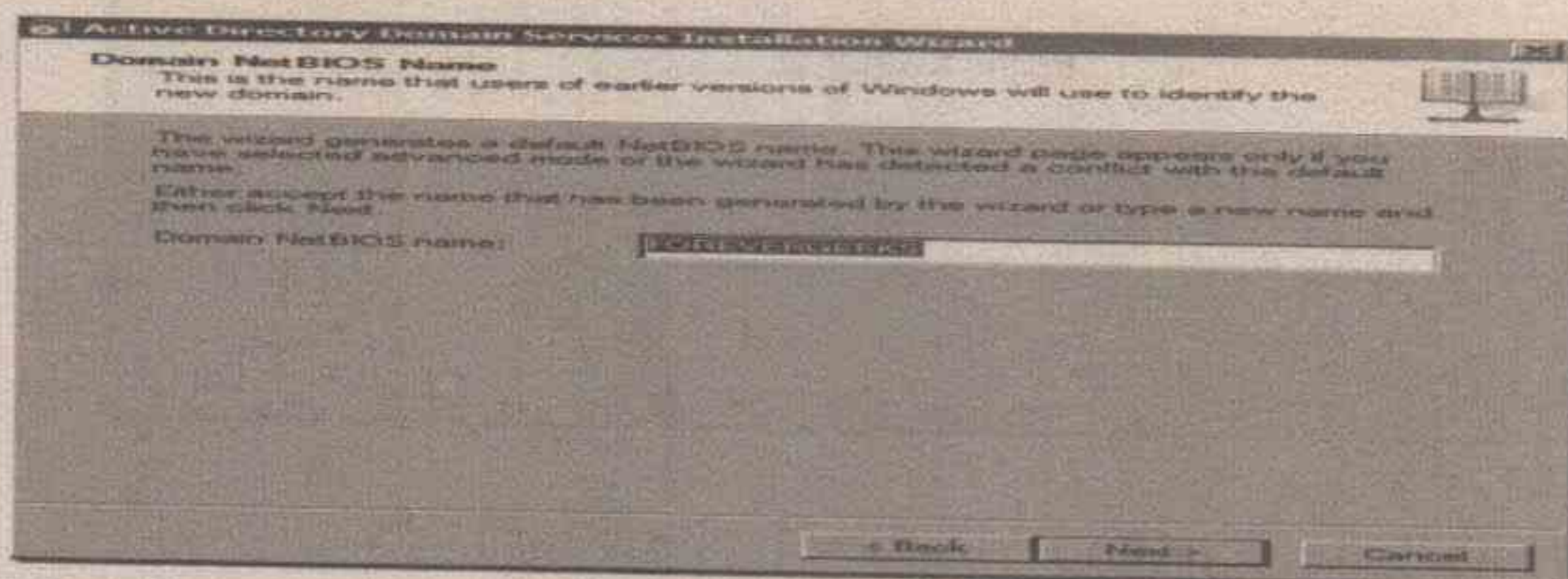
perfect24u.ocm



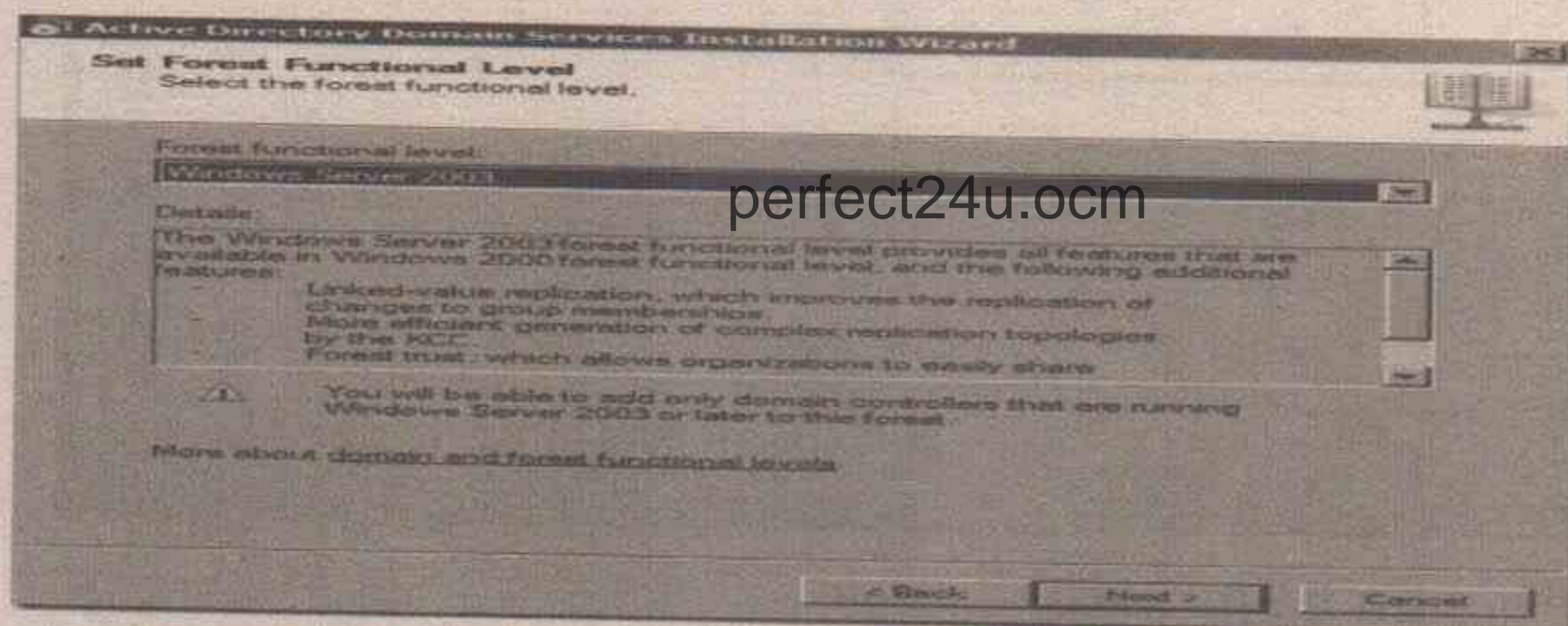
click Next after choosing your fully qualified domain name.
The wizard will check if that forest name is already in used:



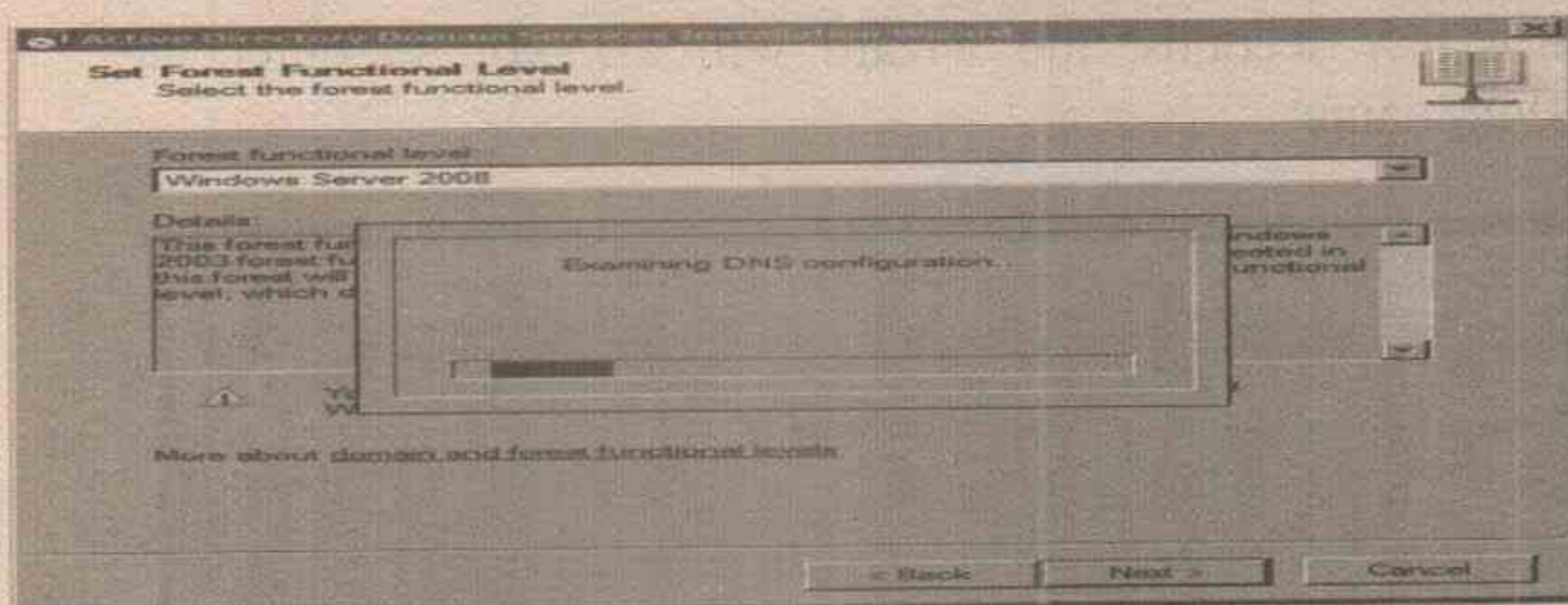
After a few seconds, the wizard will ask you to enter the NetBIOS name:



The default **NetBIOS** name should be fine. Click on the Next tab, on the following screen, choose the **forest functional level** :

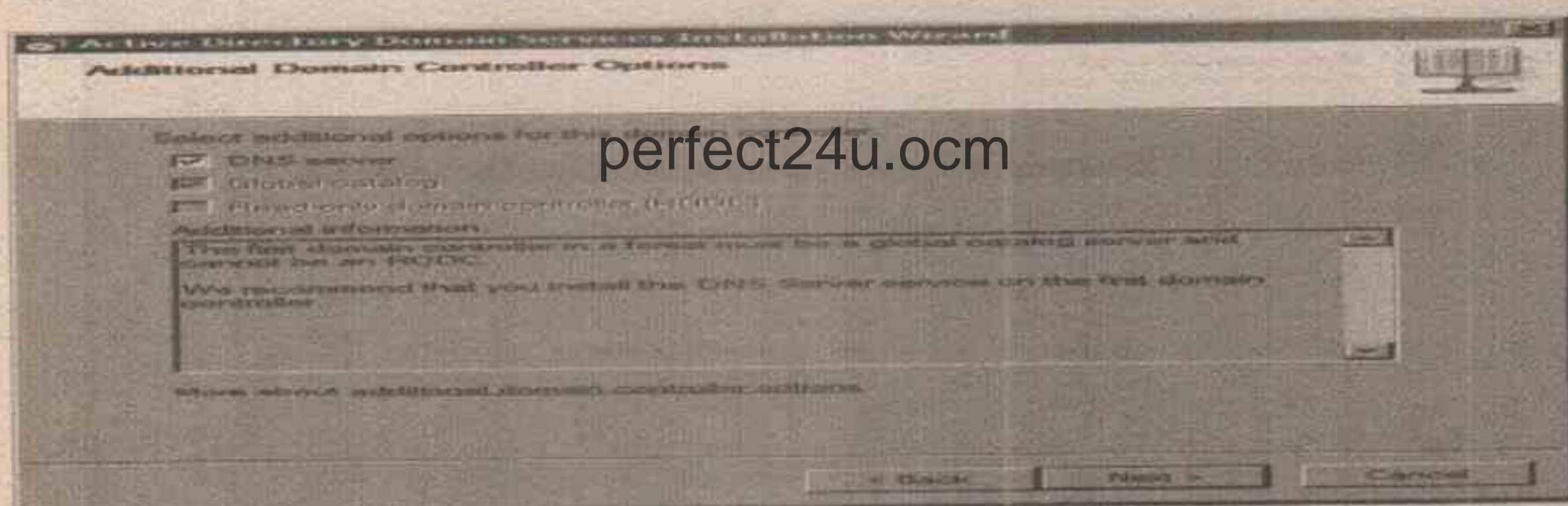


I will choose Windows Server 2003 as my functional level. Choosing windows server 2008 functional level does not provide any new features over the Windows 2003 forest functional level. However, it ensures that any new domains created in this forest will automatically operate at the Windows Server 2008 domain functional level, which does provide unique features. click on **Next**.



Clicking next, the dcpromo wizard will check for DNS configurations.

If DNS is not installed on your system, choose the DNS Server option on the following screen.

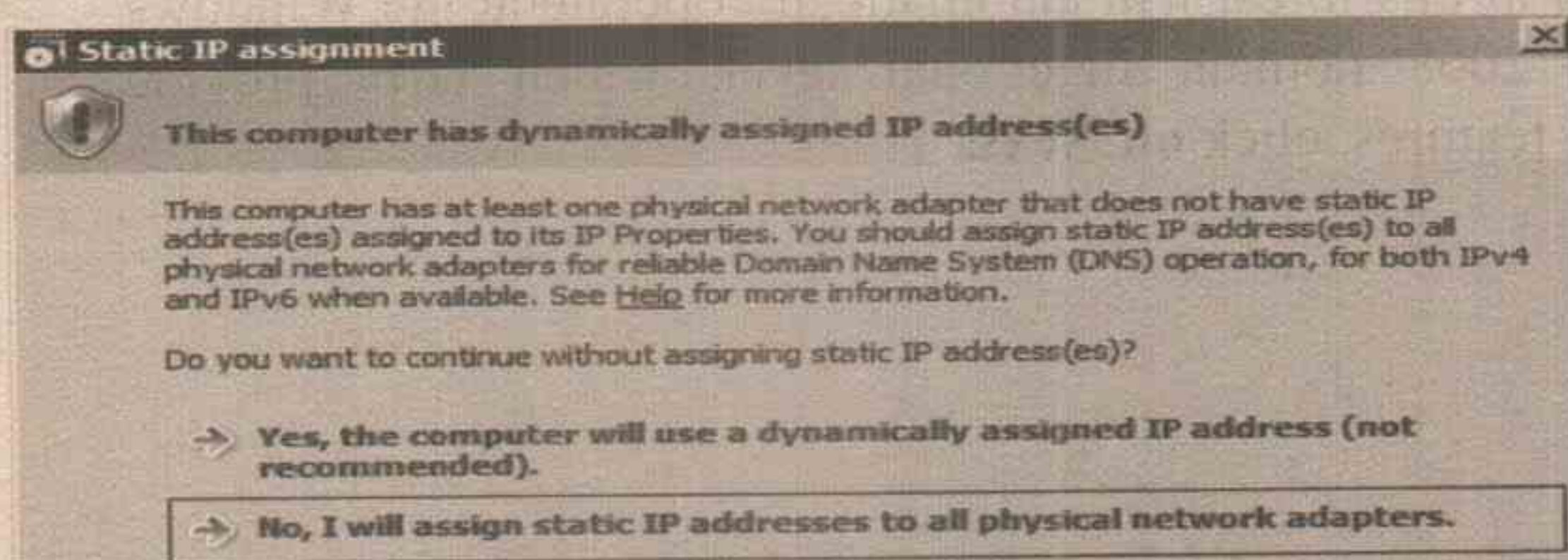


Here you get the info that tells you:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

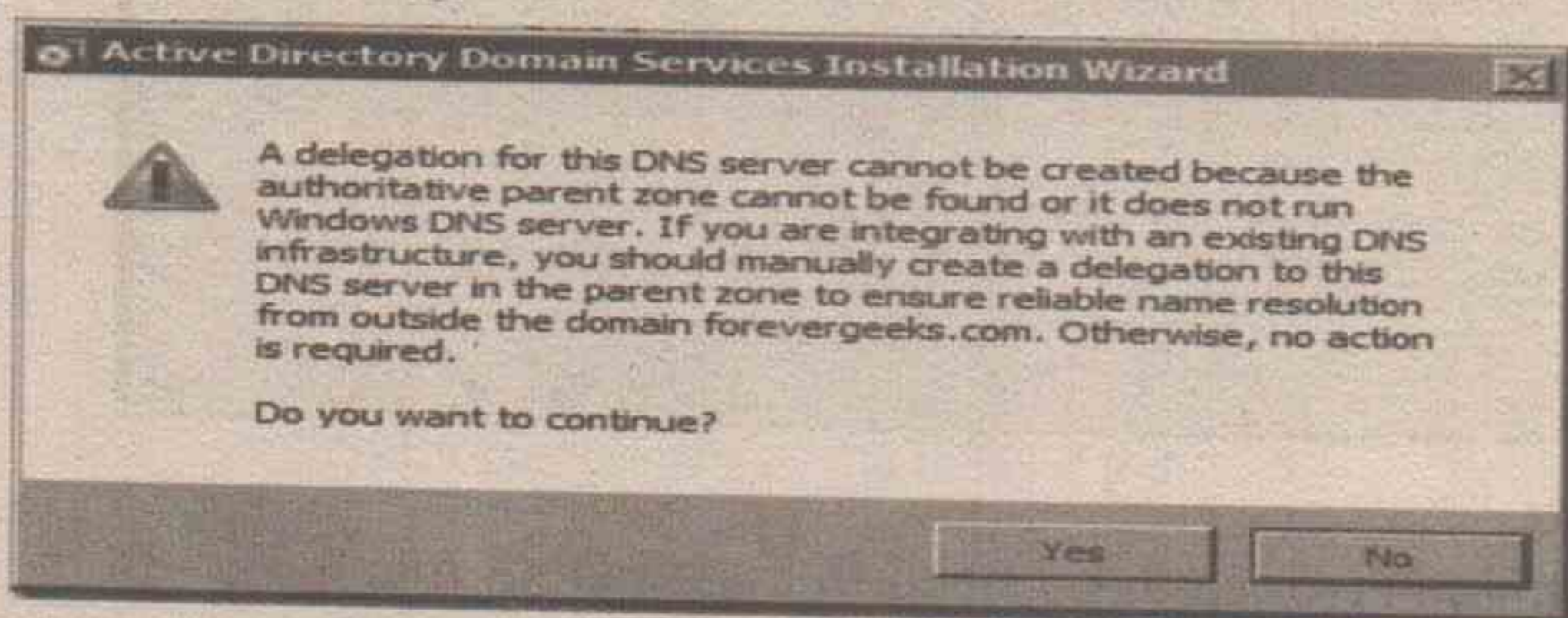
Click on **Next**.

If your server does have static IP address assigned on the server, you might get the following warning:



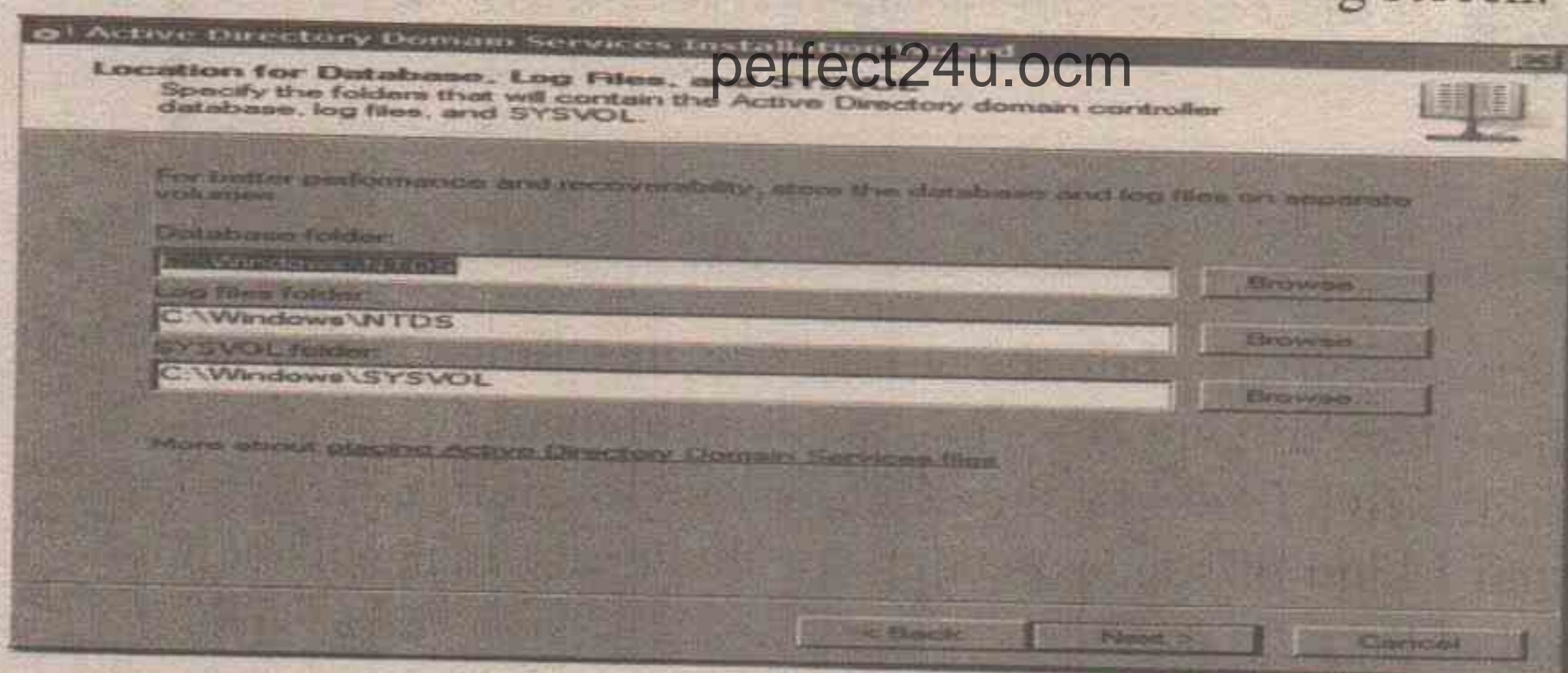
as you can see, having dynamic assigned IP address is not recommended. use static IP addresses for servers whenever is possible.

Choose your option, and click **Next** .
another warning:



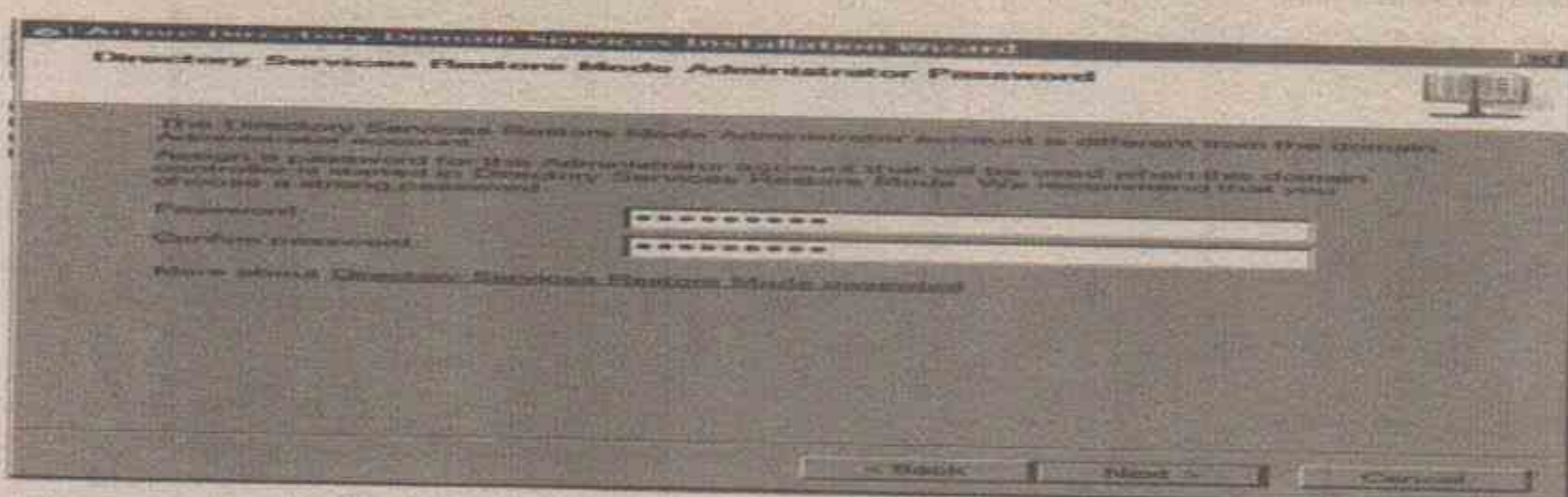
if you get this warning, click on **OK**.

choose the location of the AD database on the following screen:



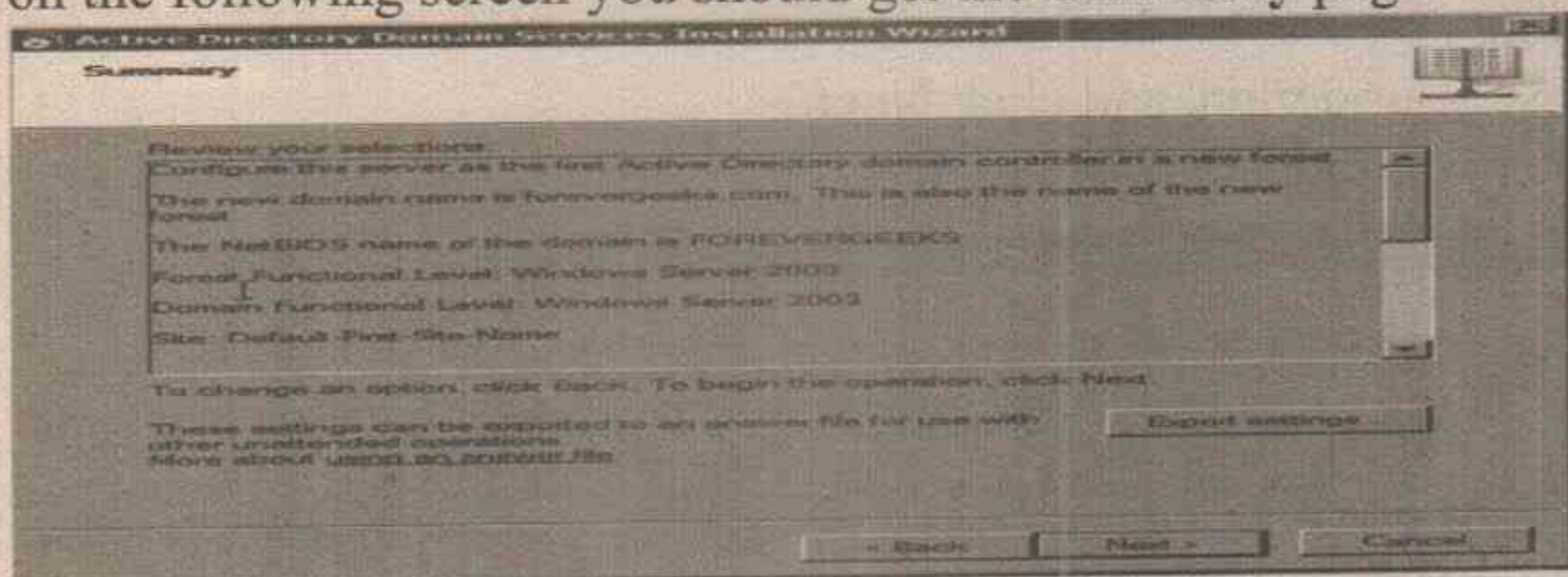
Leave the default settings, and click on **Next**.

