Some of the important and enhanced considerations when installing Windows Server 2003 are :

- **Bootable CD-ROM installation :**
  Windows Server 2003 can be installed directly from the CD-ROM. There is no support for starting installation from floppy disks.

- **Improved graphical user interface (GUI) during setup :**
  Windows Server 2003 uses a GUI during setup that resembles that of Windows XP

- **Product activation :**
  Retail and evaluation versions of Windows Server 2003 require that you activate the product.
  Volume licensing programs, such as Open License, Select License, or Enterprise Agreement, do not require activation.

Following Step required installing Windows 2003.

1. Configure the computer's BIOS or the disk controller BIOS to boot from CD-ROM. If you are not sure how to configure your computer or disk controller to boot from CD-ROM, consult your hardware documentation.

2. Insert the Windows Server 2003 installation CD-ROM into the CD-ROM drive and restart the computer.

3. After configuring the system for booting from a CD, the Windows Setup screen appears.
At this point, Setup is loading the driver files it needs to continue with installation.

4. The "Time Limited" warning screen appears with the option of Continuing Setup or Quitting.
Press ENTER to Continue Setup or F3 to Quit and reboot the system.

5. The "Welcome to Setup" screen appears with the option of Continuing Setup, Repair a previous installation, or Quitting.
- Press ENTER to Continue Setup.
- You may also choose R to Repair or F3 to Quit and reboot the system.

6. The "Windows Licensing Agreement" screen, otherwise known as "EULA," displays the legal in's and out's of this particular software package.
- You may press F8 to signify that you agree with the terms, hit ESC if you do not agree and PAGE UP or PAGE DOWN to scroll through each screen. Note: If you do not agree to the terms, setup will quit and reboot the system.

7. Hard drive partition information is now displayed. This varies with each systems hardware configuration.

8. Continue to create partitions until all space is used or the configuration meets your requirements. Note: a small portion will be unavailable to partition. This is normal. In this example, it is 8 MB.

9. Select what format you wish to use by pressing the UP ARROW and DOWN ARROW keys.
Press ENTER to confirm your selection and Continue or ESC to Cancel.

10. Watch the progress bar as Setup formats the partition, It may take awhile.

11. After the partition is a finished formatting, Setup copy various files to support booting from the hard drive and continue on.

12. The first reboot and the end of the blue background has arrived. If you are impatient, press ENTER to Restart before the 15 seconds expire.
ENTER to Restart the Computer is the only option available.

13. The new Windows Server 2003 Family boot screen is displayed.

14. Windows Server 2003 Installation:
Sit back. It may be awhile.

15. Region and Input Languages Option

16. Enter in your Name and optional Organization information, and then select the Next button.
Select the **Next** button to continue.

17. Enter your unique 25 digit Product Key that came with your CD or download, and then select the **Next** button.

18. Configure the Licensing mode.
- Options are Per server or Per seat.
- Per server is usually used for a single-server network.

- Per client is used if all of the concurrent connections is higher than the number of clients or seats that you have.

19. Enter an Administrator Password now. It is very important that you keep this information safe and remember what it is!
Select the **Next** button to continue.

20. If the chosen password does not meet acceptable guidelines, a warning box will appear with suggestions on how to make the system more secure.

21. Configure the proper information for the Date, Time and Time Zone here.
Select the **Next** button to continue.

22. Faster development of applications, but still slow install times. Wait here while the Network is installing.

23. The Network Settings Dialog is next. Under usual circumstances, the **Typical settings** are fine.
Choose your method and select the **Next** button.

24. Custom settings for network (Network Load Balancing).

25. File and Print Sharing for Microsoft Networks has several options not available with Windows XP Home or Professional.

26. TCP/IP Properties contains the standard options. Adjust them for your particular needs as required. Select the **Advanced** button to further configure your TCP/IP options.

27. Select Workgroup or Computer Domain.
Select the **Next** button after making your choice.

28. Install screen appear.
The system will reboot after all files have been copied over to the install partition. Now may be a good time to take a break. It may be awhile.