Enter your the password for your Restore Mode Administrator on the following screen.



click **Next** after entering the password.

on the following screen you should get the **Summary** page



click on **Next**.

damn it!! I got an error saying I need to install DNS manually .



“An error occurred while the wizard was installing DNS, you will have to configure **DNS** for this domain manually.

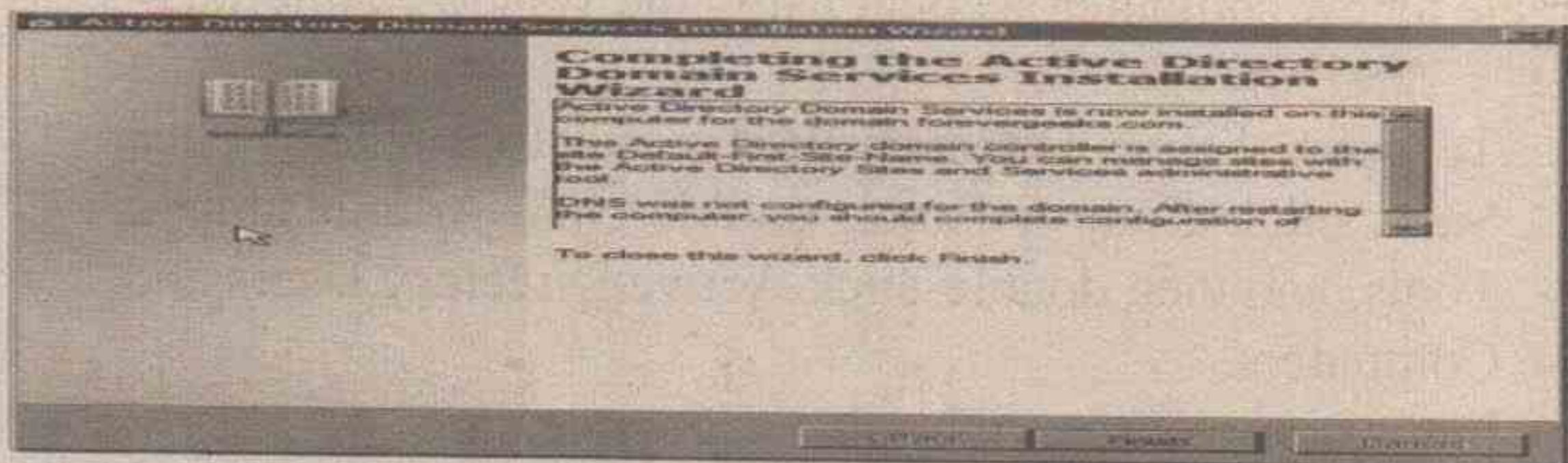
This is the first time I let the dcpromo.exe to configure DNS for me, and I kind of was expecting for this error. that will be the subject of the next article.

click **OK** on the error for now.

active directory installation should start installing. but it won't work perfect until **DNS** is install.

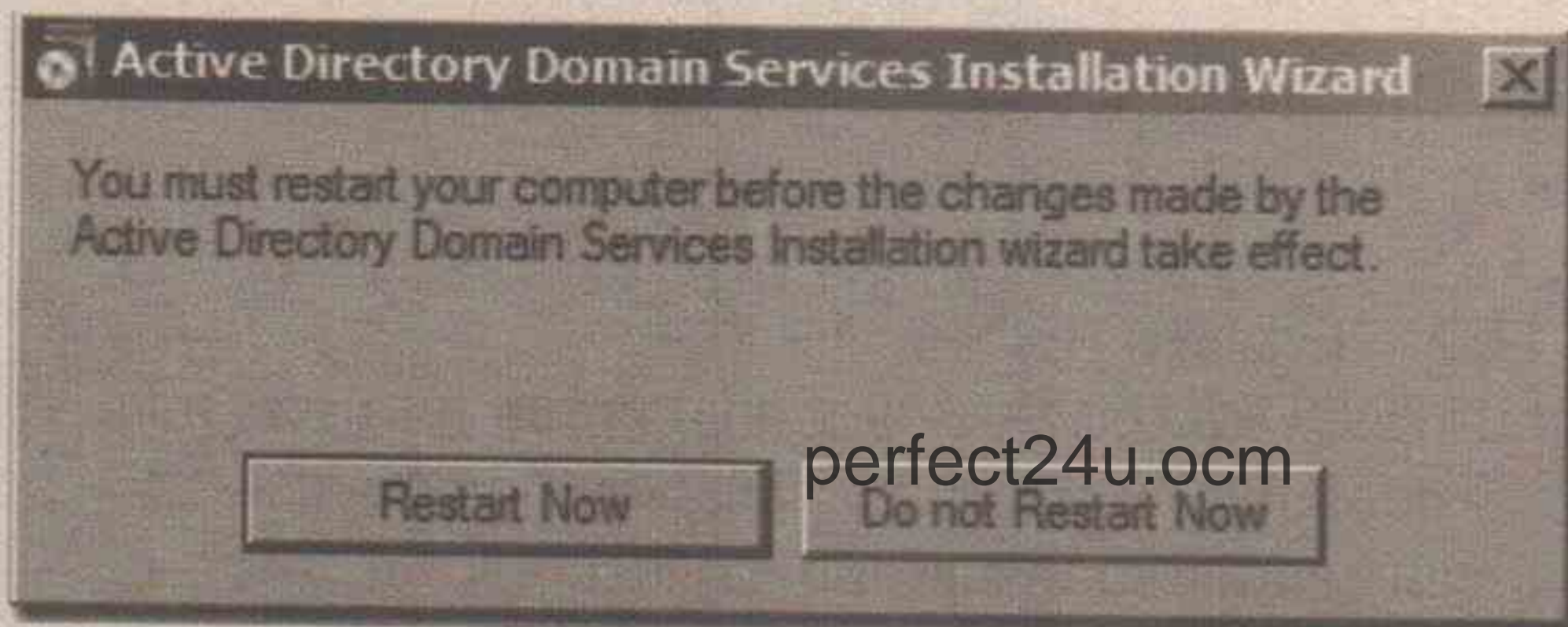


after awhile, you should get the completion window.



click on **Finish**.

you will need to reboot the computer



go ahead and restart the computer, and if you need to install DNS do so after the reboot.

MANAGING USER ACCOUNTS

1. Point to **New**, and then click **Computer**.
2. Type the computer name.
3. To manage domain users, create user accounts in Active Directory Domain Services (AD DS). In contrast, to manage users that are specific to one computer, create local user accounts.

CREATING A COMPUTER ACCOUNT

To create a new computer account using the Windows interface

1. To open Active Directory Users and Computers, click Start, click Control Panel, double-click Administrative Tools, and then double-click Active Directory Users and Computers.
2. In the console tree, right-click Computers.
3. Active Directory Users and Computers*domain node*\Computers

Or, right-click the folder in which you want to add the computer.

INTRODUCTION TO GROUP

Domain Users INTRODUCTION is a global group for users in Active Directory domains. When you create new domain users, they're automatically added to this group. By default, the local Administrator and Guest accounts are members of this group. Power Users exist only on computers that are not domain controllers.

MANAGING GROUPS

To create a Windows group on Windows Server 2003

1. On the desktop, right-click My Computer, and then click Manage.
2. In the Computer Management window, under System Tools, expand Local Users and Groups.
3. Right-click Groups and then click New Group.
4. In the New Group dialog box, do the following: ...
5. Click Create.

CREATING Organizational Unit

An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure. Each domain can implement its own organizational unit.

To create a new organizational unit using the Windows interface

1. To open Active Directory Users and Computers, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.

To open Active Directory Users and Computers in Windows Server® 2012, click **Start**, type **dsa.msc**.

2. In the console tree, right-click the domain name.
3. Point to **New**, and then click **Organizational Unit**.
4. Type the name of the organizational unit (OU).

OVERVIEW GROUP POLICY AND THE ACTIVE DIRECTORY

In Windows server 2008, administrators use Group Policy to enhance and control users' desktops. To simplify the process, administrators can create a specific desktop configuration that is applied to groups of users and computers. The Windows server 2008 Active Directory™ service enables Group Policy. The policy information is stored in Group Policy objects (GPOs), which are linked to selected Active Directory containers: sites, domains, and organizational units (OUs).

A GPO can be used to filter objects based on security group membership, which allows administrators to manage computers and users in either a centralized or a de-centralized manner. To do this, administrators can use filtering based on security groups to define the scope of Group Policy management, so that Group

Policy can be applied centrally at the domain level, or in a decentralized manner at the OU level, and can then be filtered again by security groups. Administrators can use security groups in Group Policy to:

- Filter the scope of a GPO. This defines which groups of users and computers a GPO affects.
- Delegate control of a GPO. There are two aspects to managing and delegating Group Policy: managing the group policy links and managing who can create and edit GPOs.

Administrators use the Group Policy Microsoft Management Console (MMC) snap-in to manage policy settings. Group Policy includes various features for managing these policy settings. In addition, third parties can extend Group Policy to host other policy settings. The data generated by Group Policy is stored in a Group Policy object (GPO), which is replicated in all domain controllers within a single domain.

The Group Policy snap-in includes several MMC snap-in extensions, which constitute the main nodes in the Group Policy snap-in. The extensions are as follows:

- **Administrative templates.** These include registry-based Group Policy, which you use to mandate registry settings that govern the behavior and appearance of the desktop, including the operating system components and applications.
- **Security settings.** You use the Security Settings extension to set security options for computers and users within the scope of a Group Policy object. You can

define local computer, domain, and network security settings.

- **Software installation.** You can use the Software Installation snap-in to centrally manage software in your organization. You can assign and publish software to users and assign software to computers.
- **Scripts.** You can use scripts to automate computer startup and shutdown and user logon and logoff. You can use any language supported by Windows Script Host. These include the Microsoft Visual Basic® development system, Scripting Edition (VBScript); JavaScript; PERL; and MS-DOS®-style batch files (.bat and .cmd).
- **Remote Installation Services.** You use Remote Installation Services (RIS) to control the behavior of the Remote Operating System Installation feature as displayed to client computers.
- **Internet Explorer maintenance.** You use Internet Explorer Maintenance to manage and customize Microsoft® Internet Explorer on Windows server 2008-based computers.
- **Folder redirection.** You use Folder Redirection to redirect Windows server 2008 special folders from their default user profile location to an alternate location on the network. These special folders include My Documents, Application Data, Desktop, and the Start Menu.

Figure below shows how Group Policy objects use the Active Directory hierarchy for deploying Group Policy.

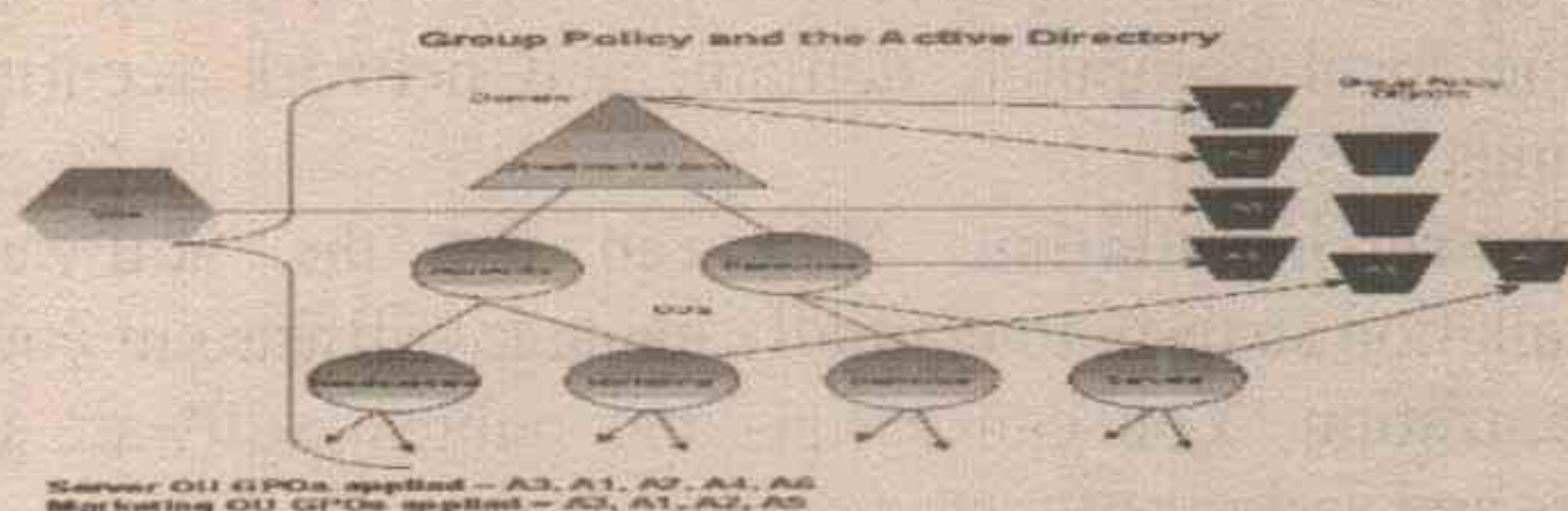


Figure: The Hierarchy of Group Policy and the Active Directory

Group Policy objects are linked to site, domain, and OU containers in the Active Directory. The default order of precedence follows the hierarchical nature of the Active Directory: sites are first, then domains, and then each OU. A GPO can be associated with more than one Active Directory container or multiple containers can be linked to a single GPO.

perfect24u.ocm

Configuring the scope of group policies objects.

(Local or Remote Computers)

To access Group Policy for a local or a remote computer, you add the Group Policy snap-in to the MMC console, and focus it on a remote or local computer. To access Group Policy for the local computer, use the GPWalkthrough console created earlier in this document, and choose the **Local Computer Policy** node. You can add other computers to the console namespace by adding another Group Policy snap-in to the GPWalkthrough console, and clicking the **Browse** button when the **Select Group Policy** object dialog box is displayed.

Note: Some of the Group Policy extensions are not loaded when Group Policy is run against a local GPO.

MANAGING AND CREATING A GROUP POLICY OBJECT

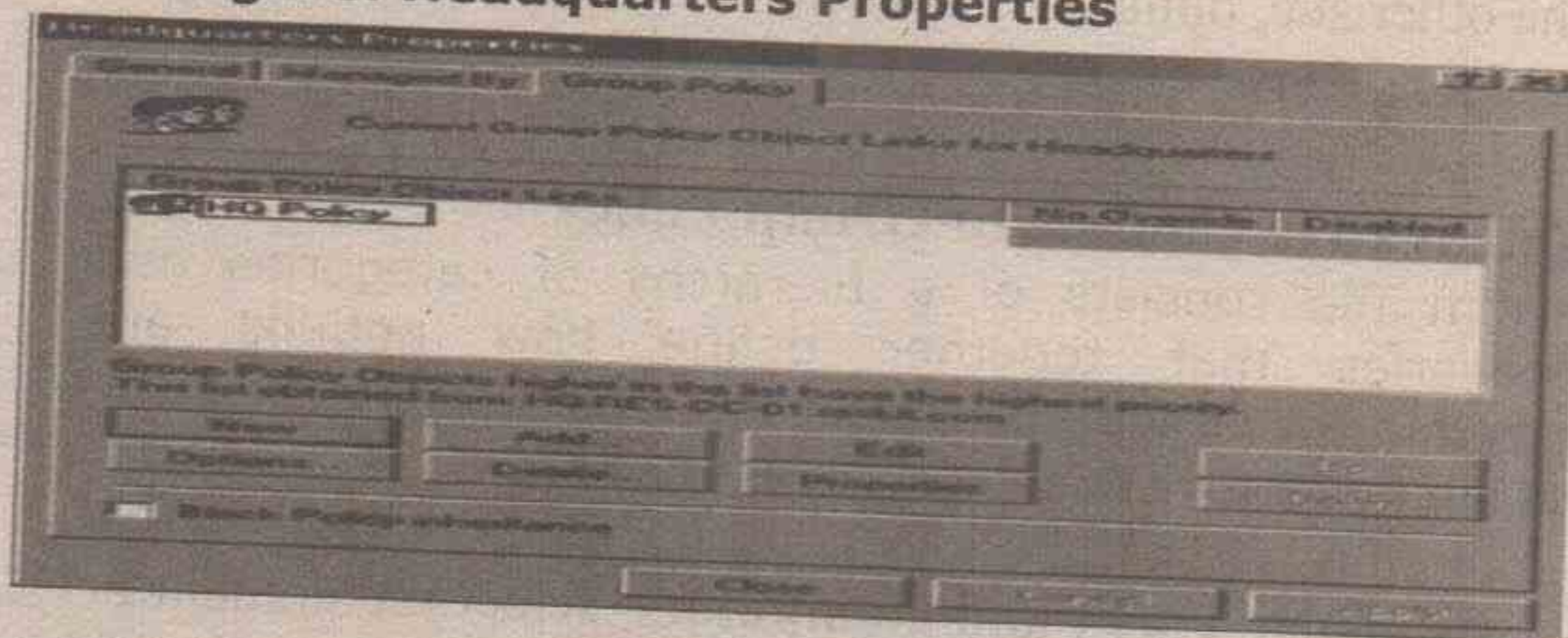
The Group Policy settings you create are contained in a Group Policy Object (GPO) that is in turn associated with selected Active Directory objects, such as sites, domains, or organizational units (OUs).

To create a Group Policy Object (GPO)

1. Open the **GPWalkthrough** MMC console.
2. Click the + next to **Active Directory Users and Computers**, and click the **reskit.com** domain.
3. Click the + next to **Accounts** to expand the tree.
4. Right-click **Headquarters**, and select **Properties** from the context menu.
5. In the **Headquarters Properties** page, click the **Group Policy** tab.
6. Click **New**, and type **HQ Policy**.

The **Headquarters Properties** page should appear as in Figure below:

Figure: Headquarters Properties



At this point you could add another GPO for the Headquarters OU, giving each one that you create a meaningful name, or you could edit the HQ Policy GPO, which starts the Group Policy snap-in for that GPO. All Group Policy functionality is derived from the snap-in extensions. In this exercise, all of these extensions are enabled. It is possible—using standard MMC

methods—to restrict the extension snap-ins that are loaded for any given snap-in. For information on this capability, see the Windows server 2008 Server Online Help for Microsoft Management Console.

There is also a Group Policy that you can use to restrict the use of MMC snap-in extensions. To access this policy, navigate to the System\Group Policy node under Administrative Templates. Use the Explain tab to learn more about the use of these policies.

If you have more than one GPO associated with an Active Directory folder, verify the GPO order; a GPO that is higher in the list has the highest precedence. Note that GPOs higher in the list are processed last (this is what gives them a higher precedence). GPOs in the list are objects; they have context menus that you use to view the properties of each GPO. You can use the context menus to obtain and modify general information about a GPO. This information includes Discretionary Access Control Lists (DACLS, which are covered in the Security Group Filtering section of this document), and lists the other site, domain, or OUs to which this GPO is linked.

7. Click Close

Administrative Control of Group Policy

The .adm file consists of a hierarchy of categories and subcategories that together define how options are organized in the Group Policy user interface.

To add administrative templates (.adm files)

1. In the Group Policy console double-click **Active Directory Users and Computers**, select the domain or OU for which you want to set policy, click **Properties**, and then click **Group Policy**.
2. In the **Group Policy** properties page, select the Group Policy Object you want to edit from the **Group Policy objects links** list, and click **Edit** to open the Group Policy snap-in.

3. In the Group Policy console, click the plus sign (+) next to either **User Configuration** or **Computer Configuration**. The .adm file defines which of these locations the policy is displayed in, so it doesn't matter which node you choose.
4. Right-click **Administrative Templates**, and select **Add/Remove Templates**. This shows a list of the currently active templates files for this Active Directory container.
5. Click **Add**. This shows a list of the available .adm files in the %systemroot%\inf directory of the computer where Group Policy is being run. You can choose an .adm file from another location. Once chosen, the .adm file is copied into the GPO.

To set registry-based settings using administrative templates

1. In the GPWalkthrough console, double-click **Active Directory Users and Computers**, double-click the **reskit.com** domain, double-click **Accounts**, right-click the **Headquarters** OU, and then click **Properties**.
2. In the **Headquarters Properties** dialog box, click **Group Policy**.
3. Double-click the **HQ Policy** GPO from the **Group Policy object links** list to edit the HQ Policy GPO.
4. In the Group Policy console, under the **User Configuration** node, click the plus sign (+) next to **Administrative Templates**.
5. Click **Start Menu & Taskbar**. Note that the details pane shows all the policies as **Not configured**.
6. In the details pane, double-click the **Remove Run menu from Start menu** policy. This displays a dialog box for the policy as shown in Figure 8 below.

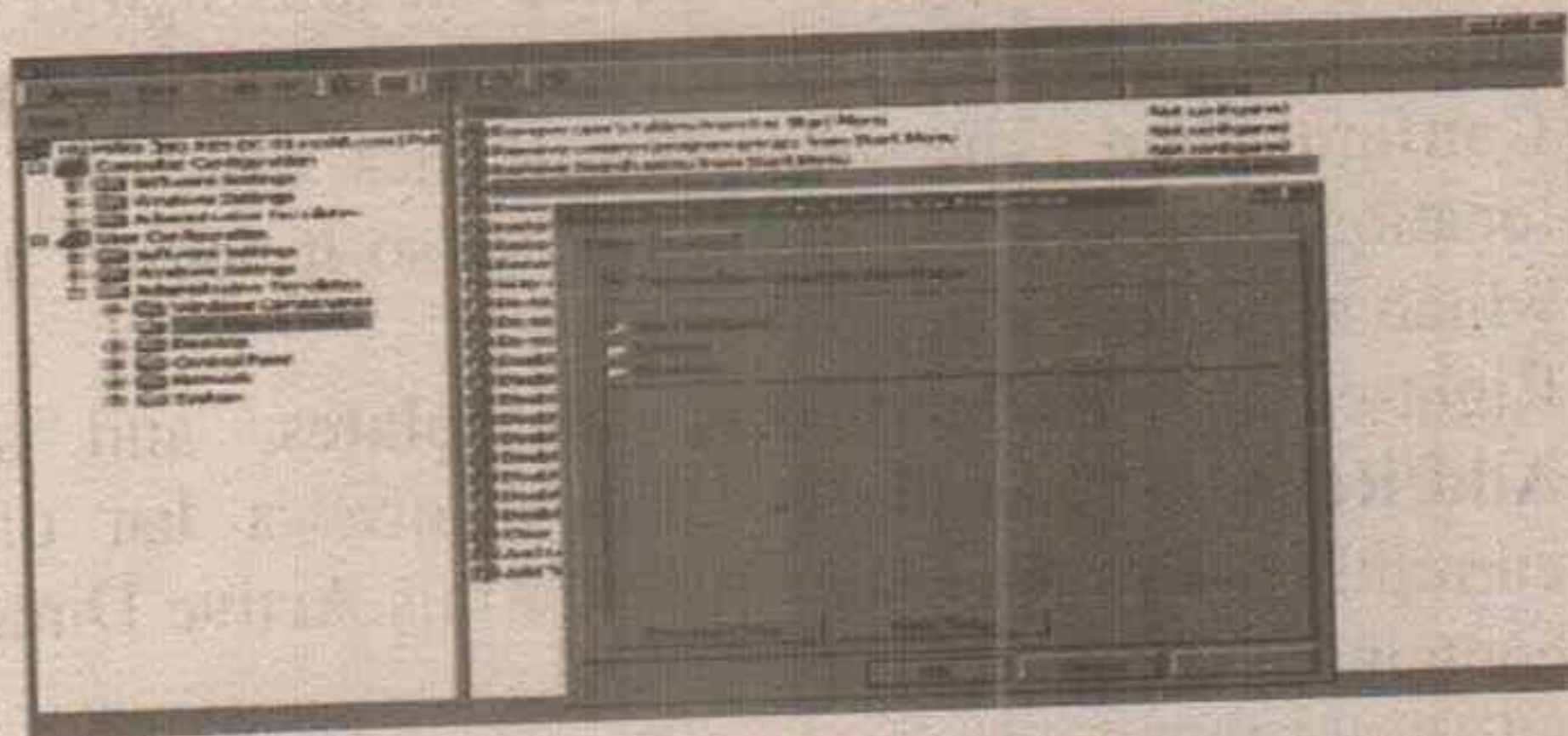


Figure 8: Remove Run menu from Start Menu

7. In the **Remove Run menu from Start menu** dialog box, click **Enabled**.

Note the **Previous Policy** and **Next Policy** buttons in the dialog box. You can use these buttons to navigate the details pane to set the state of other policies. You can also leave the dialog box open and click another policy in the details pane of the Group Policy snap-in. After the details pane has the focus, you can use the **Up** and **Down** arrow keys on the keyboard and press **Enter** to quickly browse through the settings (or **Explain** tabs) for each policy in the selected node.

8. Click **OK**. Note the change in state in the **Setting** column, in the details pane. This change is immediate; it has been saved to the GPO. If you are in a replicated domain controller (DC) environment, this action sets a flag that triggers a replication cycle.

If you log on to a workstation in the **reskit.com** domain with a user from the **Headquarters** OU, you will note that the **Run** menu has been removed.

Configuring Group Policy Setting

The IT professional describes steps to configure a security policy setting on the local computer, on a domain-joined computer, and on a domain controller.

You must have Administrators rights on the local computer, or you must have the appropriate permissions to update a Group Policy Object (GPO) on the domain controller to perform these procedures.

Configuring Security Policy

To configure a setting for your local computer

1. To open Local Security Policy, click **Start**, type, **secpol.msc**.
2. Navigate the console tree to **Local Computer Policy\Windows Settings\Security Settings**
3. Under **Security Settings** of the console tree, do one of the following:
 - Click **Account Policies** to edit the **Password Policy** or **Account Lockout Policy**.
 - Click **Local Policies** to edit an **Audit Policy**, a **User Rights Assignment**, or **Security Options**.
4. When you find the policy setting in the details pane, double-click the security policy that you want to modify.
5. Modify the security policy setting, and then click **OK**.

To configure a setting for computer that is joined to a domain

The following procedure describes how to configure a security policy setting for a Group Policy Object when you are on a workstation or server that is joined to a domain.

You must have the appropriate permissions to install and use the Microsoft Management Console (MMC), and to update a Group Policy Object (GPO) on the domain controller to perform these procedures.

1. To open the MMC and add the Group Policy Object Editor, click **Start**, type **mmc.msc**.

2. On the **File** menu of the MMC, click **Add/Remove snap-in**, and then click **Add**.
3. In **Add Standalone Snap-in**, double-click **Group Policy Object Editor**.
4. In **Select Group Policy Object**, click **Browse**, browse to the GPO you would like to modify, and then click **Finish**.
5. Click **Close**, and then click **OK**.

This procedure added the snap-in to the MMC.

6. In the console tree, locate *GroupPolicyObject [ComputerName]* Policy, click **Computer Configuration**, click **Windows Settings**, and then click **Security Settings**.
7. Do one of the following:
 - Click **Account Policies** to edit the **Password Policy** or **Account Lockout Policy**.
 - Click **Local Policies** to edit an **Audit Policy**, a **User Rights Assignment**, or **Security Options**.
 - Click **Event Log** to edit event log settings.
8. In the details pane, double-click the security policy setting that you want to modify.

Configuring an Audit Policy

An **audit policy** defines account limits for a set of users of one or more resources. It comprises rules that define the limits of a **policy** and workflows to process violations after they occur. **Audit** scans use the criteria defined in an **audit policy** to evaluate whether violations have occurred in your organization.

Auditing implementation has several steps:

1. Enable auditing on the domain controller.

2. Select objects to audit, and set the system access control lists (SACL) for the objects.
3. Configure the event log.
4. Protect the audit data from unauthorized access or modification.
5. Review and maintain the audit logs.

DNS (Domain Name Services)

Domain Name Servers (DNS) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.

INSTALL A DNS SERVER IN WINDOWS SERVER 2008

You can install a DNS server from the Control Panel or when promoting a member server to a domain controller (DC) Figure A).

During the promotion, if a DNS server is not found, you will have the option of installing it.

Domain controller

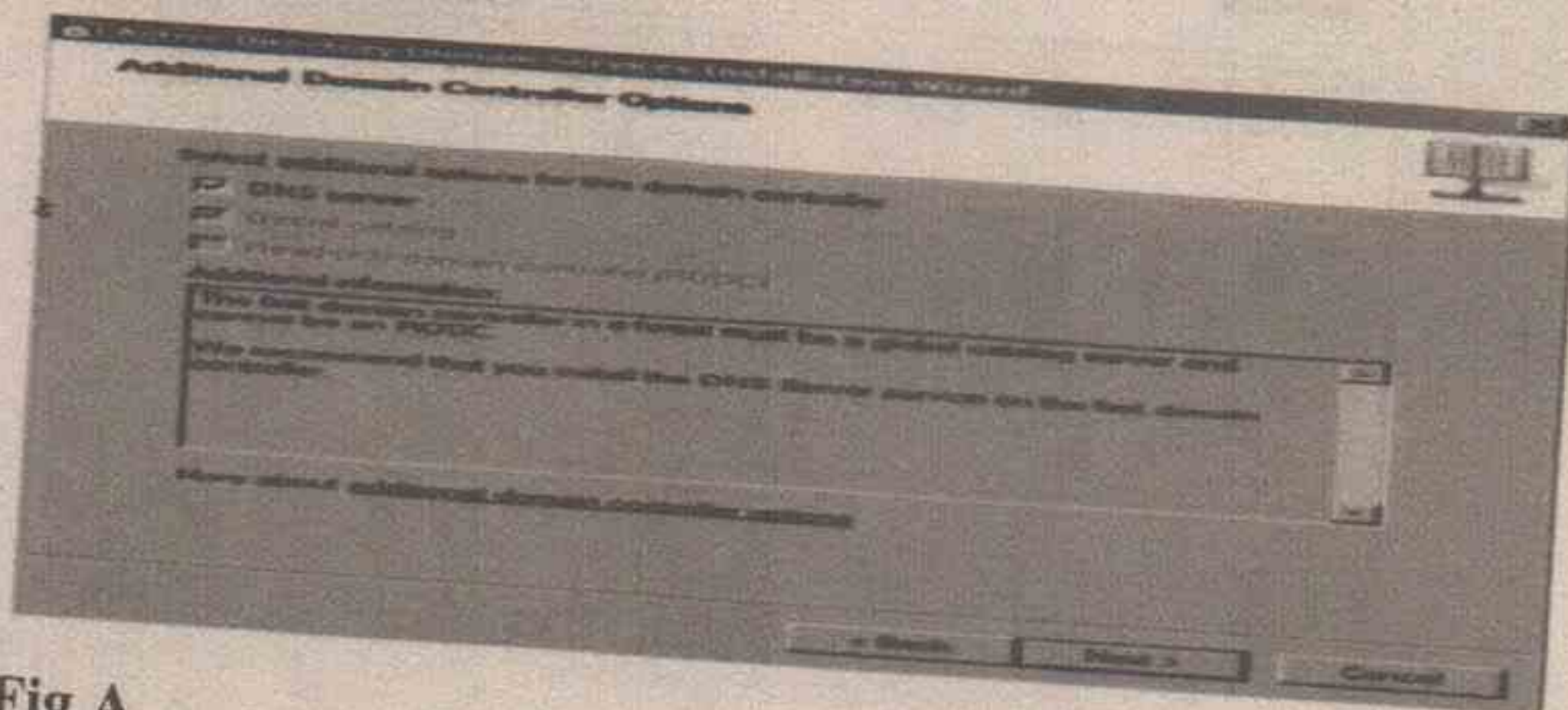
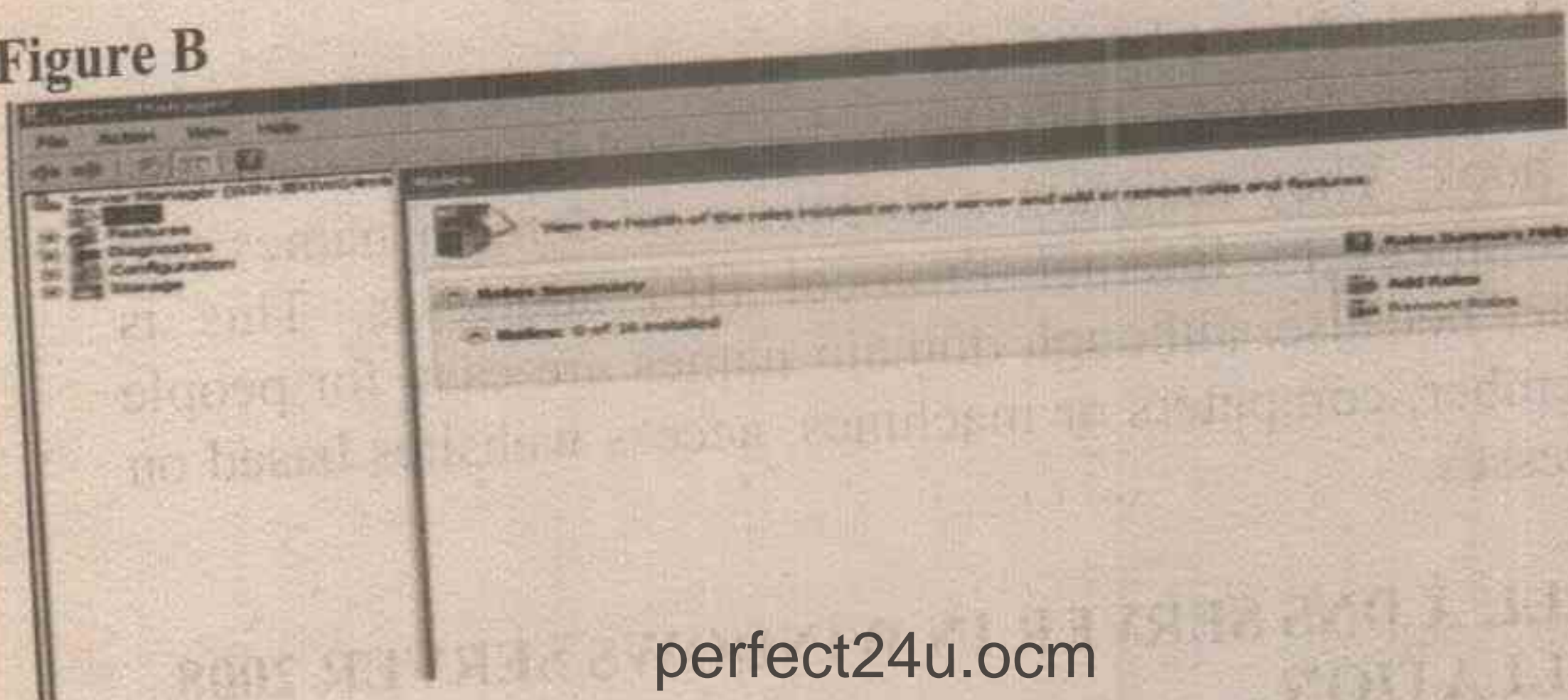


Fig A

To install a DNS server from the Control Panel, follow these steps:

- From the Start menu, select | Control Panel | Administrative Tools | Server Manager.
- Expand and click Roles (**Figure B .)**
- Choose Add Roles and follow the wizard by selecting the DNS role (**Figure C .)**
- Click Install to install DNS in Windows Server 2008 (**Figure D .)**

Figure B



perfect24u.ocm

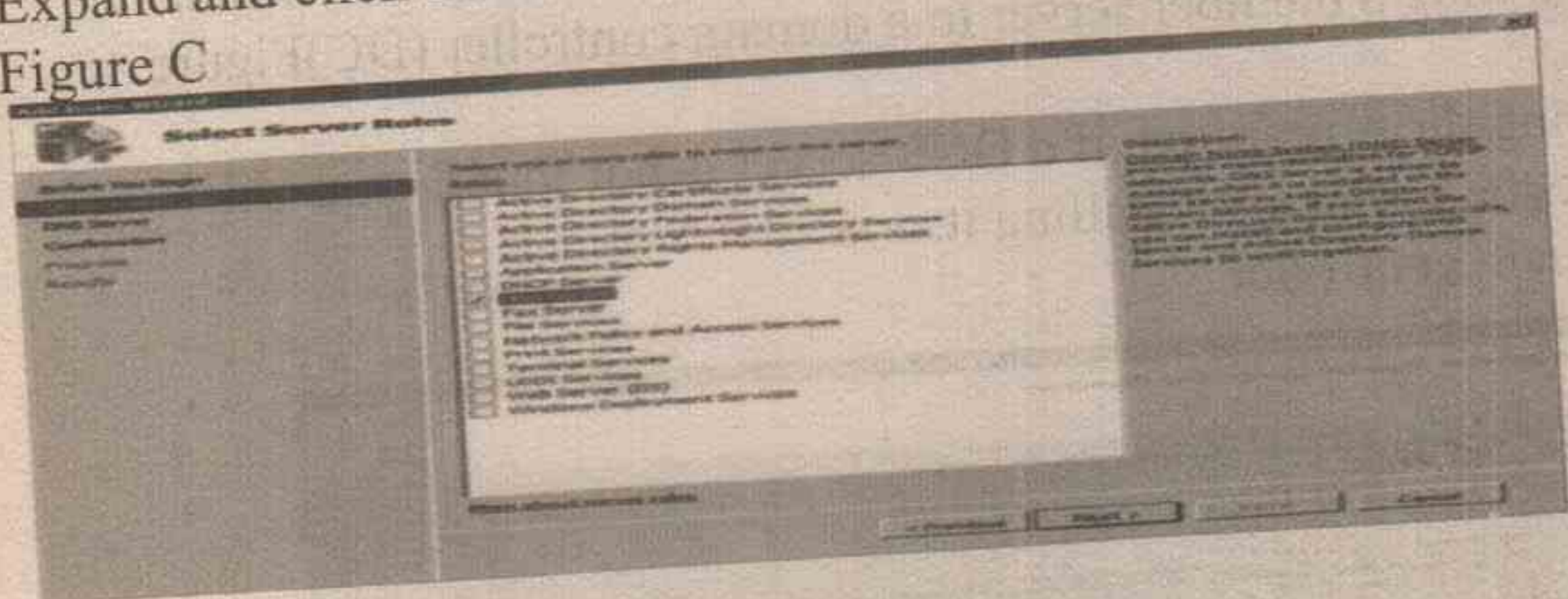
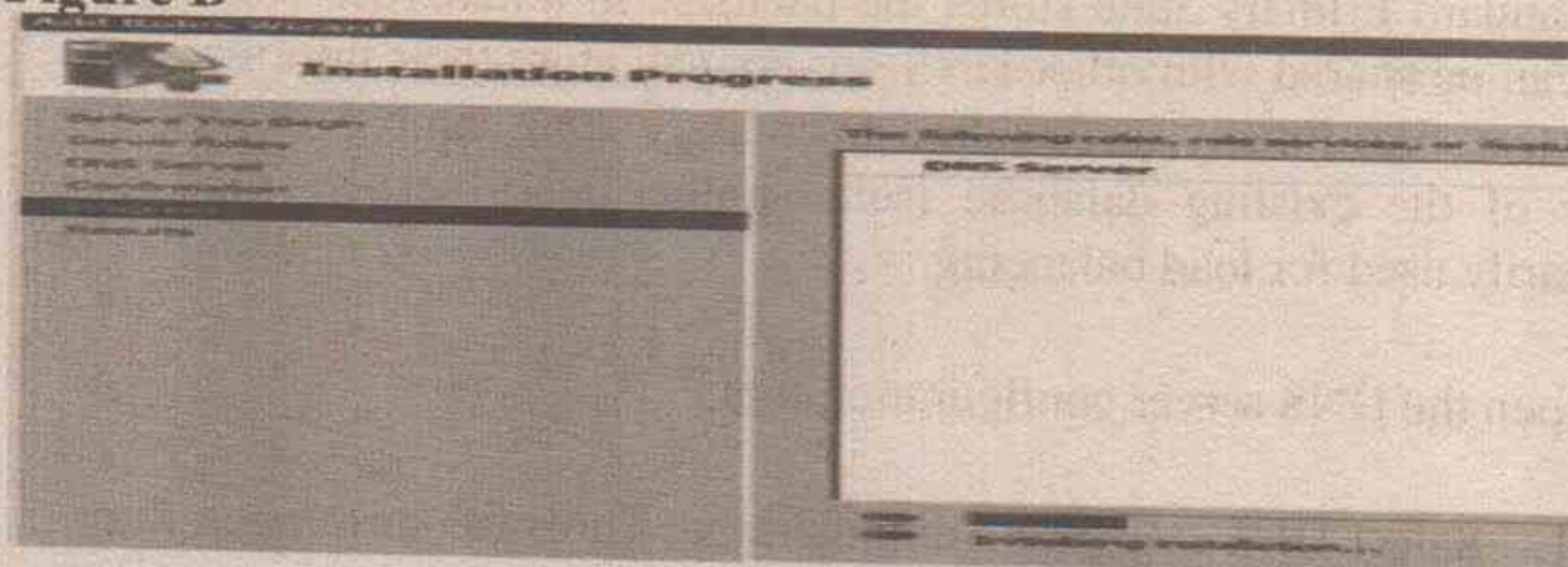
Expand and click Roles
Figure C

Figure D

Install DNS

DNS console and configuration

After installing DNS, you can find the DNS console from Start | All Programs | Administrative Tools | DNS. Windows 2008 provides a wizard to help configure DNS.

When configuring your DNS server, you must be familiar with the following concepts:

perfect24u.ocm

- Forward lookup zone
- Reverse lookup zone
- Zone types

A forward lookup zone is simply a way to resolve host names to IP addresses. A reverse lookup zone allows a DNS server to discover the DNS name of the host. Basically, it is the exact opposite of a forward lookup zone. A reverse lookup zone is not required, but it is easy to configure and will allow for your Windows Server 2008 Server to have full DNS functionality.

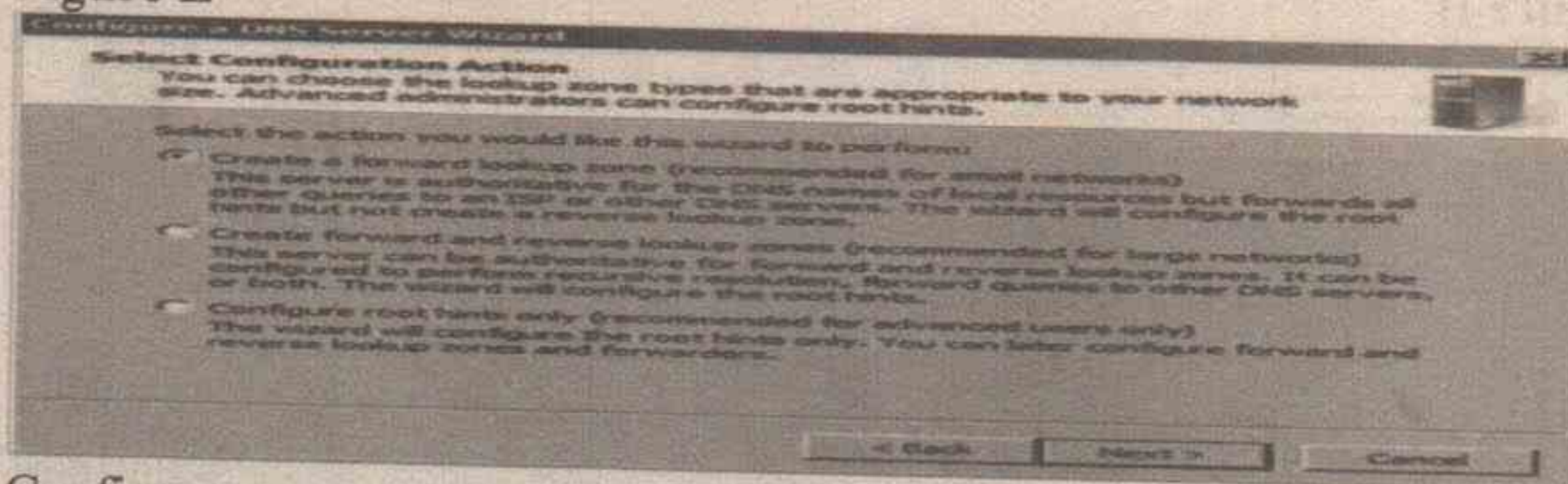
When selecting a DNS zone type, you have the following options: Active Directory (AD) Integrated, Standard Primary, and Standard Secondary. AD Integrated stores the database information in AD and allows for secure updates to the database file. This option will appear only if AD is configured. If it is configured and you select this option, AD will store and replicate your zone files.

A Standard Primary zone stores the database in a text file. This text file can be shared with other DNS servers that store their information in a text file. Finally, a Standard Secondary zone simply creates a copy of the existing database from another DNS server. This is primarily used for load balancing.