29. The moment we have all been waiting for, Windows 2003 is starting up for the first time.

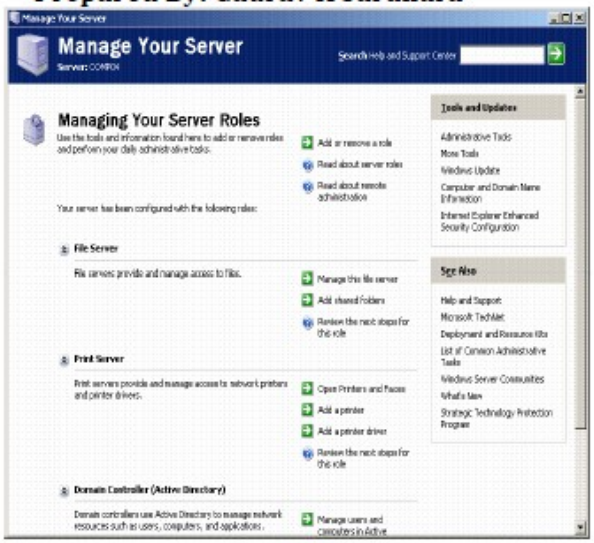
30. Hit the "Three Finger Salute" combination of Ctrl+Alt+Delete to login to the Administrator account.
You did remember your password, right?!?

31. Enter your password to login to the Administrator account.

Select **OK** to continue.

❖ Windows 2003 Enterprise Server Configuration:

- After installing and activating Windows, you can configure the server using the Manage Your Server page that launches automatically at logon.
- The page facilitates the installation of specific services, tools, and configurations based on server roles.
- Click Add or Remove a Role and the Configure Your Server Wizard appears.
- If you select Typical Configuration For A First Server, the Configure Your Server Wizard promotes the server to a domain controller in a new domain, installs Active Directory services, and, if needed, Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and Routing And Remote Access (RRAS) service.
- If you select Custom Configuration, the Configure Your Server Wizard can configure the following roles:



- **Following Step required Configuring Windows 2003 :**

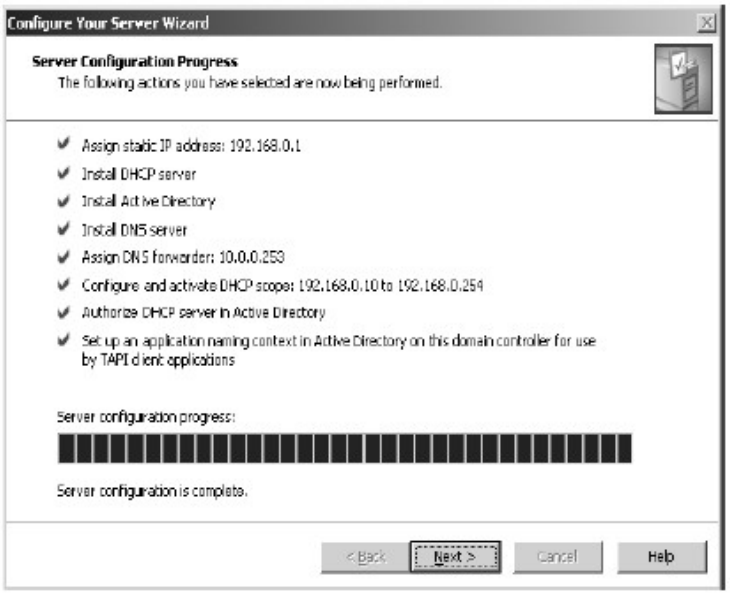
Example: Configure the server as the first domain controller in an Active Directory domain called contoso.com.

- 1. If it is not already open, open the Manage Your Server page from the Administrative Tools program group.
- 2. Click Add Or Remove A Role. The Configure Your Server Wizard appears.
- 3. Click next and the Configure Your Server Wizard detects network settings.
- 4. Click Typical Configuration For A First Server, and then click Next.
- 5. In Active Directory Domain Name, type contoso.com.
- 6. Verify that NetBIOS Domain Name reads CONTOSO and click Next.
- 7. Verify that the Summary of Selections matches that shown in Figure and click Next.

The Configure Your Server Wizard reminds you that the system will restart and asks you to close any open programs.