To open the DNS server configuration tool:

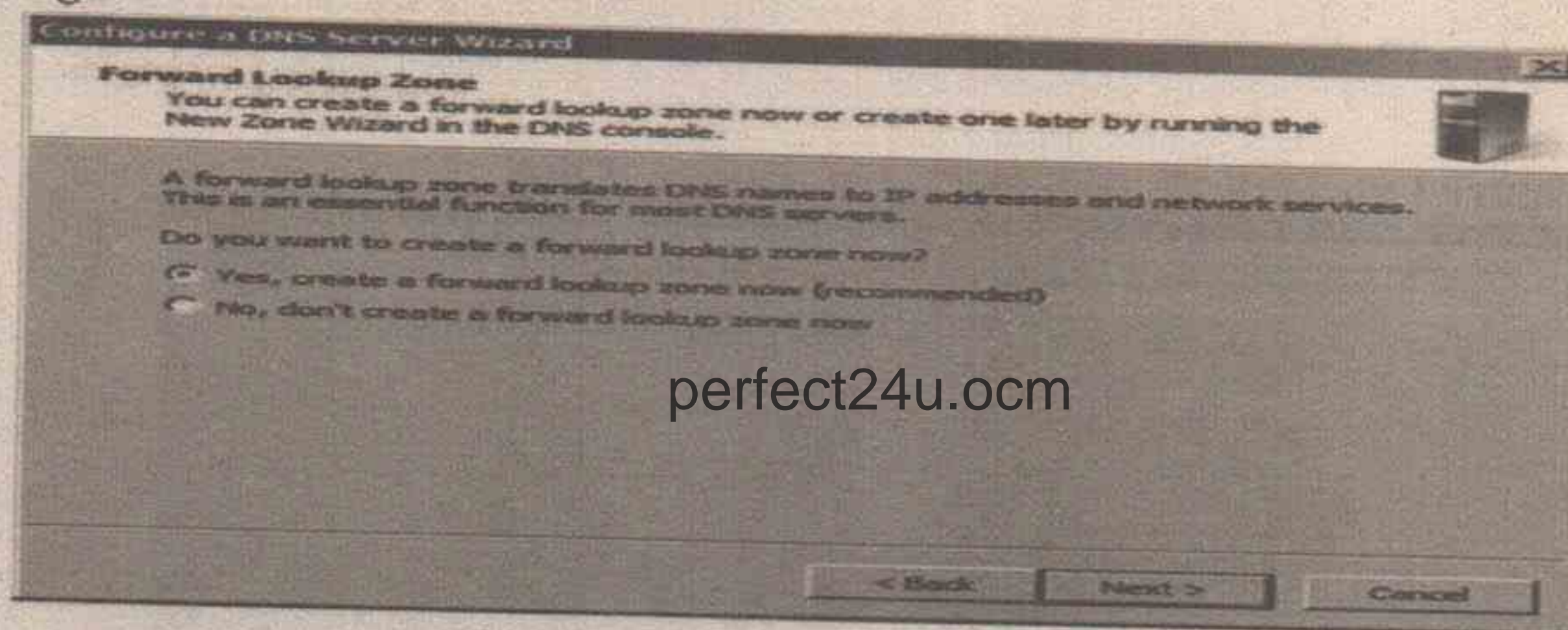
1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Highlight your computer name and choose Action | Configure a DNS Server' to launch the Configure DNS Server Wizard.
3. Click Next and choose to configure the following: forward lookup zone, forward and reverse lookup zone, root hints only (**Figure E .**)
4. Click Next and then click Yes to create a forward lookup zone (**Figure F .**)
5. Select the appropriate file to install the desired Zone Type (**Figure G .**)
6. Click Next and type the name of the zone you are creating.
7. Click Next and then click Yes to create a reverse lookup zone.
8. Repeat Step 5.
9. Choose whether you want an IPv4 or IPv6 Reverse Lookup Zone (**Figure H .**)
10. Click Next and enter the information to identify the reverse lookup zone (**Figure I .**)
11. You can choose to create a new file or use an existing DNS file (**Figure J .**)
12. On the Dynamic Update window, specify how DNS accepts secure, nonsecure, or no dynamic updates.
13. If you need to apply a DNS forwarder, you can apply it on the Forwarders window. (**Figure K .**)
14. Click Finish (**Figure L .**)

Figure E



Configure

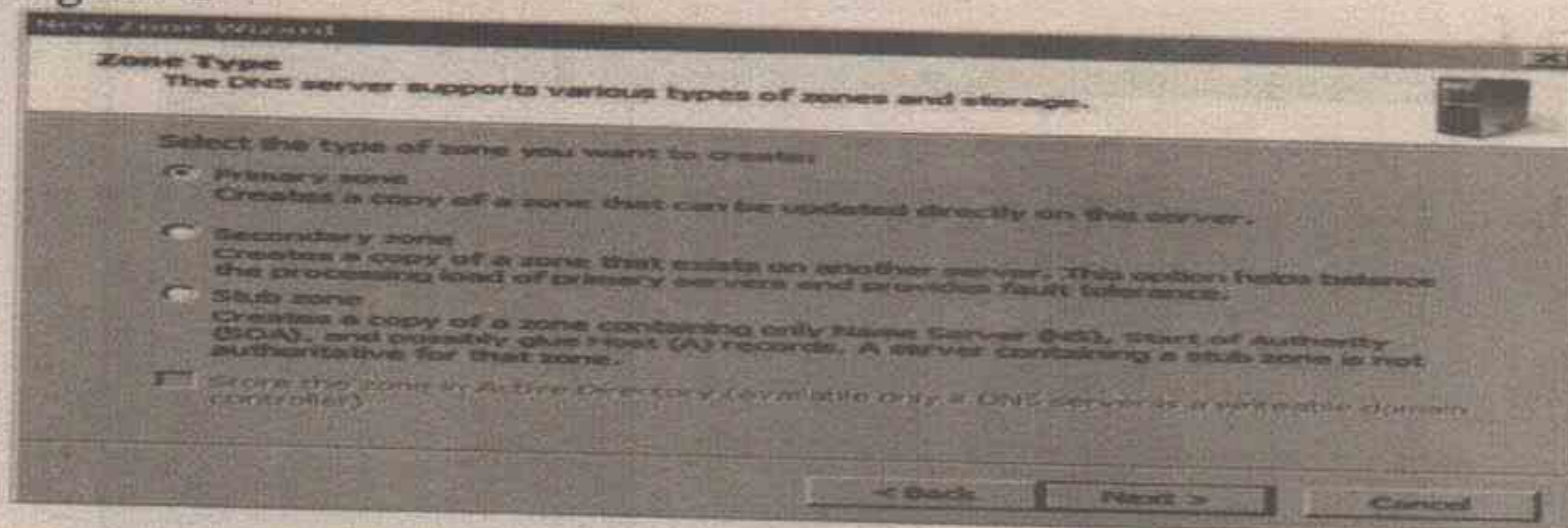
Figure F



perfect24u.ocm

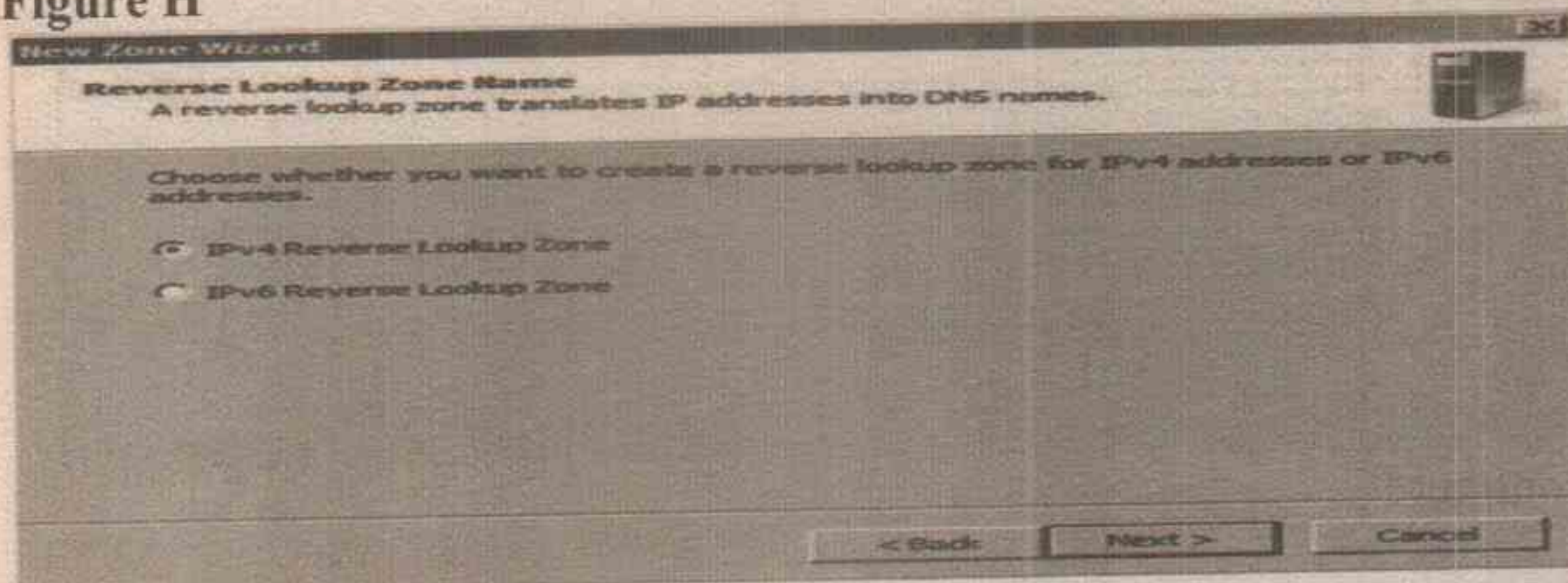
Forward lookup zone

Figure G



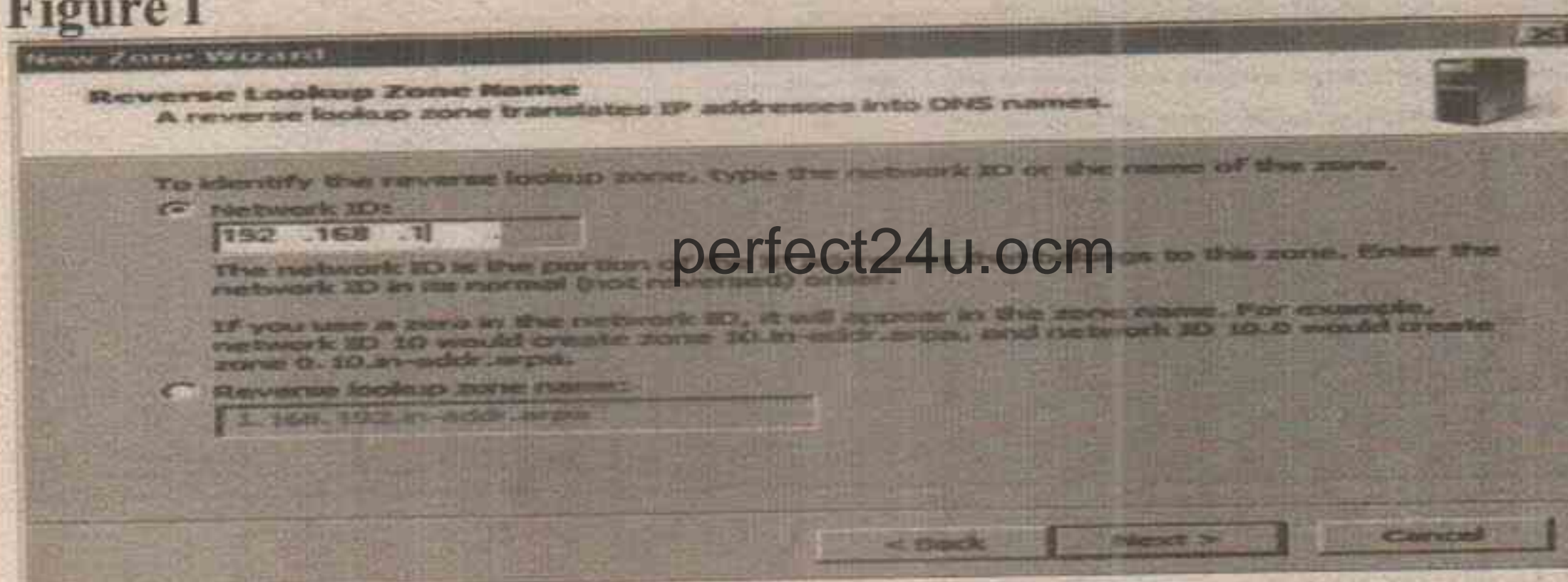
Desired zone

Figure H



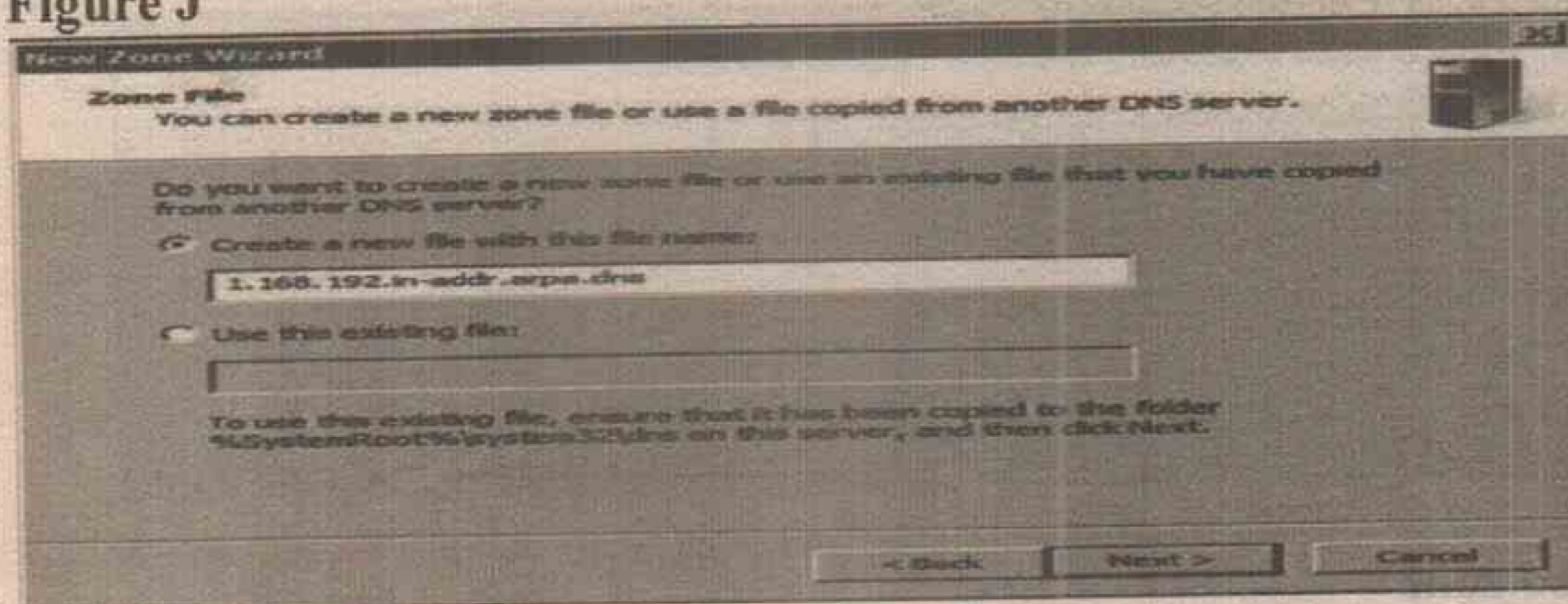
IPv4 or IPv6

Figure I



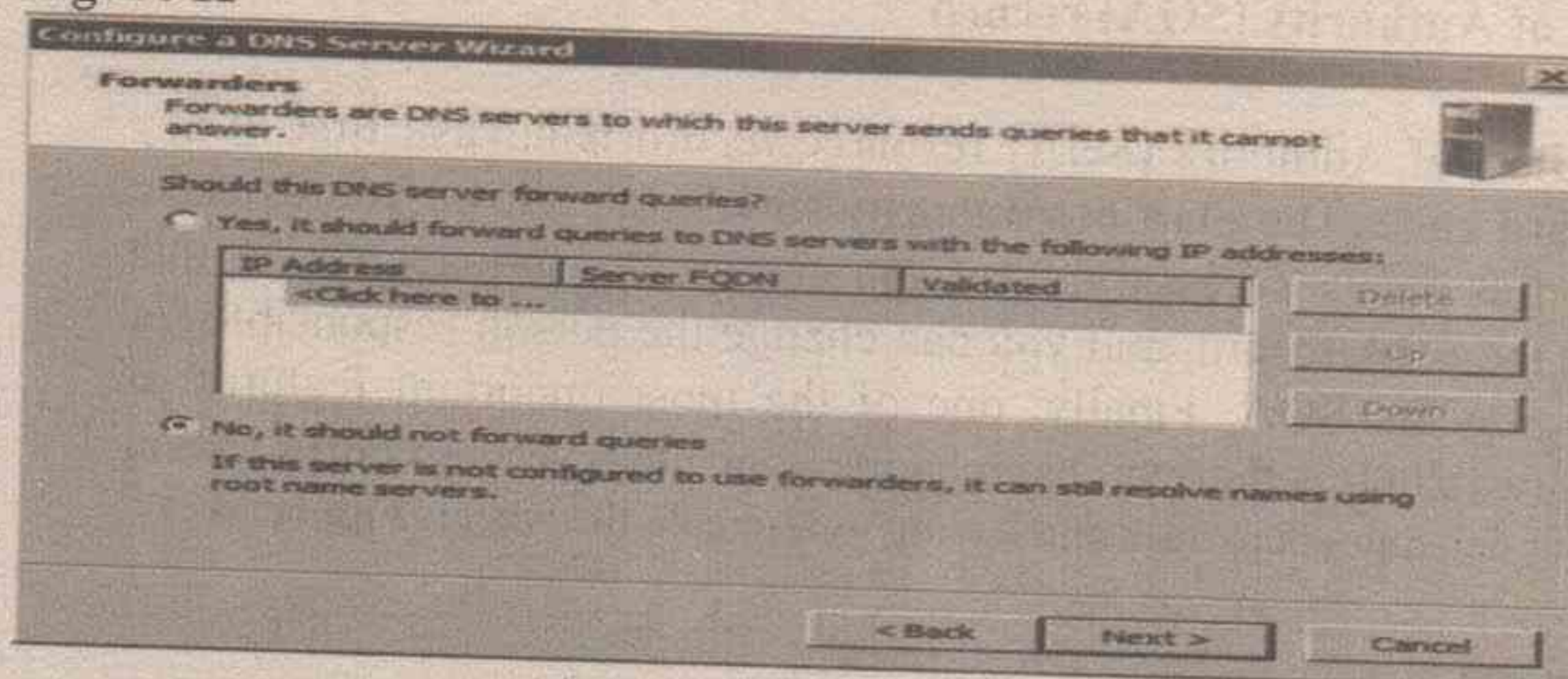
Reverse lookup zone

Figure J



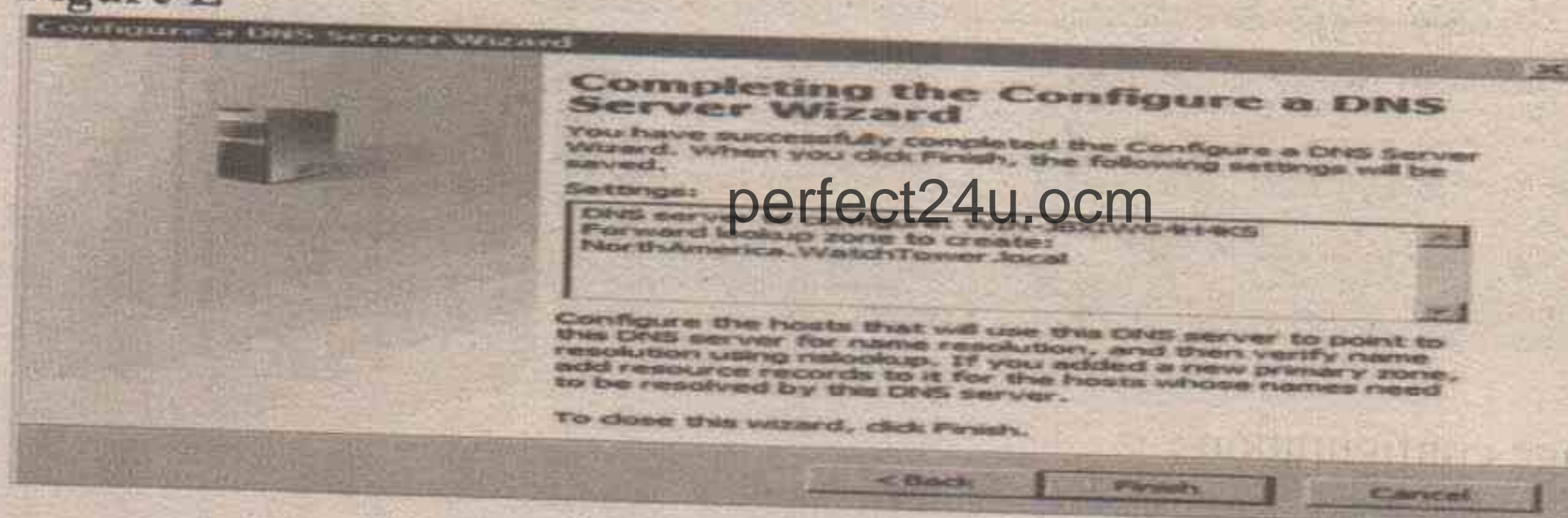
Choose new or existing DNS file

Figure K



Forwarders window

Figure L



Finish

Managing and Trouble Shooting DNS records

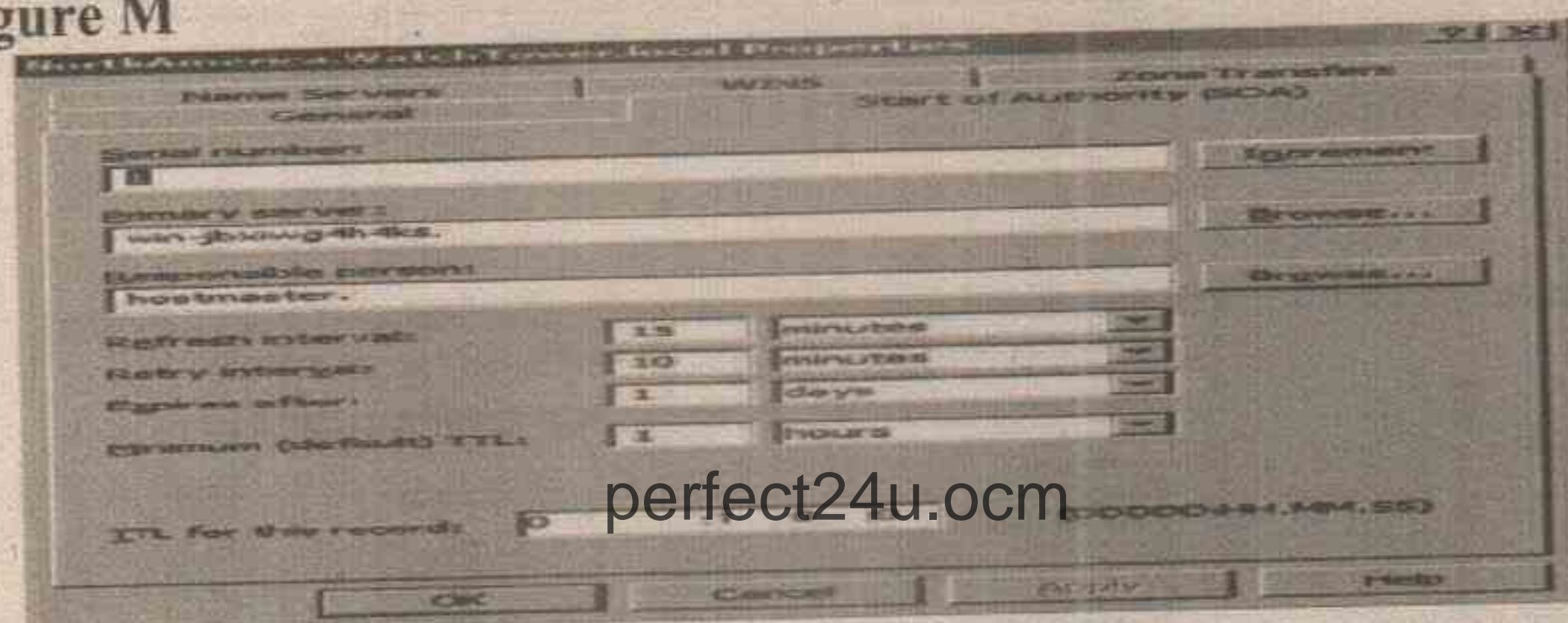
You have now installed and configured your first DNS server, and you're ready to add records to the zone(s) you created. There are various types of DNS records available. Many of them you will never use. We'll be looking at these commonly used DNS records:

- Start of Authority (SOA)
- Name Servers
- Host (A)
- Pointer (PTR)
- Canonical Name (CNAME) or Alias
- Mail Exchange (MX)

Start of Authority (SOA) record

The Start of Authority (SOA) resource record is always first in any standard zone. The Start of Authority (SOA) tab allows you to make any adjustments necessary. You can change the primary server that holds the SOA record, and you can change the person responsible for managing the SOA. Finally, one of the most important features of Windows 2000 is that you can change your DNS server configuration without deleting your zones and having to re-create the wheel (**Figure M**.)

Figure M



Change configuration

Name Servers

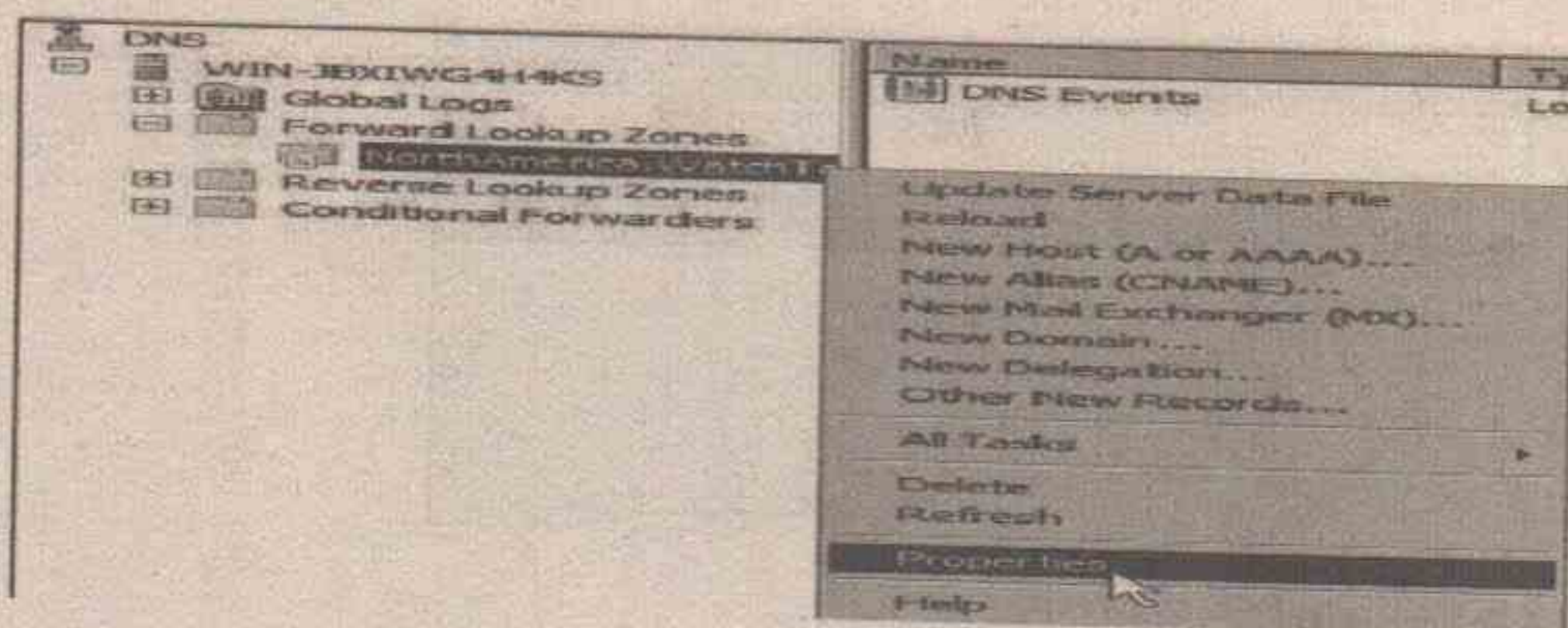
Name Servers specify all name servers for a particular domain. You set up all primary and secondary name servers through this record.