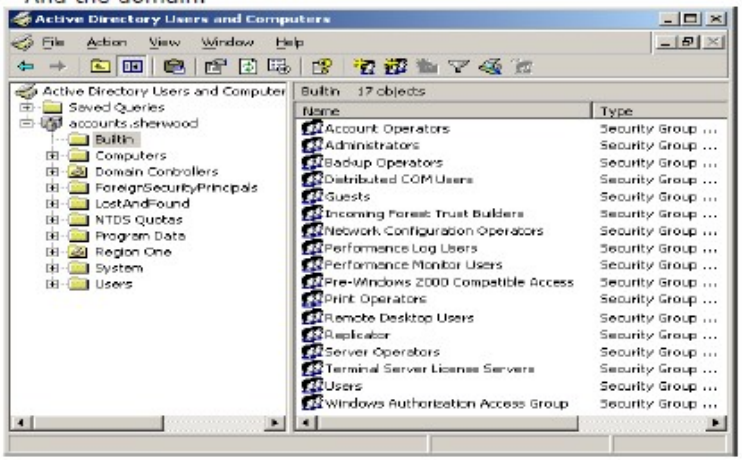
- 8. Click Yes.

- 9. After the system has restarted, log on as Administrator.
- 10. The Configure Your Server Wizard will summarize its final steps, as shown in Figure.



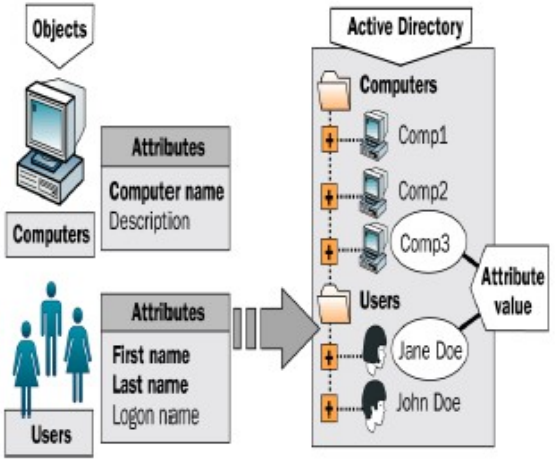
❖ Active Directory :

- Microsoft Windows networks support two directory service models:
- The workgroup
- And the domain.



- The domain model is by far the more common in organizations implementing Windows Server 2003.
- The domain model is characterized by a single directory of enterprise resources that is trusted by all secure systems that belong to the domain.
- Those systems can therefore use the security principals (user, group, and computer accounts) in the directory to secure their resources.
- **Active Directory thus acts as an identity store, providing a single trusted list of Who's Who in the domain.**
- Active Directory itself is more than just a database,
- It is a collection of supporting files including transaction logs and the system volume, or Sysvol, that contains logon scripts and group policy information.
- It is the services that support and use the database, including Lightweight Directory Access Protocol (LDAP), Kerberos security protocol, replication processes, and the File Replication Service (FRS).
- The database and its services are installed on one or more domain controllers.
- A domain controller is a server that has been promoted by running the Active Directory Installation Wizard by running DCPROMO from the command line or by running the Configure Your Server Wizard.
- Once a server has become a domain controller, it hosts a copy, or replica, of Active Directory and changes to the database on any domain controller are replicated to all domain controllers within the domain

❖ Active Directory Objects and Attributes :



❖ Active Directory Components:

Logical Structure

- Domains
- Organizational units
- Trees
- Forests

Physical Structure

- Sites
- Domain controllers

❖ Domains, Trees and Forests :

- **Domain** : Administrative unit of Active Directory
- **Tree :** A collection of one or more domains
- **Forest :** A collection of one or more trees

- Active Directory cannot exist without at least one domain.
- A domain is the core administrative unit of the Windows Server 2003 directory service.

- An enterprise may have more than one domain in its Active Directory.
- Multiple domain models create logical structures called trees when they share contiguous DNS names.
- For example **microsoft.com**, **uk.microsoft.com**, and us.microsoft.com share contiguous DNS namespace, and would therefore be referred to as a tree.
- If domains in an Active Directory do not share a common root domain, they create multiple trees.
- That leads you to the largest structure in an Active Directory: the forest.
- An Active Directory forest includes all domains within that Active Directory.
- A forest may contain multiple domains in multiple trees, or just one domain.
-
- When more than one domain exists, a component of Active Directory called the **Global Catalog** becomes important because it provides information about objects that are located in other domains in the forest and reduces LDAP queries to Active Directory.