To create a Name Server, follow these steps:

1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Expand the Forward Lookup Zone.
3. Right-click on the appropriate domain and choose Properties (**Figure N**.)
4. Select the Name Servers tab and click Add.
5. Enter the appropriate FQDN Server name and IP address of the DNS server you want to add.

Figure

N



Name Server

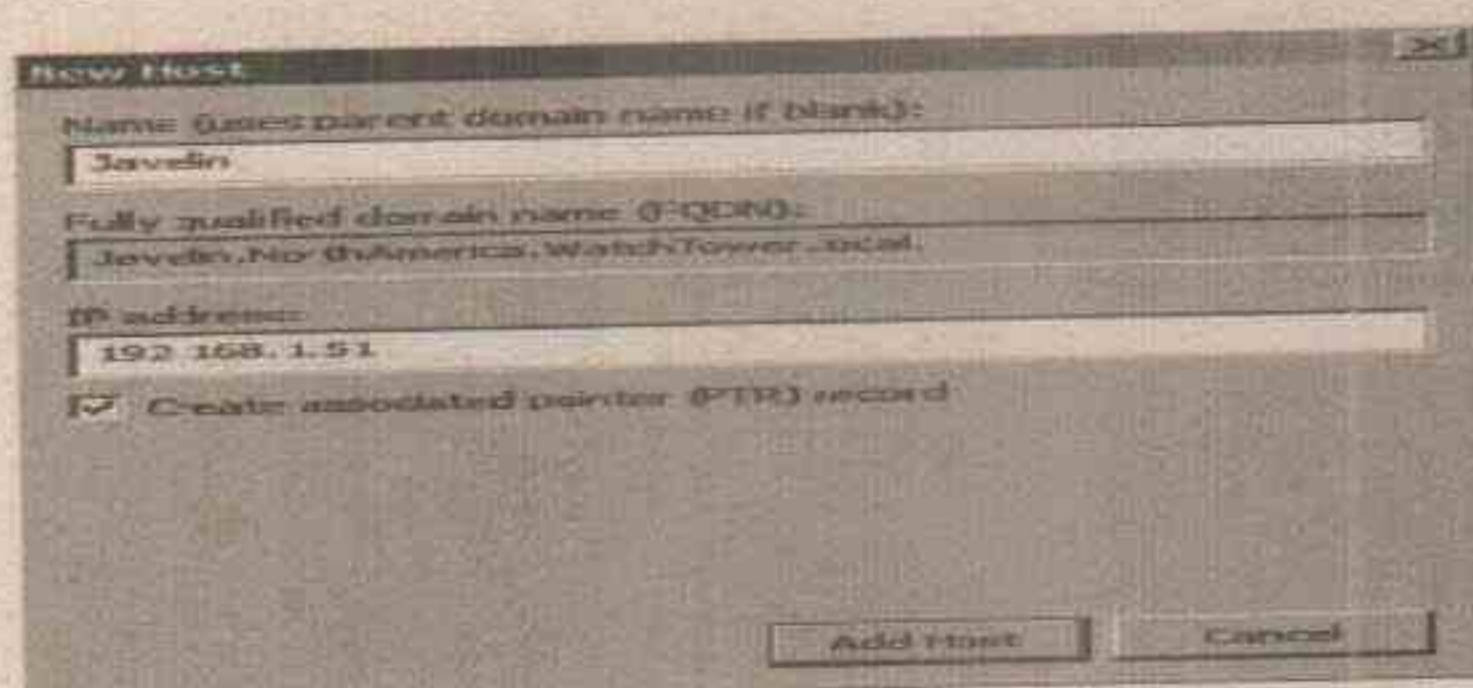
Host (A) records

A Host (A) record maps a host name to an IP address. These records help you easily identify another server in a forward lookup zone. Host records improve query performance in multiple environments, and you can also create a Pointer (PTR) record at the same time. A PTR record resolves an IP address to a host name.

To create a Host record:

1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Expand the Forward Lookup Zone and click on the folder representing your domain.
3. From the Action menu, select New Host.
4. Enter the Name and IP Address of the host you are creating (**Figure O .**)
5. Select the Create Associated Pointer (PTR) Record check box if you want to create the PTR record at the same time. Otherwise, you can create it later.
6. Click the Add Host button.

Figure O



A Host (A) record

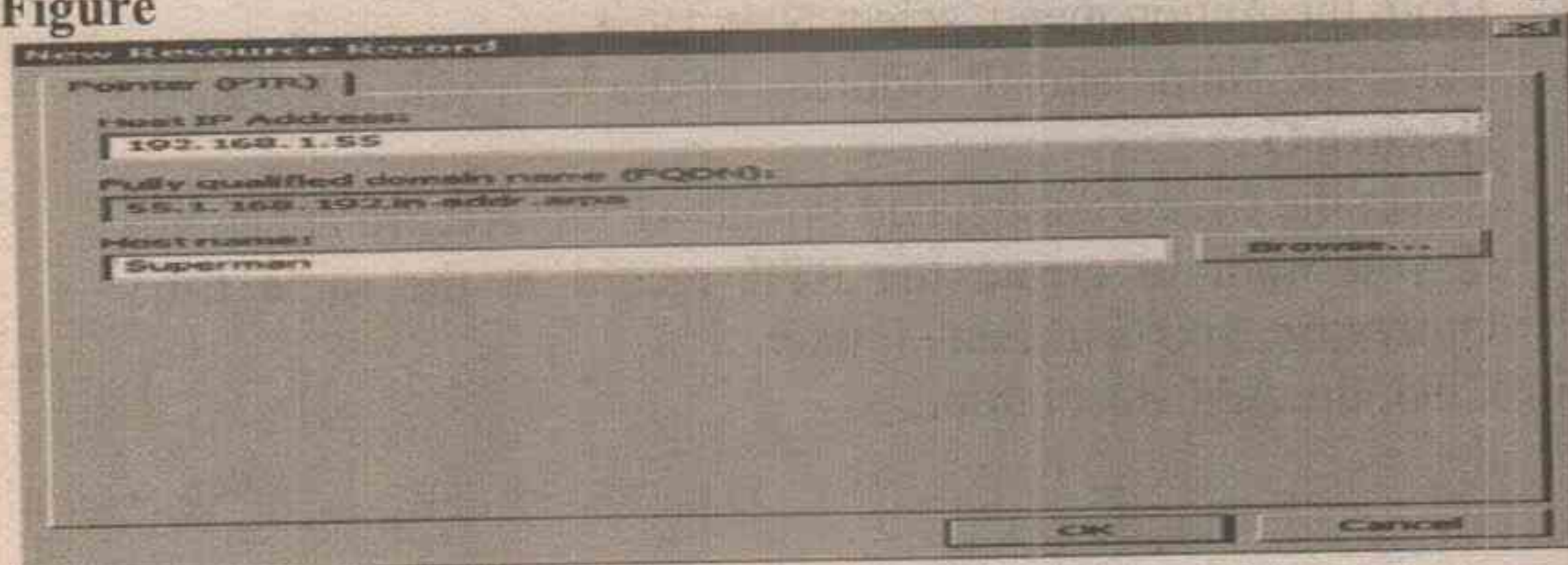
Pointer (PTR) records

A Pointer (PTR) record creates the appropriate entry in the reverse lookup zone for reverse queries. As you saw in Figure H, you have the option of creating a PTR record when creating a Host record. If you did not choose to create your PTR record at that time, you can do it at any point.

To create a PTR record: perfect24u.ocm

1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Choose the reverse lookup zone where you want your PTR record created.
3. From the Action menu, select New Pointer (Figure P.)
4. Enter the Host IP Number and Host Name.
5. Click OK.

Figure



New Pointer

Canonical Name (CNAME) or Alias records

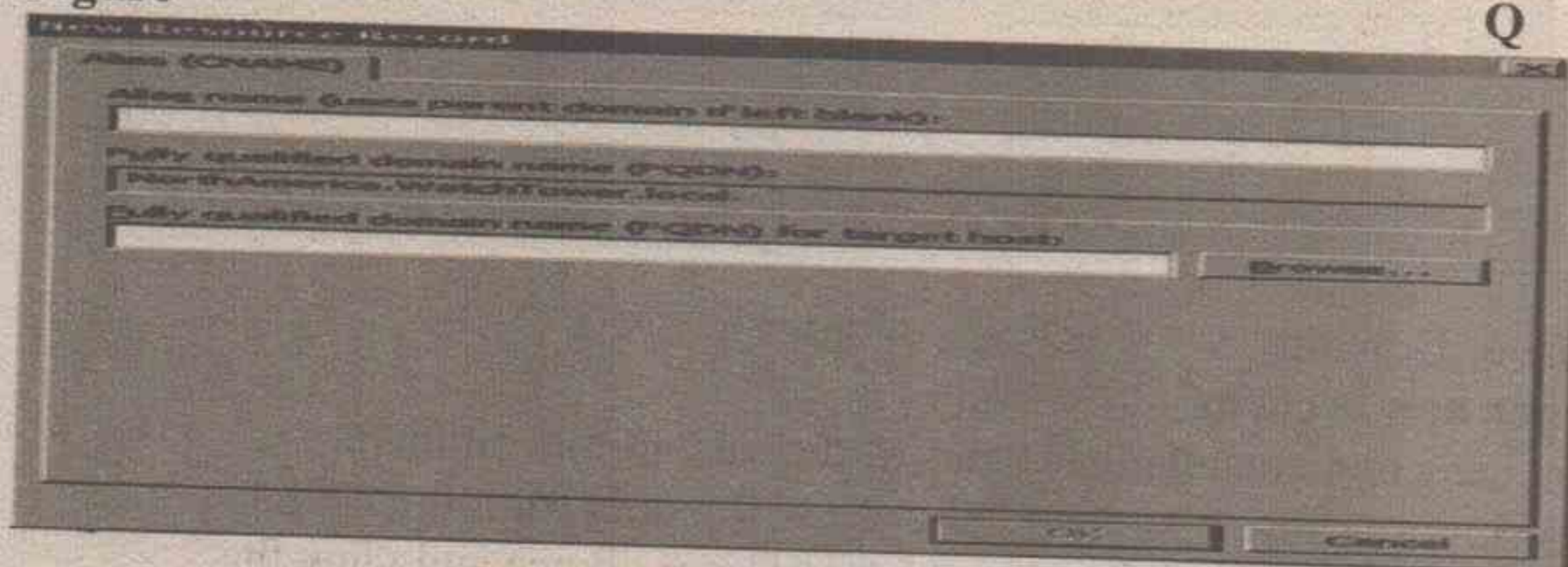
A Canonical Name (CNAME) or Alias record allows a DNS server to have multiple names for a single host. For example, an Alias record can have several records that point to a single server in your environment. This is a common approach if you have both your Web server and your mail server running on the same machine.

To create a DNS Alias:

1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Expand the Forward Lookup Zone and highlight the folder representing your domain.
3. From the Action menu, select New Alias.
4. Enter your Alias Name (**Figure Q .**)
5. Enter the fully qualified domain name (FQDN).
6. Click OK.

perfect24u.ocm

Figure



Alias Name

Mail Exchange (MX) records

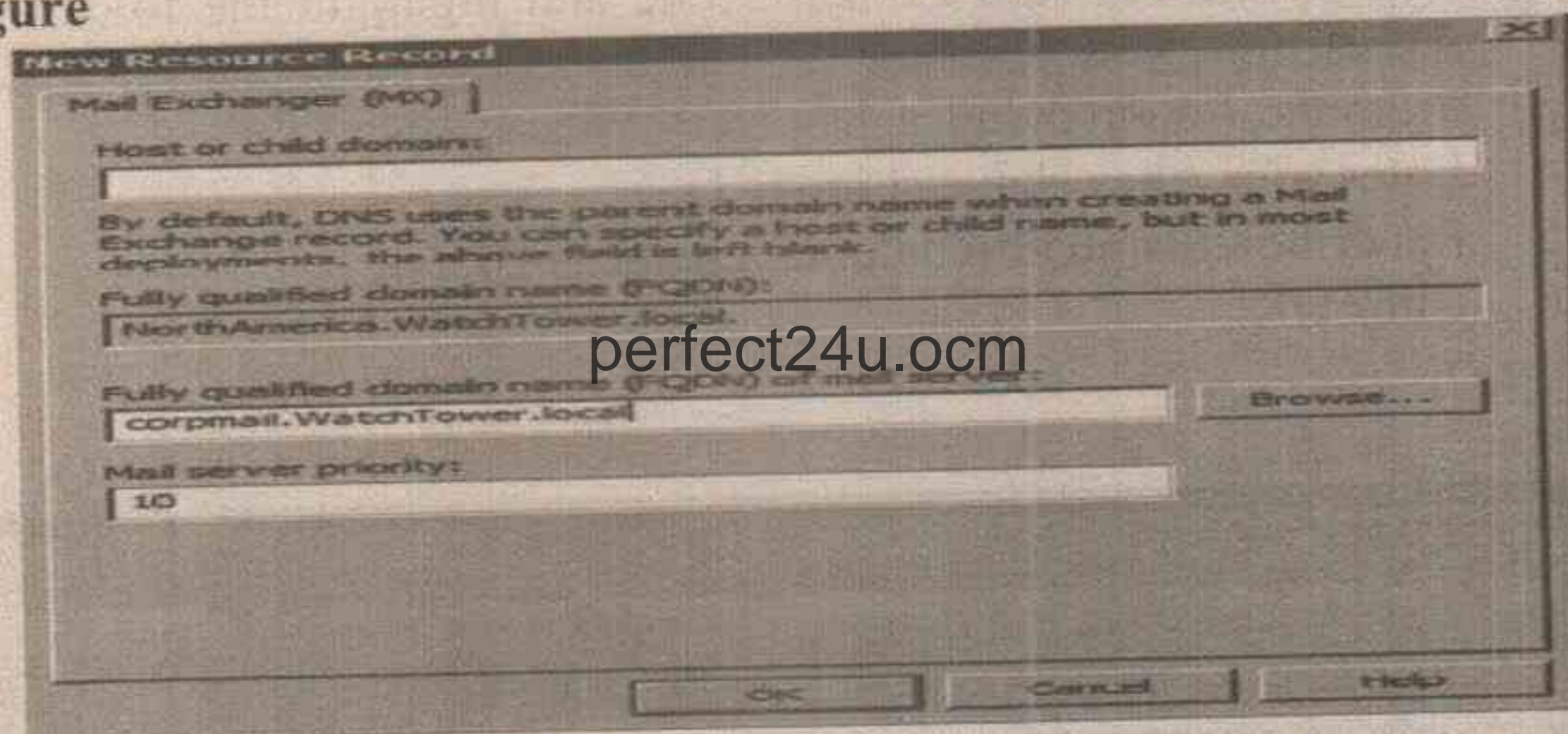
Mail Exchange records help you identify mail servers within a zone in your DNS database. With this feature, you can prioritize which mail servers will receive the highest priority. Creating MX records will help you keep track of the location of all of your mail servers.

To create a Mail Exchange (MX) record:

1. Select DNS from the Administrative Tools folder to open the DNS console.
2. Expand the Forward Lookup Zone and highlight the folder representing your domain.
3. From the Action menu, select New Mail Exchanger.
4. Enter the Host Or Domain (**Figure R.**)
5. Enter the Mail Server and Mail Server Priority.
6. Click OK.

Figure

R



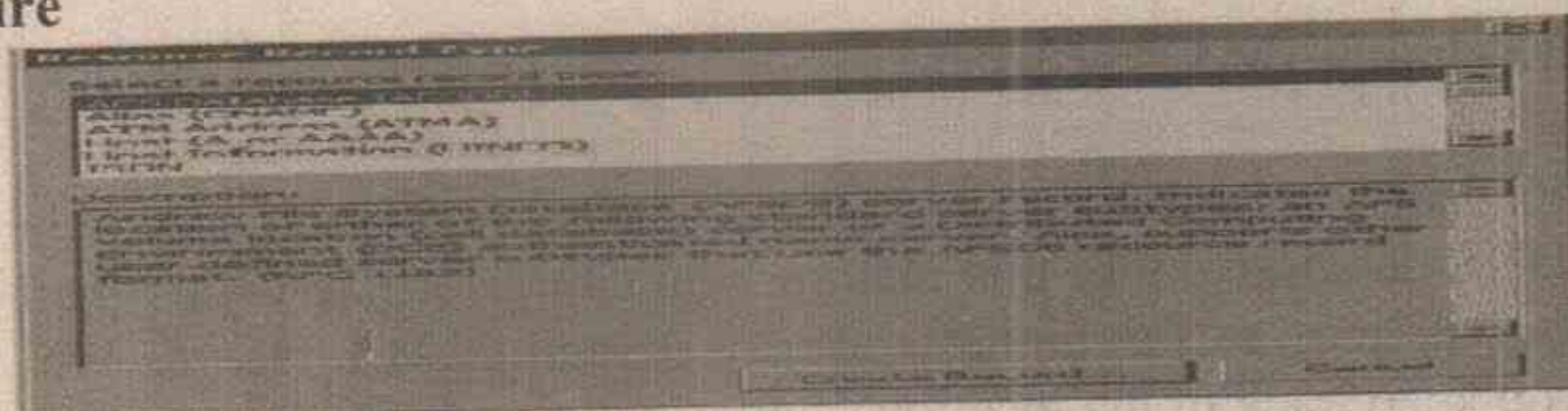
Host or Domain

Other new records

You can create many other types of records. For a complete description, choose Action | Other New Records from the DNS console (**Figure S**). Select the record of your choice and view the description.

Figure

S



Create records from the DNS console

Implement strong passwords

Password policies are a set of rules that can enhance the security of your Windows SBS 2008 network. Using strong password provides an additional layer of defense against an unauthorized user gaining access to your network.

To help implement strong passwords, password policies are enabled by default in Windows SBS 2008 during installation. You can ensure that users implement strong passwords by enforcing password policies in your network.

The password policies in Windows SBS 2008 include the following:

Minimum length Enable this policy to determine the least number of characters that a password can contain. Setting a minimum length helps protect your network by preventing users from having short or blank passwords. The default is eight characters.

Complexity Enable this policy to determine whether passwords must contain different types of characters. If this policy is enabled, passwords cannot contain all or part of a user's account name, and it must contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphanumeric characters (such as , !, \$, #, %)

Maximum age Enable this policy to determine the period of time (in days) that a password can be used before the system requires that the user change it. The default is 180 days.

Educate users

After implementing strong password policies, educate users about strong and weak passwords. Ask users to treat their password as they would private information, such as a credit card personal identification number (PIN).

Following are typical guidelines for creating a strong password. When implemented, they provide protection for your local network.

A password should not include any of the following:

- All or part of the user's account name.
- User's name or e-mail alias.
- Name of the user's child, parent, spouse/partner, or friend.
- Any word found in a dictionary.
- Old password that is reused by appending numbers.
- User's birth date.
- User's phone number.
- User's Social Security Number or other identification number.

Any easily obtained personal information (for example, a city of birth).

A strong password consists of the following:

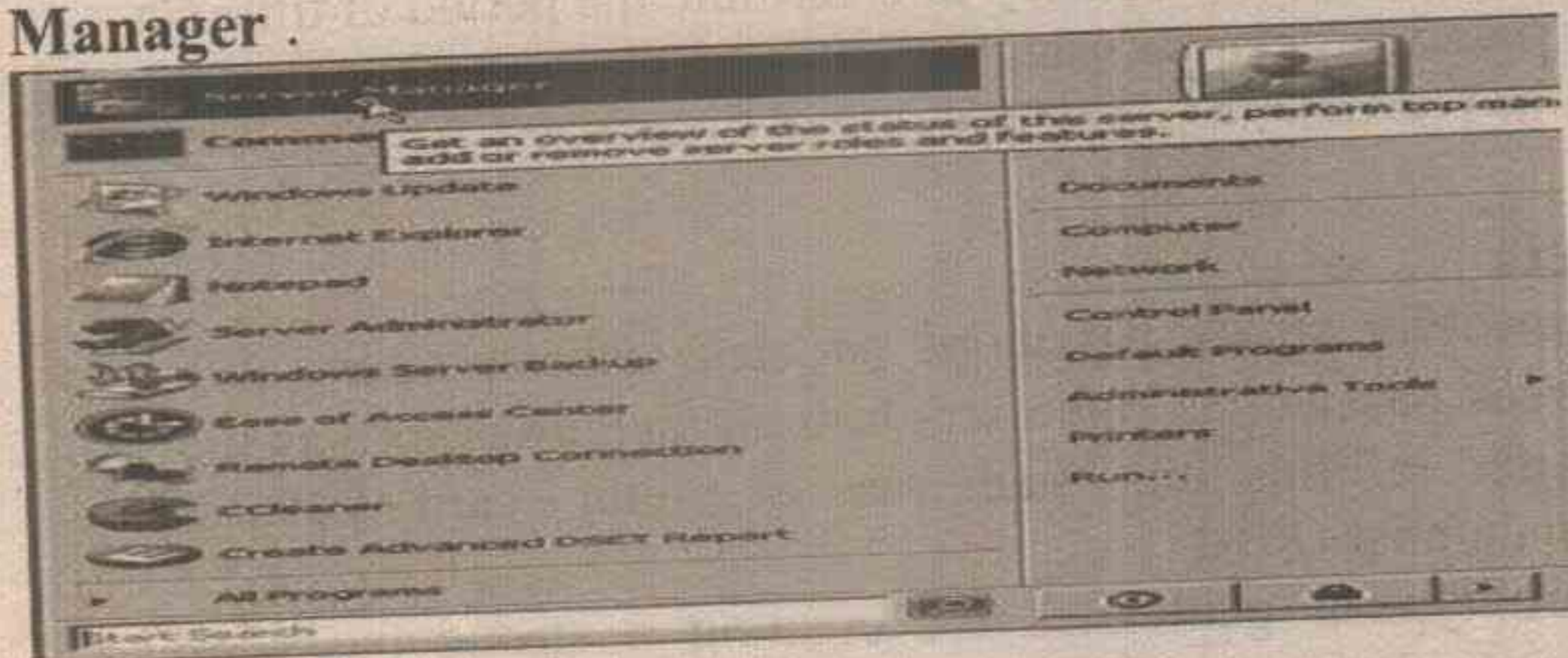
- At least eight characters.
- Characters from three of the following four categories:
- Uppercase letters (A through Z)
- Lowercase letters (a through z)
- Numbers (0 through 9)
- Non-alphanumeric characters (for example, !, \$, #,)%

BACKUP WITH WINDOWS SERVER 2008

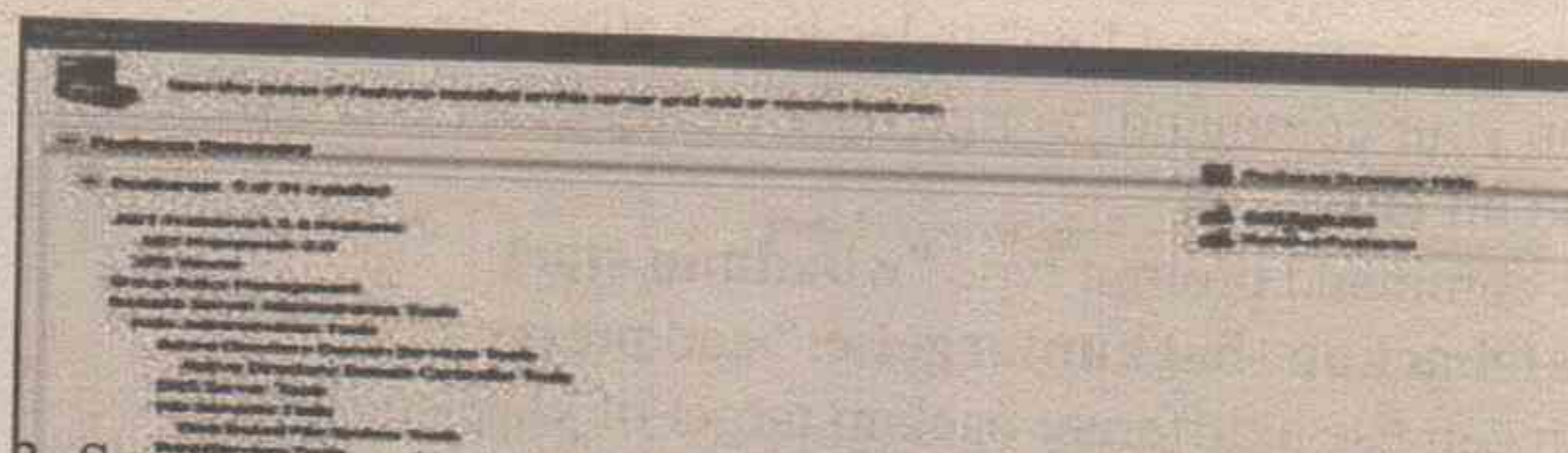
Planning Backup Policy on Windows Server 2008

Before you can backup Server 2008 you need to install the backup features from the Server Manager.