Fig: Domain Tree

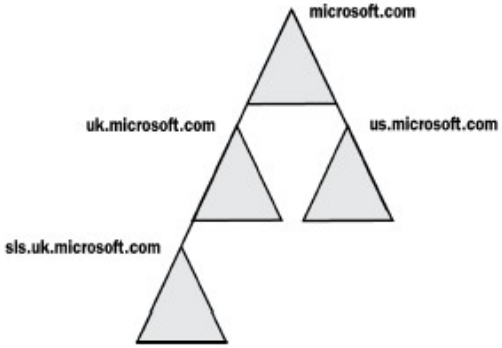


Fig: Domain Forest

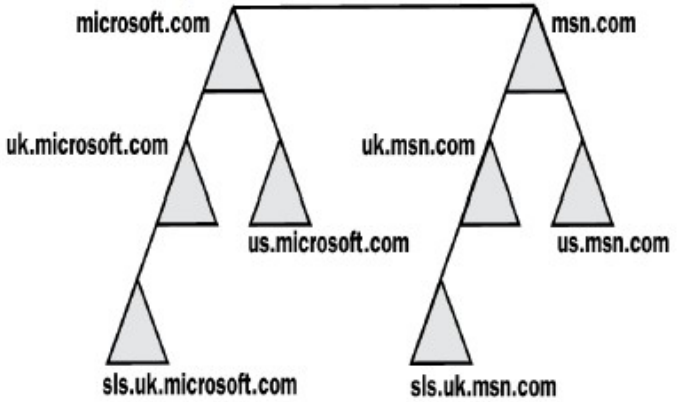
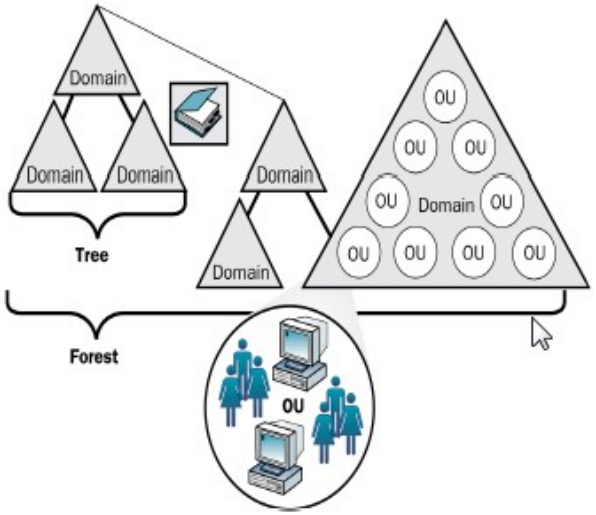


Fig: Logical Hierarchy



❖ Managing Active Directory Objects :

- When you first install Active Directory, a number of Containers are created to hold built-in users and groups, as well as computer accounts by default

- Organizational Units (OUs) allow the assignment of Group Policy and delegation of administrative control to junior administrators
- User accounts are best arranged into Organizational Units and have certain management functions that can be delegated at the OU level and inherited by lower levels.

- **User Account :**

A user account consists of

- Username and password
- Group membership
- Rights and permissions to access resources.

Windows Server 2003 Computer configured as a Domain Controller with Active Directory

- User accounts are managed by Active Directory Users and computers.

Windows Server 2003 computer member Server (not a Domain Controller) and Windows XP workstations

- User accounts are managed by Local Users and Groups

- **Computer Account :**

- Computer accounts are created and stored in the Active Directory like User and group accounts.

- Like users and group accounts, computer accounts have their own **specific attributes or properties** by which they can be searched and identified in the Active Directory.

- They can be members of security or distribution groups and inherit permissions from group objects.

- They inherit group policy settings from container objects such as domains, sites and Organizational Units (OUs).

- Computer accounts are used to identify computers in a domain with their security principles – SID

- A user with a valid user account and a password in Active Directory cannot log on to a domain, if the computer is not represented in that domain.

- Each Windows Server 2003 computer, Windows XP, Windows 2000 Server and Professional computer, Windows NT Server and workstation computer must have a computer account in an Active Directory - Domain Controller (DC) to participate in a domain.

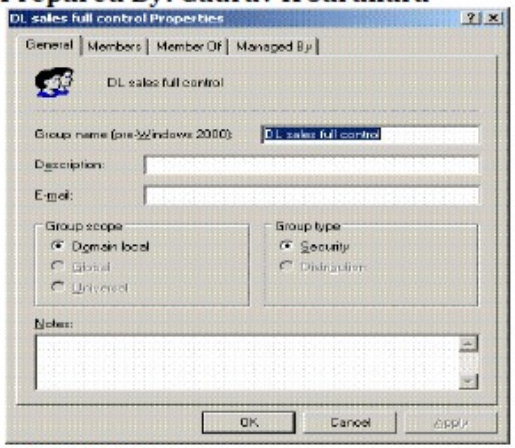
- Windows 95, 98, Me computers must install Active Directory Client software to participate in a domain
- Computer account password is generated automatically by the operating system and kept hidden