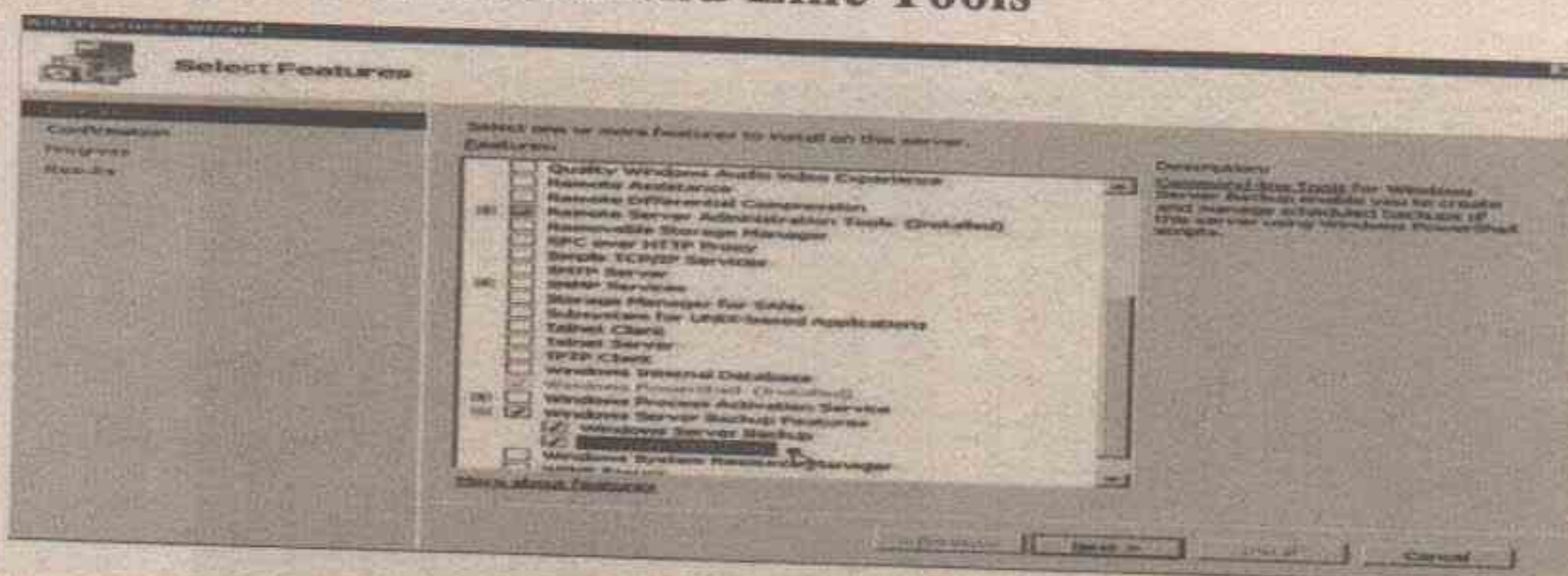
1. To install the **backup** features click **Start → Server Manager**.



2. Next click **Features → Add Features**



B. Scroll to the bottom and select both the **Windows Server Backup** and the **Command Line Tools**



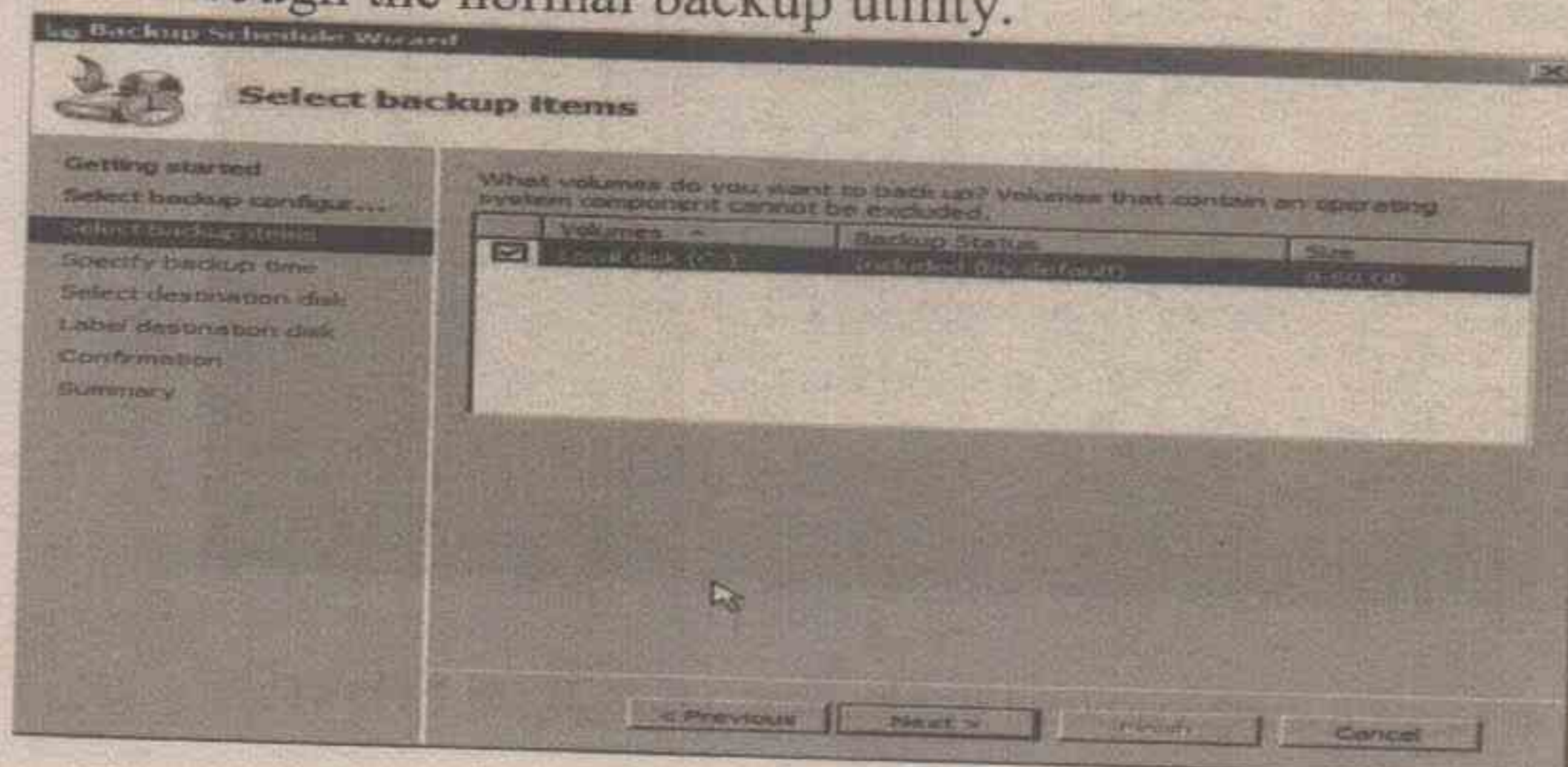
perfect24u.ocm

4. Click **Next**, then click **Install**

BACKING UP SERVER 2008 ACTIVE DIRECTORY

Now that we have the backup features installed we need to backup Active Directory.

In Server 2008, there is no option to backup the System State data through the normal backup utility.



We need to go "command line" to backup Active Directory.

1. Open up your command prompt by clicking **Start** and type "**cmd**" and hit **enter**.

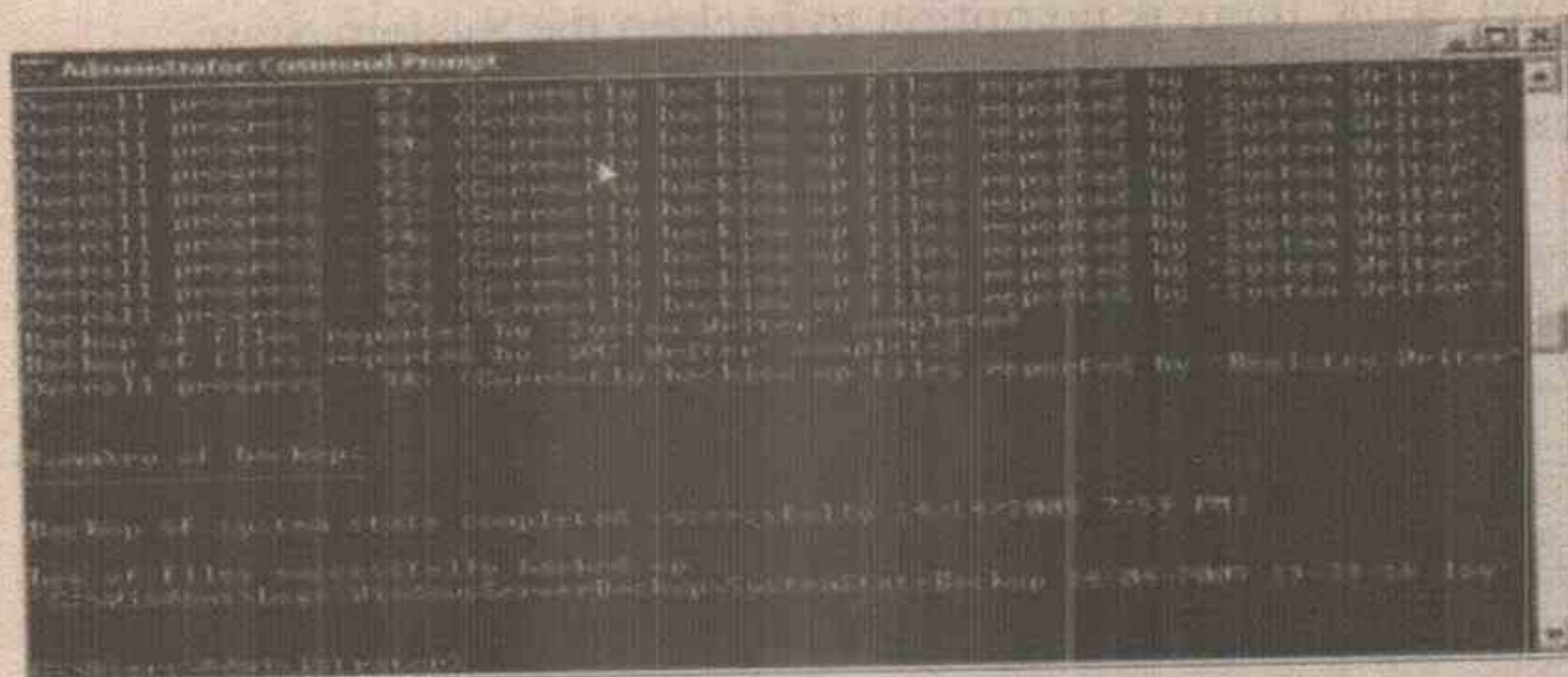
2. In your command prompt type "**wbadmin start systemstatebackup -backuptarget:e:**" and press enter.

Note: You can use a different backup target of your choosing

3. Type "**y**" and press enter to start the backup process.



When the backup is finished running you should get a message that the backup completed successfully. If it did not complete properly you will need to troubleshoot.



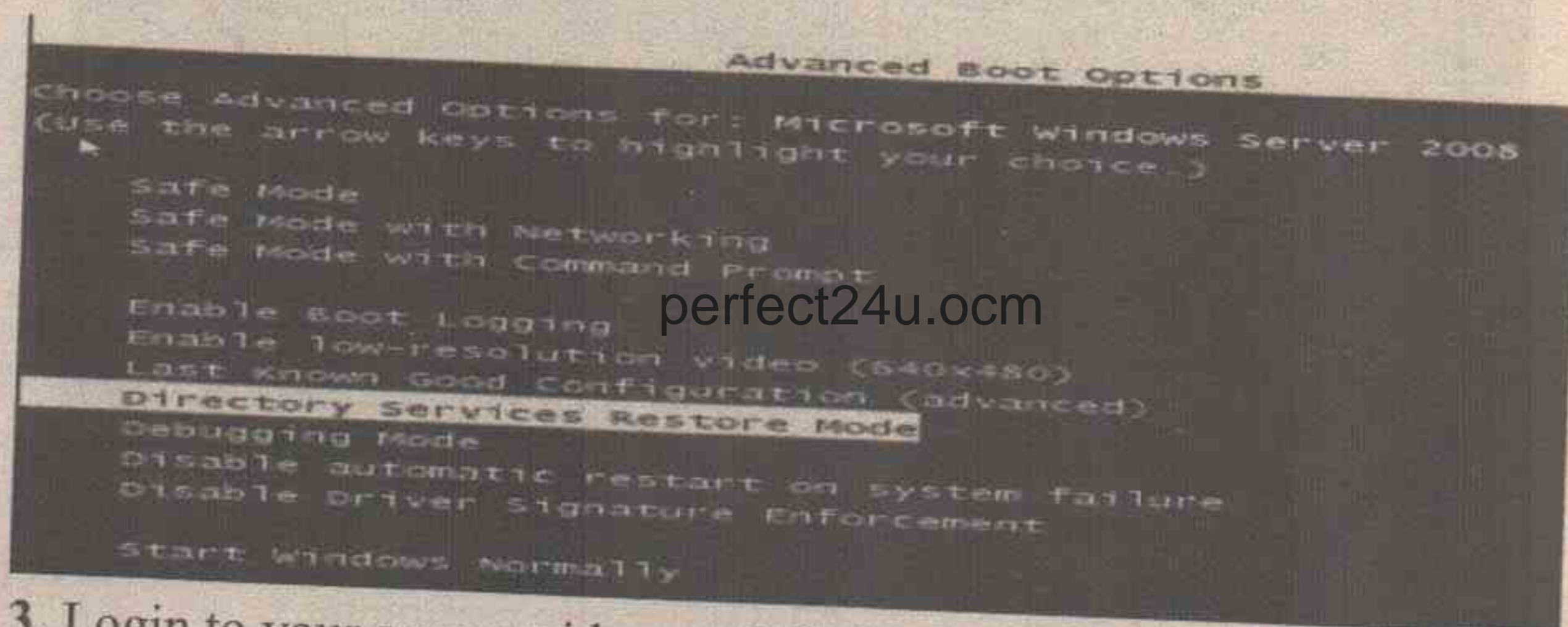
.Now you have a system state backup of your 2008 Server!

PLANNING A SERVER RESTORE POLICY

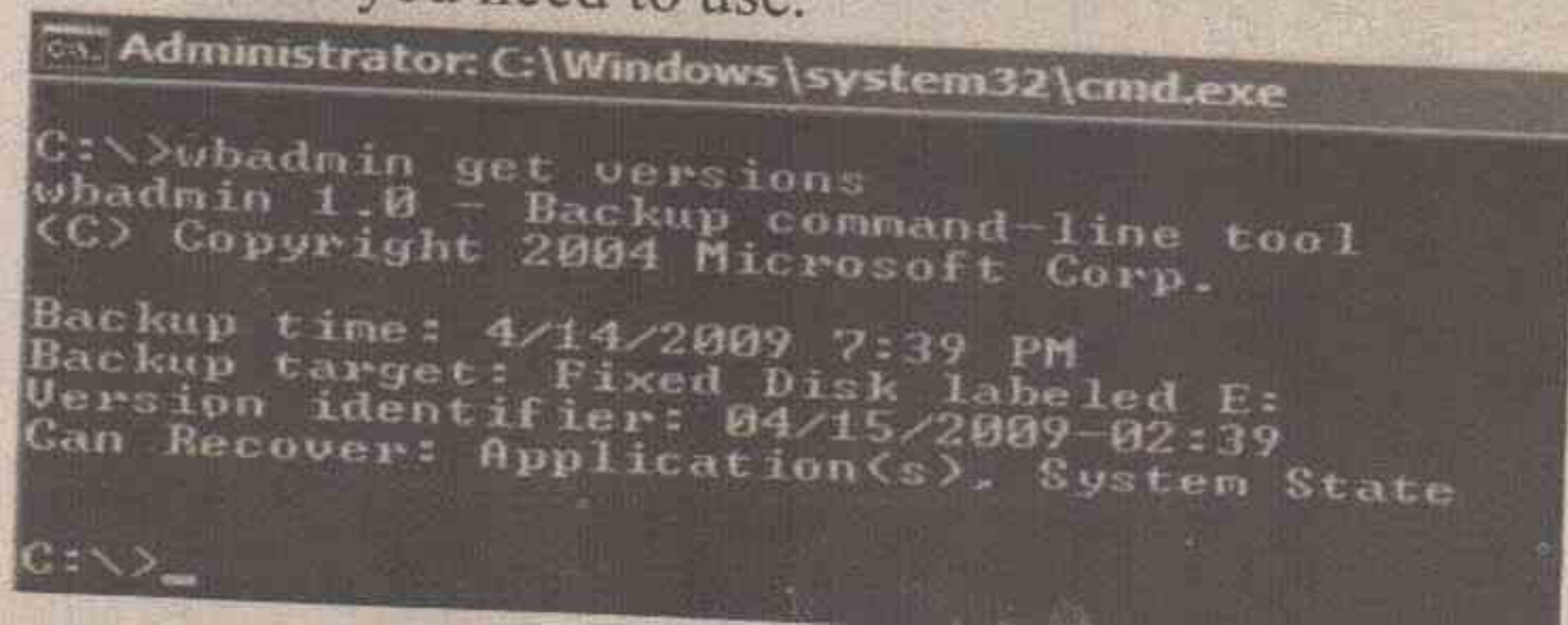
Authoritative Restore of Active Directory

If you accidentally delete an OU, group, or a user account and it's already replicated to your other servers. We will need to perform an authoritative restore of the Active Directory object you accidentally deleted.

1. To do this you will need to boot into DSRM (Directory Services Restore Mode) by restarting your server and pressing F8 during the restart.
2. Choose **Directory Services Restore Mode** from the Advanced Boot menu.



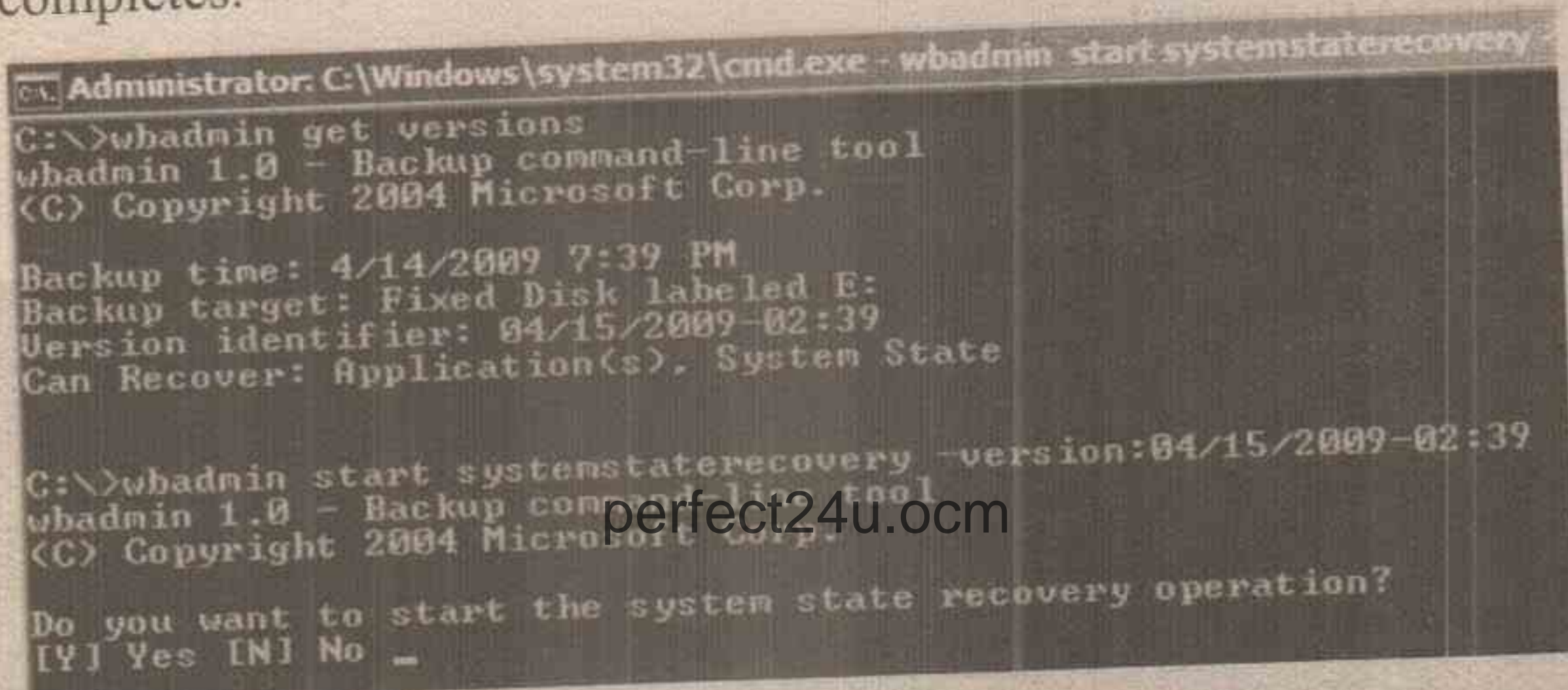
3. Login to your server with your DSRM password you created during Active Directory installation.
4. Once you're logged into your server and in DSRM safe mode, open a command prompt by clicking **Start**, type "**cmd**", and press enter.
5. To make sure you restore the correct backup it's a good idea to use the "**wbadmin get versions**" command and write down the version you need to use.



6. Now we need to perform a non-authoritative restore of Active Directory by typing "**wbadmin start systemstaterecovery -version:04/14/2009-02:39**".

Note: The version of backup will vary depending on your situation. Type "y" and press enter to start the non authoritative restore.

7. Go grab some coffee and take a break while the restore completes.



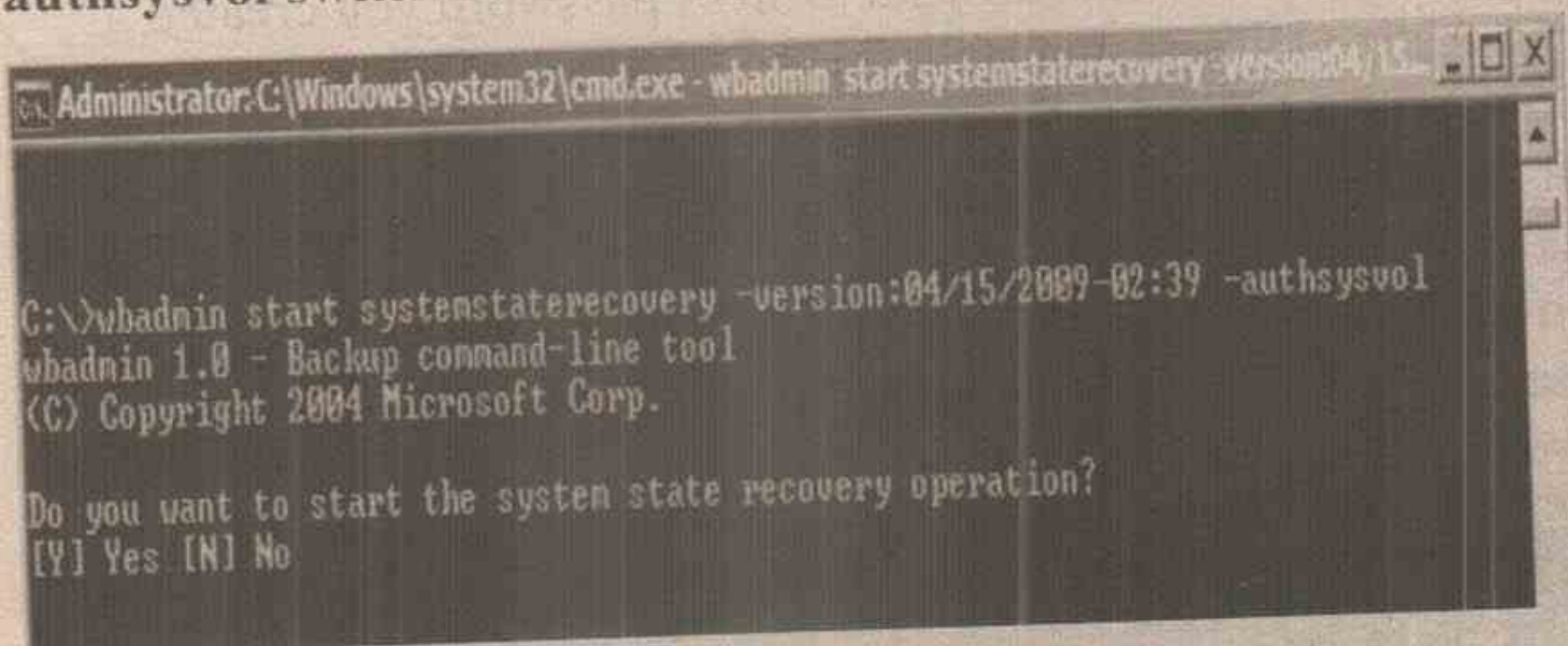
```
Administrator: C:\Windows\system32\cmd.exe - wbadmin start systemstaterecovery
C:\>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Backup time: 4/14/2009 7:39 PM
Backup target: Fixed Disk labeled E:
Version identifier: 04/15/2009-02:39
Can Recover: Application(s), System State

C:\>wbadmin start systemstaterecovery -version:04/15/2009-02:39
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Do you want to start the system state recovery operation?
[Y] Yes [N] No _
```

8. You can mark the sysvol as authoritative by adding the **authsysvol** switch to the end of the wbadmin command.



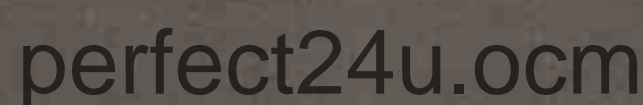
```
Administrator: C:\Windows\system32\cmd.exe - wbadmin start systemstaterecovery -version:04/15/2009-02:39 -authsysvol
C:\>wbadmin start systemstaterecovery -version:04/15/2009-02:39 -authsysvol
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Do you want to start the system state recovery operation?
[Y] Yes [N] No
```

9. But if you want to restore a specific Active Directory object then you can use the ever familiar ntdsutil.

For this example we are going to restore a user account with a distinguished name of **CN=Test**


```
restore object "cn=Test User,cn=Users,dc=home,dc=local"
```



10. Reboot your server into normal mode and you're finished. The object will be marked as authoritative and replicate to the rest of your domain.

HISTORY OF LINUX

In August 1991, A student from university of Helsinki in Finland began a post to the Comp.os.minix, news group with word "Hello every body out there using minix, I am doing a free operating System (Just a hobby, won't be big and professional like GNU) for 386(486) at colons. Name Linus Torvalds," The hobby he spoke of eventually become what we know today LINUX

At that time UNIX and other operating systems was costly then PC hardware. While versions of UNIX have long been available for PC's. They never had the grace of power of operating system available for mini computers, mainframes and today servers. This lack of accessing ultimately give birth to LINUX as a means to make a UNIX like operating system available on wide spread basis.

Today's Linux was developed with the assistance of programmer's word wide; Linus Torvalds still retains control of evolving core of Linux operating system. In march 1992, version 1.0 of the Kernel was first official release of Linux.

MAIN FEATURES AND ADVANTAGES OF LINUX

Linux system offers many salient features, for example

1) MULTITASKING CAPABILITY

Full multitasking and 32-bit support. Linux, is a real multitasking system, allowing multiple users to run many programs on the same system at once.

2) MULTIUSER CAPABILITY

Multiuser operating system permits several users to use the same computer to carry out their computing jobs. can run programs, access files and print documents at the same time.

3) SYSTEM PORTABILITY

Linux has this outstanding feature that it is not written for specific hardware platforms. It can be ported to another system (installation) without the need to make any major changes.

4) SYSTEM SECURITY

Several levels of security exist in Linux.

First level is system security is A login is simply the name that you supply to Linux to identify yourself to the operating system. Linux keeps track of which names are permitted to log in or access the system, and only allows valid users to have access.

a- Another level of security is when it comes to accessing files.

Three permissions "Read, Write and Execute" can be assigned by the owner of the file to each of his files. All of these permissions can be individually either granted or denied to all the users of the system.

b- Third level of security allows users to encrypt data files on the disk so that even if someone manage to access then he can't make much sense of it.

5. LINUX APPLICATION

a. Text and word processing application

In addition to commercial word processing software's such as Word perfect, star office, appixware, Linux offers powerful tools for editing text files and processing text in an automated fashion.

b. Programming Languages

There is a wide variety of programming and scripting languages & tools available for Linux

c. Internet tools

In addition to supporting Well-Known software such as Netscape Communicator and Mosaic, Linux provide wide verity of internet software and full range of software needed to create internet services such as Web Server, Mail Server plus complete network support to connect to the internet via Local network or modem

d. Databases

Linux provide robust platform for running client server database application such as free database mSQL and postgre available for Linux also commercial database such as Oracle, Sybase and Informix

6. DOS and Window compatibility

Linux can run DOS software with a high degree of stability and compatibility and offers several approaches to run Windows software, Wabi, Wine, VM ware

7. Linux is free Software

Linux kernel and most of the applications written for Linux are available for free on the Internet, often with no restriction on the copying and redistribution of the software.

8. Virtual memory and shared libraries.

Linux can use a portion of your hard drive as virtual memory, expanding your total amount of available RAM. Linux also implements shared libraries, allowing programs that use standard subroutines to find the code for these subroutines in the libraries at runtime. This saves a large amount of space on your system;

9. Linux supports (almost) all of the features of commercial versions of UNIX.

In fact, some of the features found in Linux may not be available on other proprietary UNIX systems

10. GNU software support (Free Software's).

Linux supports a wide range of free software written by the GNU Project, including utilities such as the GNU C and C++ compiler, gawk, groff, and so on. Many of the essential system utilities used by Linux are GNU software

11. Built-in support for networking, multitasking, and other features

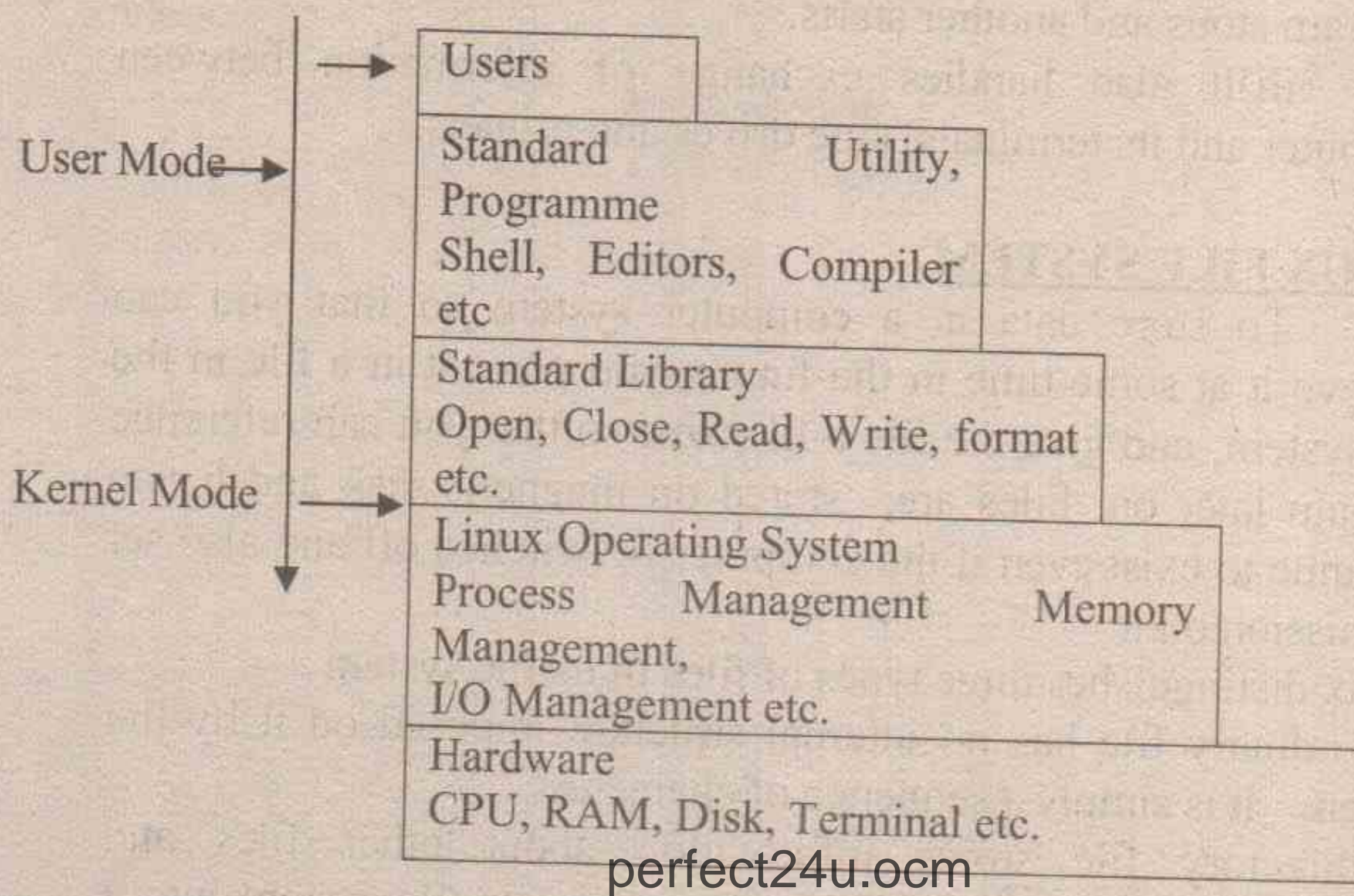
12. X Windows System. The X Window convert text base Linux to graphics Operating system A complete version of the X Window System, known as XFree86, is available for Linux. The X Window System is a very powerful graphics interface, supporting many applications

Hardware Requirement

You can run an entire system from a single, high-density 5.25-inch floppy. but Hardware requirement depends upon Linux software & accessories selection.

Component	Minimum	Good Pc
Processor	386	Pentium 133
RAM	4 MB	32 -64 MB
Hard disk	150 MB	1GB
Display VGA, Mouse, CD-ROM Etc	-	-

STRUCTURE OF THE LINUX SYSTEM



Linux Tools and Applications:

The outermost layer of the Linux operating system is its tools and applications. These tools can be invoked from the command line itself and help perform the day-to-day as well as complex tasks of the system.

The Shell:

It is the command interpreter of the operating system. It accepts commands from users and analyses and interprets these commands.

The Linux Kernel:

It is the core of the system. It controls all the tasks, schedules all the processes and carries out all the crucial functions of the operating system. All operating systems have a kernel that contains thousands of routines to carry out the numerous tasks that the operating system has to handle. The major duties of the kernel are as under:

- i) To keep track of the programs that are executing

ii) All processor time to each and also decide when one program stops and another starts.

iii) It also handles exchange of information between computer and its terminals, tape drives and printers.

LINUX FILE SYSTEM

To store data in a computer system so that you can retrieve it at some time in the future, you place it in a file in the file system and give the file a filename so that you can reference it again later on. Files are stored on magnetic disk and hence continue to exist even if the computer is switched off and also set permission on it.

Linux distinguishes three types of files in its file system –

An ordinary file has no internal structure imposed on it by the system - it is simply a sequence of characters.

A directory file stores information about other files and directories. This enables Linux to organize its file system into a hierarchy of files and directories.

The special files are the input/output devices attached to a particular computer system.

Important Directories in the Linux File System

Most of the directories that hold Linux system files are "standard." some of the most important directories on your Linux system.

/ This is the root directory. It holds the actual Linux program, as well as subdirectories. Do not store your own files here.

/home This directory holds users' home directories. After logging to the system this is PWD for a user.

/bin This directory holds many of the basic Linux programs. bin stands for binaries, files that are executable and that hold text only computers could understand.

/usr This directory holds many other user-oriented directories. Like games, help files

/dev Linux treats everything as a file! The **/dev** directory holds devices. These are special files that serve as gateways to physical computer components. For instance, if you copy to **/dev/fd0**, you're actually sending data to the system's floppy disk. Your terminal is one of the **/dev/tty** files. Partitions on the hard drive are of the form **/dev/hd0**. Even the system's memory is a device!

/usr/sbin This directory holds system administration files. If you do an **ls -l**, you see that you must be the owner, root, to run these commands.

/sbin This directory holds system files that are usually run automatically by the Linux system.

/etc This directory and its subdirectories hold many of the Linux configuration files. These files are usually text, and they can be edited to change the system's configuration.

File and Directories:

A file as a container of information. Once information is stored in a file, it will remain there until it is changed or the file is removed from the system.

A Linux allows filenames to be up to 256 characters long. These characters can be lower- and uppercase letters, numbers, and other characters, usually the dash (-), the underscore (_), and the dot (.).

DIRECTORY

A directory is simply a file that contains the names of other files and information about how to locate them. There is no limit imposed by Linux on the number of levels of sub-directories that may be created by a user.

HOME DIRECTORY:

Whenever a new user is created in the Linux system to use Linux, a directory is created for that user which has a unique name. This directory is called the home directory. When you login successfully, Linux makes your home directory the current directory and you are then ready to begin your session. You can

create, modify and delete files; you can also make and remove sub-directories.

File naming Rules:

- 1) A filename must be 1 to 255 characters long.
- 2) All characters are legal except (/) which is used for separating directory levels and files.
- 3) Spaces and tabs must be quoted if used as a part of filename. Avoid using following characters:

(?	*	&	^	\$	#	@
)	[]	{	}	,	"	<
/	\		;	'			>
	space	Tab	Esc	Ctrl-characters			

- 4) A (.) at the beginning of a filename hides it from ls command.
- 5) Upper and lower case characters are interpreted differently. TMP is different from tmp.
- 6) Do not use following at beginning of filename:

+ - = _

Wildcards:

*It matches any string with zero or more characters.

? It matches any single character.

[characters] It matches any one of the character enclosed in [] c1-c2 will match characters c1 through c2

![characters] It matches any one of characters not enclosed in .] [

Examples using wildcards:

1. ls *.db It displays all files ending with .db
2. ls [0-9]* It displays all files beginning with a number
3. ls [!0-9]* It displays all files not beginning with a number
4. ls *. [bdfg] It displays all files ending with characters b, d, f or g
5. ls !(m*) It displays all files not beginning with m

The Shell:

It is the command interpreter of the operating system. It accepts commands from users and analyses and interprets these commands. Most of the Linux commands are executable C

programs. Shell interprets user command and starts executing appropriate executable file. It then request kernel to carry out actual transfer of data which finally leads to output that is displayed on the screen of the terminal. Shell acts as middle man between kernel and user of the operating system. These shells are mainly used with Linux:

1) **Bourne Shell (sh):**

This is one of the most widely used shells in the Linux world. It was developed by Steve Bourne of AT&T Bell Laboratories in the late 1970's. It is the primary Linux command interpreter and comes along with every Unix system. It introduced many shell concepts such as the ability to test program for success of failure status, allows for sophisticated scripting (Programming) but lack of features such as history list and command line editing. The prompt used by the Bourne shell in the Linux installation is shown by a (\$) dollar sign.

2) **C Shell (Csh):**

The C shell was developed by Bill Joy at the University of California at Berkeley. The C shell is the default shell in the Berkeley version of Unix. It has a few principal advantages over the Bourne shell.

(i) A history mechanism: The C shell remembers the commands that the user types and allows him to recall them without having to retype them.

Aliasing: The C shell permits you to call frequently used commands by your own formulated abbreviations. This is a type of "macro" facility that is available at the command line.

Arithmetic calculation and comparison ,testing can be performed by the shell itself.

3) **Korn Shell (Ksh):**

Developed by David Korn at AT&T, this shell was designed to be much bigger than the Bourne shell and includes several features that make it more superior. It includes all the enhancement of C

shell like command history and aliasing and offers a few more features itself which makes it more efficient than the Bourne shell.

4) Bourne Again Shell (Bash)

it is the most common shell installed with Linux Distribution. It is based on Bourne Shell and provides additional feature set including command line editing . a history list and filename completion and allow to write sophisticated shell scripts using Bourne Shell like syntax

What is Distribution?

Distribution is different sets of applications, utilities, tools and drivers modules are built on same versions of Kernel (the heart of the Operating System), can include and can offer different installation and upgrade programmes to ease management of the system.

As windows 98 or Windows NT defines the complete set of windows utilities applications, and drivers that Microsoft ships. There is no room for variation in any application, drivers or Utility

But Linux has opened the door to different flavors of Linux meet differed need. On the same Kernel version they allow to add are remove applications, derivers and utility and allow to redistribute their product. Hence each product are called Distribution

Following are the different types of Distributions.

1. Red Hat

Red Hat Linux distribution from Red Hat Software (www.redhat.com) has emerged as the favorite Linux distribution for most users. Red Hat gained fame for its tools for installation and upgrading the operating system. It introduce GNOME Desktop some feature are Improve installation, improved Administration Tools like LinuxConfig, Xconfigurator, GNOME Desktop environment for X Windows,

improved performance features like Symmetrical Multiprocessing and offer different RAID Techniques .

2.

3. Slack ware

Before Red Hat Linux come to fame, slack ware was the distribution to beat but still a popular distribution and found on (www.slackware.com) the distribution offers the full Range of expected utilities, tools, applications, including X windows, development tools such as GNU computers Full Java Support and Java SDK for Linux. It can be downloaded Walnut Creek FTP site (<ftp.cdram.com>)

4. Debian.

Debian has no commercial organization backing it. It is produced by a team of volunteers. Debian offer more than 1000 software packages and published their bugs on website (www.debian.org). It is offer free distribution redistribution right, available source code.

5. Caldera open Linux.

This distribution can be downloaded at no cost from Caldera Website at (www.calerasystems.com). It include K desktop environment and non commercial Star office for Linux, Word Perfect 6 for Linux Netware support and licence of DR-DOS for Dos compatibility.

Installing Linux(Redhat)

Step by Step guide to installing Redhat

Screen 1 If you have booted your system with the Redhat installation media or are installing by NFS you will see the Redhat welcome screen. Press *enter* for install in graphical mode.

Screen 2 Press *next*

Screen 3 for language select English

Screen 4 Keyboard type. Choose *US International*

Screen 5 Mouse type. Select your mouse type here and, if you are going to use this system as a desktop, enable the *emulate 3 buttons* check box.

Screen 6 Installation type. Choose *Custom*

Screen 7 Disk Partitioning. Choose *Manually with Disk Druid*

Screen 8 Disk Setup. Delete all existing partitions

(WARNING: ALL Data currently on the disk is erased!)

Depending on your needs, create new partitions. for simplicity, creating two partitions, one for use as swap which I make twice as large as the amount of physical RAM and one for all other data, called a root partition. Here's how;

Select *new* then enter the following into the pop-up box;

file system type *swap*

size (*2x RAM*) e.g. 64

then *OK*

then;

Select *new*

enter the following into the pop-up box;

Mount Point /

File system type *EXT3*

and click the *Fill to maximum allowable size* checkbox

then click *OK*

You should now have two visible partitions, called */dev/hda1* and */dev/hda2* underneath the */dev/hda* entry. One will be type *EXT3* and one will be type *swap*.

At this stage we have finished configuring partitions. Click *next* to go to the next screen.

Screen 9 Boot Loader. Grub is the preferred boot loader and the default options are suitable, so nothing needs to be changed here. Click *next*.

Screen 10 Network configuration. You will see a list of your network interfaces (such as *eth0*). Configure each one to suit

your own physical network requirements, here we don't use DHCP for wired machines so we select to configure *manually* and enter the IP information in the box provided.

Note that your wireless card probably has not been detected by this stage. Don't worry we'll configure it later.

Screen 11 Firewall configuration. If you intend to run NoCat your entries here will be superseded by the NoCat configuration process. For the purpose of the initail configuration, select *Medium* security level and *ETH0* as a *trusted device*. Allow Incoming *ssh*.

Screen 12 Additional Language Support. Select Other language from the list and uncheck *English (USA)*

Screen 13 Time zone. Click on the map of pakistan to set the time zone.

Screen 14 Root password. This screen where we set the password for the super-user. Create a root password that you will remember. Click *OK* then *Next*

Screen 15 Authentication Configuration. The default settings don't need to be changed. Click *Next*.

Screen 16 Package selection. The packages you chose here will depend on what you want to do with your system, so the recommendations we make below are guidelines. Anything that you omit here but need later can be installed at a later stage. Here it is section by section;

In **Editors** *Emacs* can be removed and *vim-enhanced* can be added

In **Graphical Internet** *evolution*, *gaim*, *mozilla-mail*, *pan* and *xchat* can be removed.

In **Office/Productivity** *mrproject* and *openoffice* can be removed.

In **Sound and Video** Any selected packages in this section can be removed.

In **Graphics** *gimp*, *gimp-data-extras*, *gtkam*, *sane-frontends*, *xsane* and *xsane-gimp* can be removed.

In **Server Configuration Tools** select all of the GUI configuration tools you require for the various services you intend to have on the box. You may find *redhat-config-bind*, *redhat-config-httpd*, *redhat-config-network* and *redhat-config-services* useful.

In **Web server** select all that are applicable for your situation if you intend to use this system as a web server in addition to an Access Point. For use with NoCat you will need *mod_perl* and *mod_ssl*

In **Network Servers** Select all of the services you wish to run. For our Access Point we need *ZEBRA* and *DHCP* *cipe*, *pxe*, *rsh-server*, *talk-server*, *telnet-server* and *ypserv* can be removed.

In **Administration Tools** select all of the GUI config tools that you think you require. They are safe to install even if you don't end up using them.

In **System Tools** *amanda*, *ethereal*, *ethereal-gnome*, *nmap* and *nmap-front-end* are useful and can be installed and we will use *shapcfg* in appendix C for configuring bandwidth management.

Click next to begin the actual RedHat installation. The install process will begin by formatting the new partitions and installing the various packages required for a functioning Linux system. The installation should take approximately 25 minutes. At the end of this process, configure the X display system for your hardware if required. It is a good idea to turn off *Graphical* login type at this point. You will be presented with the option to create a bootdisk once the install is complete. It is a good idea to do so.

Turning off unnecessary services

One last job remains; after you have logged into your system and are satisfied that it is working correctly, we'll turn off some of the plethora of services that Redhat has enabled. Access it with this command;


```
[root@accesspoint root]# setup
```

A menu will come up. Scroll down to *System services* and press *enter* to select it. You will see a list of services, those with an asterix are enabled. Disable the following services by highlighting the asterix and pressing the *space bar*.

anacron Scheduling daemon

apmd Power management daemon

atd Scheduling daemon

autofs Automounting of remote filesystems

cups Unix print daemon

gpm Console mouse support daemon

isdn isdn

iptables Firewalling

kudzu Hardware maintenance daemon

netfs Remote file system mounter daemon

nfslock Network File System daemon

pcmcia PCMCIA monitor daemon

portmap RPC control daemon

rhnsd Redhat update daemon

sendmail Mail server daemon

xinetd TCP/IP services super-daemon

This leaves us with only these services enabled; **crond**, **keytable**, **network**, **random**, **rawdevices**, **sgi_fam**, **sshd**, **syslog** and **xfs** which will make the system more responsive.

Note that **xfs**, the X font server, can be disabled as well if you have no intention of running X.

Reboot and test

You may like to reboot your system now to make sure that it comes back up OK. Reboot with this command;

```
[root@accesspoint root]# shutdown -r now
```

once your system comes back up and you're satisfied that it is functioning nominally,

LINUX FILE SYSTEM MANAGEMENT

badblocks	Used to search a disk or partition for badblocks.
cfdisk	Similar to fdisk but with a nicer interface.
debugfs	Allows direct access to filesystems data structure.
df	Shows the disk free space on one or more filesystems.
dosfsck	Check and repair MS-Dos filesystems.
du	Shows how much disk space a directory and all its files contain.
dump	Used to back up an ext2 filesystem. Complement is restore.
dumpe2fs	Dump filesystem superblock and blocks group information. Ex: dumpe2fs /dev/hda2
e2fsck	Check a Linux second extended file system.
e2label	Change the label on an ext2 file system.
exportfs	Used to set up file systems to export for nfs (network file sharing).
fdisk	Used to fix or create partitions on a hard drive.
fdformat	Formats a floppy disk.
fsck	Used to add new blocks to a file system. Must not be run on a mounted file system.
hdparm	Get/set hard disk geometry parameters, cylinders, heads, sectors.
mkfs	Initializes a Linux file system. This is a front end that runs a separate program depending on the file system's type.
mke2fs	Create a Linux second extended file system.
mkswap	Sets up a Linux swap area on a device or file.
mount	Used to mount a filesystem. Complement is umount.
rdev	Query/set image root device, swap device, RAM disk size of video mode. What this does is code the device containing the root filesystem into the kernel image specified.
rdump	Same as dump.
rmt	Remote magtape protocol module.
restore	Used to restore an ext2 filesystem.
setfdprm	Set floppy drive parameters.
swapoff(8)	Used to de-activate a swap partition.
swapon(8)	Used to activate a swap partition.
sync	Forces all unwritten blocks in the buffer cache to be written to disk.
tune2fs	Adjust tunable filesystem parameters on second extended filesystems.
umount	Unmounts a filesystem. Complement is mount.