- **Group Account :**

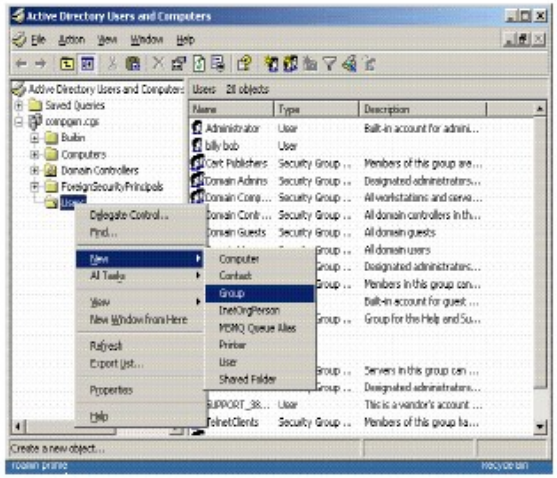
- Groups are a collection of user and computer accounts that you manage as a single unit.
- Groups simplify administration by enabling you to grant permissions to resources to the group rather that to each user individually.
- Are characterized by Scope and Type.
- Groups can be nested (groups can be members of other groups).
- In addition to user accounts, you can add other groups, contacts, and computers to groups
- Windows 2000 provides the ability to create groups:
- in a stand-alone computer security accounts database
- in Active Directory

Types of Groups:

- **Security groups :**
  - Windows 2000 itself only uses security groups, which you use to assign permissions to access resources and rights to perform tasks
  - Has all of the same functionality as distribution groups.
  -
- **Distribution groups :**
  - Applications can use distribution groups as lists for non security-related functions
  - You cannot use distribution groups to assign rights and permissions



- **How to Create a Group :**
  - Active Directory Users and Computers Right click the OU or Container you want to create a group in and click New>>Group



❖ **Monitoring Performance :**

- One of the most important tasks that should be performed on the network is some form of statistical collecting.
- These statistics can range from the performance of servers, workstations, and other

- Devices on the network to the performance of individual components within a program or service itself.
- Generally Several types of performance monitoring tools:
  - Simple Network Management Protocol (SNMP),
  - Windows NT Performance Monitor, and
  - Windows 95's System Monitor.

- **Simple Network Management Protocol (SNMP) :**

- Many types of software and hardware on the market enable you to collect statistics on the network.
- One important protocol used within the TCP/IP protocol suite that assists in statistic collecting is the Simple Network Management Protocol (SNMP).
- SNMP is a protocol that is supported by most pieces of hardware and software that support the TCP/IP protocol stack.
- This protocol allows for the collection of statistics of various resources on the network.
  For this information to be collected about a resource, the resource must run an SNMP service, or have some other device run the SNMP service on its behalf.
- The SNMP service collects predefined information. This information is stored in a Management Information Base (MIB).
- An MIB is a database of information that can be read by management software designed to work with SNMP.

Management software issues one of the following three main commands:

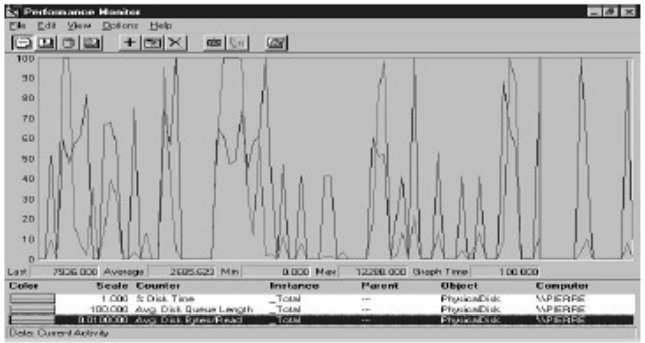
. The get command gathers information within an MIB.
. The get next command gets the next piece of information within the MIB.
. The set command places information within the MIB.

- These devices that have an SNMP service monitoring them can also be configured to issue traps, or system messages, when certain parameters are reached or exceeded.

- **Windows NT Performance Monitor :**

- Windows NT's Performance Monitor tool lets you monitor important system parameters for the computers on your network in real-time.
- Performance Monitor can keep an eye on a large number of system parameters, providing a graphical or tabular profile of system and network trends.
- Performance Monitor also can save performance data in a log for later reference.