CREATING A USER ACCOUNT

When you first started your Red Hat Enterprise Linux system after installation, you were given the opportunity to create one or more user accounts using the **Setup Agent**. If you did not create at least one account (not including the root account) you should do so now. You should avoid working in the root account for daily tasks.

There are two ways to create new and/or additional user accounts: using the graphical **User Manager** application or from a shell prompt.

To create a user account graphically using the **User Manager** :

1. Select **Applications** (the main menu on the panel) => **System Settings** => **Users & Groups** from the panel. You can also start the **User Manager** by typing `redhat-config-users` at a shell prompt.
2. If you are not logged in as root, you will be prompted for your root password.
3. The window shown in Figure will appear. Click **Add User** .

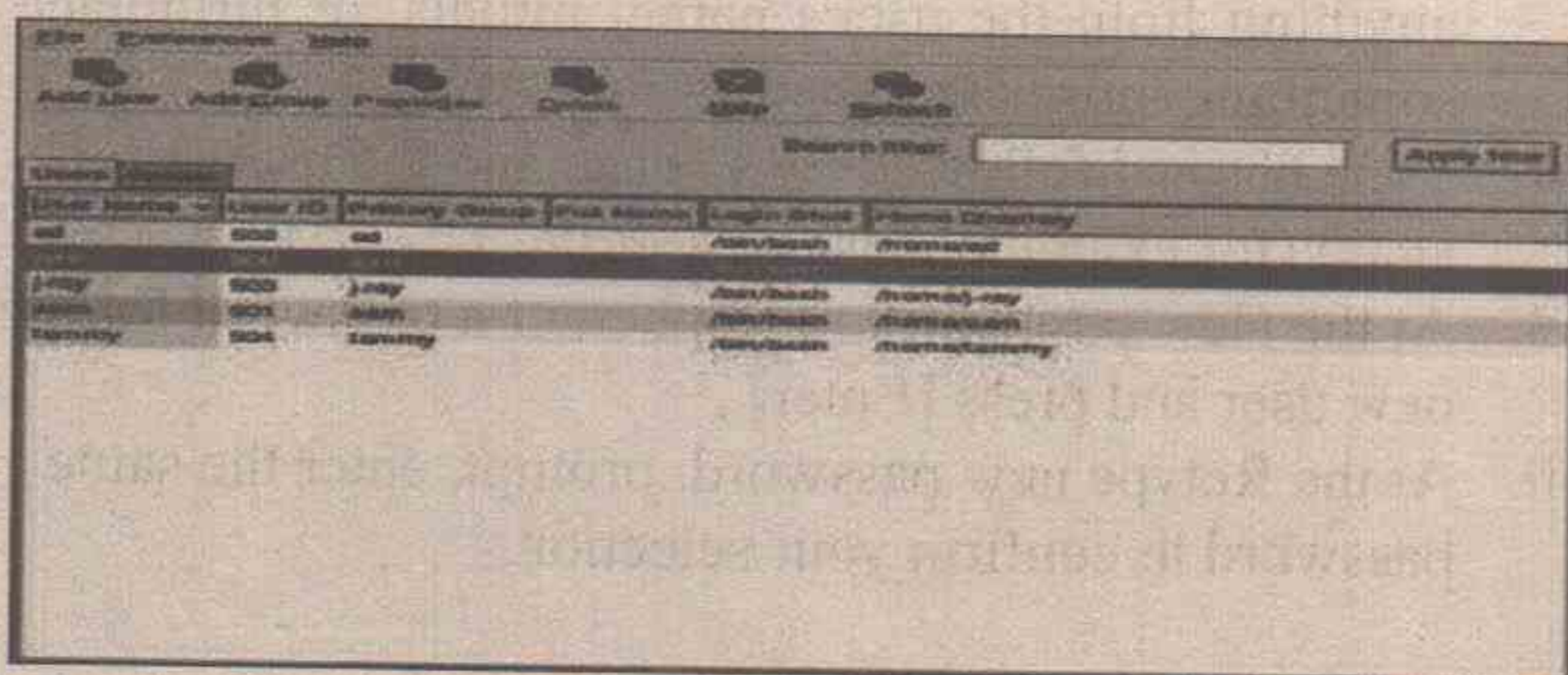


Figure. The Red Hat User Manager

4. In the **Create New User** dialog box, enter a username (this can be an abbreviation or nickname), the full name of the user for whom this account is being created, and a password (which you will enter a second time for verification). The name of this user's home directory and the name of the login shell should appear by default. For most users, you can accept the defaults for the other configuration options. Refer to the *Red Hat Enterprise Linux System Administration Guide* for details about additional options.
5. Click **OK**. The new user will appear in the user list, signaling that the user account creation is complete.

To create a user account from a shell prompt:

1. Open a shell prompt.
2. If you are not logged in as root, type the command `su -` and enter the root password.
3. Type `useradd` followed by a space and the username for the new account you are creating at the command line (for example, `useradd jsmith`). Press [Enter]. Often, usernames are variations on the user's name, such as `jsmith` for John Smith. User account names can be anything from the user's name, initials, or birthplace to something more creative.
4. Type `passwd` followed by a space and the username again (for example, `passwd jsmith .`)
5. At the New password: prompt enter a password for the new user and press [Enter].
6. At the Retype new password: prompt, enter the same password to confirm your selection.

How to add a new user in Redhat

To add a user and set up the directories you want that user to have, use the **useradd** command. By default, this will add a

user and create a home directory for that user, which will be located in /home.

EXAMPLE: **/usr/sbin/useradd** *yourname* will create the user *yourname*, and make the directory */home/yourname*

Set the password for the new user by running **passwd**. This will give the user a password and activate the account.

EXAMPLE: **/usr/bin/passwd** *yourname*. You will be prompted twice for a password.

NOTE: If you want useradd to create more default directories than just /home/newuser, you can add them to /etc/skel.

Anything you add to this directory will be created when you add a new user.

EXAMPLE: **mkdir** */etc/skel/www* will add a directory called *www* to the *skel* dir. Now whenever you run useradd to create a new user, it will also create a *www* directory in the new users home directory.

perfect24u.ocm

There are also some options for useradd you can add if you wish, such as changing where the users home directory will be, or which skeleton directory to use

INSTALLATION APPLICATION SOFTWARE IN LINUX

1. Open a console.
2. Use the command **cd** to navigate to the correct folder. If there is a README file with installation instructions, use that instead.
3. Extract the files with one of the commands. If it's tar.gz use **tar xvzf** *PACKAGENAME.tar.gz*. ...
4. **./configure**.
5. **Make**.
6. **sudo make install**.

Configuring device drivers in Linux

To install hardware devices on Windows servers, admins must install the appropriate device drivers first. Here are some guidelines for installing, configuring and troubleshooting device drivers.

Methods of installing device drivers

Admins can install device drivers on a server in four ways.

1. Running the Setup. Device drivers are automatically installed for all detected devices during installation of Windows 2000 system on the server computer
2. Starting the computer. Whenever the server is started, new devices are detected and their device drivers are automatically installed
3. Scanning for new hardware. Add/Remove Hardware Wizard can be used to perform the hardware-detection process and desired device driver installation
4. Manual installation. You can use the Add/Remove Hardware Wizard to specify the device you want to install, or you can right-click the .INF file that comes with the driver and choose Install.

Updating and removing device drivers

Administrators often have to update the existing device drivers or remove them.

To update a device driver:

1. Start Device Manager by typing 'Devmgmt.msc' in the Run dialog box.
2. Right-click the desired device and select Properties.
3. Click the 'Driver' tab and then click the Update Driver button.
- 4.

To remove a device:

1. Start Device Manager by typing 'Devmgmt.msc' in the Run dialog box.
2. Right-click the desired device and select Properties.
3. Click the 'Driver' tab and then click Uninstall button

BASIC COMMAND**Q) explain the following linux command****clear Command:**

The external clear command clears your terminal screen if possible.

\$ clear and press <Enter>

the terminal screen is cleared and the shell prompt \$ appears at the top of the screen.

pwd Command:

perfect24u.ocm

pwd command displays the full path of your present working directory. Present working directory is your current working directory. The format of the command is

\$ pwd

cd Command:

The internal cd command changes your current working directory. cd lets you do the following:

- change working directory
- change to last previous working directory
- use a string substitute in the current path to change to a similar directory path

The general format of the command is:

\$ chdir/cd -

\$ cd [directory]

\$ cd.. The present working directory is changed to previous working directory.

mkdir Command:

The external mkdir command makes a new directory. You can pass multiple arguments to mkdir. Each argument is used by mkdir as the name of a new directory to create.

The general format of mkdir command is

```
$ mkdir [-m mode] [-p] directory_list
```

Options:

-m mode : Mode to use for new directories. This allows you to specify what mode all of new directories will have when they are created.

-p : Parent directory creator. If you specify a pathname to create a new directory and the parent directories do not exist, mkdir will create them as needed.

Note: You must have write permission for the directory when you are creating new subdirectories. If no write permission is available, you will not be able to create new directories.

Examples:

(1) To create a subdirectory called misc which has another subdirectory named misc1

```
$ mkdir misc misc/misc1
```

rmdir Command:

The external rmdir command removes a directory. The directory must be empty.

rmdir is a safe way to perform directory removal than using rm -r command. It checks the directory for existence of files and subdirectories. If any exists, rmdir complaints and exits without removing the directory.

The general format of rmdir is

```
$ rmdir [-ps] directory_list
```

```
or $ rm -r directory_list
```

Options:

-p : Removes empty directories specified in the directory path. Name of each directory is displayed on standard output as it is

removed. Directories that are not removed are displayed on standard error.

-s : Suppress any messages produced. Both standard output and standard error are suppressed.

Examples:

(1) \$ rmdir misc/misc1 misc

To check whether the directories misc and misc/misc1 are removed use the following command to list the directory

\$ ls -l

cat command:

The external cat command reads each file in the argument list and displays the data to the standard output. It can read data from files or from standard input. It only writes to the standard output. By using shell re-direction capabilities cat can be used to combine multiple files into one large file that is why it is called concatenate. Some of the uses of cat command are as under:

- Display contents of ASCII files.
- Make a copy of a file.
- Combine multiple files into one file.
- Copy input from your keyboard to a file.
- Send output to a pipe used for multiple file input.
- Combine input from screen and a file into one output stream.

General format of the cat command is

cat [-] [-su] [-v [-et]] file_list

Options:

- : Read from standard input, treated as one input file.
- s : Error messages for non-existent files are suppressed.
- v : Prints non-printing characters in visible form. Control characters e.g., Control-X is printed as ^X.
- e : Print a \$ sign to represent new-line character.
- t : Print a ^I (Control-I) in place of tabs.

file_list : One or more files in sequential order and write to standard output. If no argument is specified cat reads from standard input.

Examples:

- (1) \$ cat myfile
- To display a file
- (2) \$ cat mylist yourlist hislist -To display multiple files
- (3) \$ cat originalfile > newfile -To copy a file
- (4) \$ cat file1 file2 file3 > file123 - Combining multiple files
- (5) \$ cat > newfile - Creating a file from keyboard
{ here you type whatever you like and at the end press Ctrl-D }

ls command:

ls command is used to display files and directories names. The format of ls command is:

\$ ls [*options*] [filenames or wild cords)

Some of the essential options are:

- a: lists all files. Including hidden files starting form "."
- d: displays data about directories.
- l: long list files and directories.
- t: lists file in order of last modification time.
- R: recursively lists files in all subdirectories.
- r: displays files in reverse alphabetical order of filenames.
- U: Sort entries by the last access time
- x: Sort files by file extension in alphabetical order

mv command:

The external mv command moves a file from an existing location to a new location. It is also used as the rename command to change the name of a file. It has three formats:

- rename a file with a new filename
- move one or more files to reside under a different directory
- rename a directory with a new directory name

General format of the mv format is:

\$ mv [-if] filename new_filename

\$ mv [-if] filename directory

\$ mv [-if] *old_directory new_directory*

Options:

- f: Force the move to occur. Response "Yes" is assumed and move is performed.
- i: Commands runs in interactive mode. If destination file already exists, mv prompts you with the filename followed by a question mark (?). If you respond with 'Y' or 'Yes', move is performed. Any other response will cause mv to skip to next move.

Examples:

- (1) Display the list of files in the current directory

\$ ls -x

caller file1 file2 db letters

Now use mv command to rename the file file2 as stuff

\$ mv file2 stuff

Now display the list

\$ ls -x

caller file1 db letters stuff

cp command: The external cp command copies a file. It reads the contents of a file and creates a new file or overwrites an existing file. There are two basic formats of cp that allow you to:

- copy one file to another file
- copy multiple files to a directory
- copy input from your keyboard to a file
- copy a file to your terminal

General format of the cp command is

\$ cp [-ip] *source_file dest_file*

\$ cp [-ipr] *source_file_list dest directory*

\$ cp [-ip] *source_directory dest_directory*

First format copies one ordinary file to a new file. Second format will copy one or more files to a specific directory. Third format

allows you to copy an entire directory structure to a new directory.

Options:

-i : Interactive confirmation is required. You are prompted if an existing file is overwritten. If 'Y' or 'Yes' is given in response, copy is performed otherwise not.

-p : Preserve the characteristics of the source file. Copy the contents, modification times and permission modes of the source file to the destination file.

-r : Recursively copy any source directories. If a directory is given as the source file, then all of its files and subdirectories are copied. The destination must be a directory.

Examples:

- (1) \$ cp letter letter.bak # make a backup copy of file letter
- (2) \$ cp letter ../temp perfect24u.com letter to temp working directory
- (3) \$ cp /dev/tty note # copy input from keyboard to file note
- (4) \$ cp file1 stuff # copy file1 to file stuff
- (5) \$ cp calendar letters # copy file calendar to directory letters

rm command:

The external rm command removes (deletes) files or directories.

The general format of the rm command is

\$ rm [fi] file_list

\$ rm [-fir] directory_list [file_list]

Options:

-f : Forces the removal of all files listed. Does not check whether file is write-protected or not. Does not prompt for confirmation. If directory is write-protected, files are never removed.

-i : Interactive file removal. Response is awaited.

-r : Recursively removes files and directories. All files are removed from each directory. Each directory is then removed. If a

file is write-protected, then rm prompts you for confirmation to remove the file.

Examples:

- (1) `$ rm stuff` # to remove a file named stuff
- (2) `$ rm -ri letters`
`letters/calendar ? y`
`letters/file1 ? y`
`letters ?`
press Return not to delete letters directory.

more/page Command:

The external more command allows you to view a file on your terminal. . It lets you view one screen of text at a time. The page command performs the same function as more but with a different screen control. The screen is cleared before each full screen of text is displayed.

The general format of the more command is

`$ more [-option] [+linenum] [file_list]`
or `$ page [-option] [+linenum] [file_list]`

Options:

- f : Do not fold long lines. Count logical lines instead of screen lines. Normally more truncates lines longer than the screen width
- s : Squeeze out adjacent blank lines. Two or more blank lines are grouped together and are reduced to one blank line. This increases amount of text displayed on the screen
- w : Prompts and waits for any key to be pressed before exiting. By default more/page will exit without waiting when end-of-file reaches
- rows : Specifies the No. of rows (lines) to display on your terminal screen
- +linenum : Begin display at line number linenum of the input
- file_list : The list of files to be read by more.

Examples:

(1) type `more /etc/passwd /etc/group /u1/ts/mylogin/file1` and press Return. First screen of `/etc/passwd` file will appear.

(2) press Spacebar, next screen of data is displayed. (If the data in the file has been finished, next file is started)

(3) type `2:n` to skip to `/etc/group` file. The output will look like

... skipping

... skipping to file `/u1/ts/mylogin/file1`

---more---(Next file: `/u1/ts/mylogin/file1`)

(4) To return to second file, type `:p` to skip backward to `/etc/group` file.

... skipping

... skipping to file `/etc/group`

---more---(Next file: `/etc/group`)

(5) press Spacebar to move from one screen

(6) press Spacebar to move until (Next file: `/u1/ts/mylogin/file1`) appears

At the end, type `'q'` to exit from more.

Grep Command

Search files for lines matching a specified pattern and display the lines

Syntax `Grep [option] [pattern] files`

`-c` instead of displaying matching lines simply output a count of total number matching the expression

`-i` ignore case in both the pattern and files

`-L` instead of displaying each line simply display the name of each file that contains no matches for the pattern

`-n` prefixes each output line its line number in the file

`-w` Display only those lines with matches for the patterns that complete word

`-x` Display only those lines with matches for the patterns that complete line

zip Command

Create a Zip archive from one or more files and directories

Syntax zip zipfilename file1 file2 file3

-r Recursively work with directories adding all files in the subdirectories to the archive

-m move files into the archive deleting them from original location.

-e Encrypt the archive after prompting for a password .this password will be use in extracting

unzip command

Manipulates and extract ZIP archive

Syntax unzip [option] zipped filename

-f: Extract only those files that are newer than already-existing version of the file

-l: Displays the contents of the archive without extraction

Chmod Command

Change the access permission of one or more files or Directory

Syntax chmod [option] mode files

options

-r recursive Recursively changes the permissions of all files in all subdirectories

-v verbose Displays the results of all permission changes

-f silent Suppress display of error messages when files permissions cannot be changed

Mode it is in the form [ugoa][+ -=] [rwx]

u = user who owned the file

g = all members of the group that owns the file

o = anyone who is not the owner or in the owner

group

a = all user

+ = Specified modes should be add to already specified permission

- = Specified modes should be remove from already specified permission

= = Specified modes will replace existing permission

r = read permission

w = write permission

x = execute permission

Example \$ Chmod u+x a.bat will give execute permission to user on a.bat file

\$ Chmod u-x a.bat will remove execute permission to user

\$ Chmod a+x a.bat will give execute permission to all user

\$ Chmod a=rx a.bat will give read and execute permission to all user and remove existing permissions

at command

Schedules commands to be executed at a specific time. User is prompted for the commands.

Syntax at [options] time

-f filename: read commands from the specified file rather than prompting for the commands

example

\$at 2.30

rm*. Temp ctrl-d

specifying times

now = specifies the current time

today = specifies the today

tomorrow = specifies the next day

+ = specify offsets in minutes hours days of weeks

now+ 2 hours = two hours from now

oday + 3 days = 3 days form today

Job Control

Using Job control, it is possible to use a single shell to execute and control multiple programs running simultaneously

Normally, when you execute a command, it runs in the foreground. That is, the shell executes the command and the prompt doesn't return until the command is finished

I.e. executing a command

\$ find / -name '*.tmp' -print >findfile

This command searches the entire structure of Linux system for files with the .tmp extension and store the result in the findfile

file. While executing this command you won't be able to run other commands while find is running

To place a job in the background is to add an ampersand(&) to the end of the command when you run it

```
$ find / -name '*.tmp' -print &
```

once you press enter to execute this command, you are immediately presented with a new command prompt; at the same time and you will be able to execute the next command same time thus you can execute multiple task an the same time

jobs command

This command will list all jobs running

```
$ jobs
```

```
[1]      Running
```

```
$ find / -name '*.tmp' -print >findfile &
```

```
[2]      Running
```

```
$ ls -lR / '*.bmp' >dirlist &
```

fg command

This command bring the background job to foreground

Syntax

```
fg Jobs no
```

Example

```
$ fg 1
```

this will bring \$ find / -name '*.tmp' -print >findfile from background to foreground ie on screen

bg command

This command start the stopped job in the background

Syntax

```
bg Jobs no
```

The foreground job first stopped by pressing Ctrl-Z and command prompt will be available. Where you can run the bg command to run the stopped command in the background

Example

Suppose you enter another command

```
$ ls -lR / '*.bmp' >dirlist
```

This will execute in the foreground then press Ctrl-Z . This will temporary stopped the ls job

And give command prompt .to see the all current job

```
$ jobs
```


[1] Running find / -name '*.tmp' -print
>findfile &

[2] Stopped \$ ls -lR / '*.bmp' >dirlist &
Now to start the stopped job ie [2] enter the command and prompt

\$ bg 2
to see the result

\$ jobs

[1] Running \$ find / -name '*.tmp' -print >findfile &

[2] Running \$ ls -lR / '*.bmp' >dirlist &

cal Command:

The external cal command generates a simple calendar and write it to the standard output. The default output for cal is current month. Using specific argument, a calendar for specific year or year and month can be created. Valid years are 1 to 9999. Valid months are 1 to 12.

The general format of the cal command is

\$ cal [[month] year]

year : Produces calendar for given year

month : Produces calendar for specified month of given year

Example:

To create a calendar for September 1924, the command is given as

\$ cal 9 1924

echo command

Displays a line of text to your terminal. Some of the feature and use of echo are 1) Display string of text 2) Display variables

3) Display menu screen

Syntax echo "string"

Example \$ echo "my home directory is \$home"

write Command:

The external write command sends messages you type on your terminal to another user's terminal. write reads the standard input and writes to the specified user's terminal tty. The write command is used to communicate with the fellow users on an interactive basis. It is useful to send a brief message to someone immediately

or to carry on conversations using terminals. The general format of the write command is

`$ write user_name [tty]`

Options:

`\user_name`: The name of a user who is currently logged in to the system. Use the who command to list who is on the system

`tty`: Specify which terminal tty to connect to if the same user is logged on more than once.

Examples:

(1) Create a file and type some message in it, then use the following command:

`$ write alpha < tempmesg`

where alpha is the name of the user to whom the message is to send while tempmesg is the file containing the text of the message.

(2) Type the following command

`$ echo "How are you? I want to meet you in the library at 9:00" | write alpha`. The echo will send the message to write via a pipe.

The message will appear on the screen of username alpha all at one time as shown below:

message from mylogin tty11 [date & time]

How are you? I want to meet you in the library at 9:00

wall Command:

The external wall command performs a write to all users currently logged on to the system.

The general format of the wall command is

`$ wall`

The wall message precedes its message text with the following line:

Broadcast message from use_name

It is usually used by super user to warn all users of immediate problems. The most common warning is that the system is being shutdown within 60 seconds.

The super user can write to any user's terminal regardless of the permissions set by that user using mesg command. The wall

command is commonly used by the super user. It can also be used by any user but many users do not need to send message to every one on the system. Common formats are:

\$ wall < mesgfile
or \$ cat mesgfile | wall

Examples:

(1) \$ wall

man Command:

The external man command display help about any command to your terminal screen.

The general format of the man command is

\$ man command

Example

\$ man cp

will display help page of cp command.

head Command:

The external head command will display the first 23 lines of a file on screen

The general format of the head command is

\$head file name

Example:

\$ head abc

will display first 23 lines of abc file .

tail Command:

The external tail command will display the last 23 lines of a file on screen.

The general format of the tail command is

\$ tail file_list

Example \$ tail abc

will display last 23 lines of abc file .

mail Command:

The external mail command is an electronic post office. You can send, receive and store messages using mail command. There is a long list of options associated with mail command which can be

used according to the requirement. The general format of mail command is

\$ mail options

To read mail, use the following command

\$ mail

all the messages stored in the mailbox can be displayed.

To send mail to another user of the system, the following command is used:

\$ mail user_name

Examples:

(1) To send mail to a user named alpha

\$ mail alpha and press Return. The following screen appears

Subject: ----- (type the subject of the message) (type the message) press Ctrl-d to end the message

(2) To read mail, type

\$ mail

The display will show *mail version 01/29/99 Type ? for help*

Shutdown command

The external Shutdown command will shutdown the system. the root user are allowed to use this command on server, specifying time, will broadcast the message to all connected users. This command be used according to the requirement. The general format of shutdown command is

\$ shutdown options time [message]

option

-h will halt after shutdown

-r system will reboot after the shutdown .

Time time specified in minutes

Example \$ shutdown -h 3 "please save you work , the system is shutdowning in 3 minutes"



Khyber Pakhtunkhwa Board of Technical Education Peshawar

Diploma in Information Technology

(Part - I)

2nd Term Examination 2017

Paper: - Operating System

Time Allowed: - 03 Hours.

Max. Marks: - 50

Note: -

Attempt any five questions. Select at least two questions from each part. All Questions carry equal marks. Mobile Phone & Programmable calculators are not allowed.

(Part - I)

Q.1: -

Define the Operating System. Briefly explain popular operating systems.

Q.2:-

perfect24u.ccm

Briefly explain any two of the following:

- a) Resource Management
- b) Memory Management
- c) File Management

Q.3:-

What is Scheduling? Explain.

Q.4:-

Explain the steps of installation of Windows Server 2008.

(Part - II)

Q.5:-

Briefly discuss the history of Linux.

Q.6:-

Write short note on any two of the following.

a) GUI b) Command Prompt

c) Free Software

Q.7: -

Discuss any two of the following.
a) File b) Directory

c)Linux Shell

Q.8:-

Explain any two of the following Linux Commands.

- i) ls command
- ii) mkdir command
- iii) cd command