- You can use Performance Monitor to track statistical Measurements (called counters) for any of several hardware or software components (called objects).
- An example of these counters for an object being displayed in a chart format can be seen in Figure.



Some Performance Monitor objects that relate to network behavior are as follows:

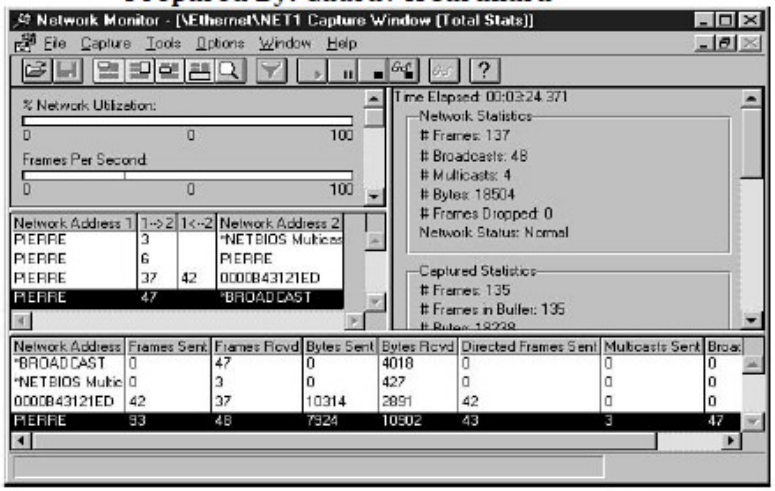
. Network segment
. Server
. Server work queues
. Workstation or other Redirectors
. Protocol-related objects, such as TCP, UDP IP, NetBEUI, NWLink, and NetBIOS
. Service-related objects, such as Browser and Gateway Services for NetWare.

Some Performance Monitor counters that relate to the performance of components or resources on a computer are as follows:

. Processor
. Memory
. Physical Disk

❖ Monitoring Network Traffic :

- Protocol analysis tools monitor network traffic by intercepting and decoding frames.
- Software-based tools, such as Windows NT Server's Network Monitor (see Figure), analyze frames coming and going, in real time, from the computer on which they run.



- Network Monitor records a number of statistics, including the percent of network utilization and the broadcasts per second.
- In addition, Network Monitor tabulates frame statistics (such as frames sent and received) for each network address.
- An enhanced version of Network Monitor, which is included with the Microsoft BackOffice System Management Server (SMS) package, monitors traffic on more than just the traffic between the local computer and other devices.
- It will also monitor traffic that is just between other devices, and also traffic on remote networks, provided a monitor agent is installed on the remote network segment.
- For large networks, or for networks with complex traffic patterns, you might want to use a hardware-based protocol-analysis tool.
- A hardware-based protocol analyzer is a portable device that can be as small as a palmtop PC or as large as a suitcase.

- The advantage of a hardware-based protocol analyzer is that you can carry it to strategic places around the network (such as a network node or a busy cabling intersection) and monitor the traffic at that point.
- A hardware-based protocol analyzer is often a good investment for a large network because it concentrates a considerable amount of monitoring and troubleshooting power into a single, portable unit.

- For a smaller network, however, a hardware-based analyzer might not be worth the initial five-figure expense because less expensive software-based products perform many of the same functions.

❖ Monitoring Network Traffic :

- Some operating systems, such as Windows NT, have the capability to keep a running log of system events.
- That log serves as a record of previous errors, warnings, and other messages from the system.
- Studying the event log can help you find recurring errors and discover when a problem first appeared.
- The event log should also be scanned on a regular basis to look for any indications of potential problems.
- Windows NT's Event Viewer application provides you with access to the event log.

- **You can use Event Viewer to monitor the following types of events:**
- **System events:**. Warnings, error messages, and other notices describing significant system events. Examples of system log entries include browser elections, service failures, and network Connection failures.
- **Security events:** Events tracked through Windows NT's auditing features.
- **Application events**. you can check the application log for an application-related error or warning message, provided the application is programmed to write to the event log. Some NT services such as the JET database engine used by WINS record their information in the application events log rather than the system log.

- **The Windows NT Event Viewer utility contains the following five types of events:**

1. **Information.** These events simply state that something of importance has been done, such as the loading of a protocol. These events are recorded for a matter of information only.

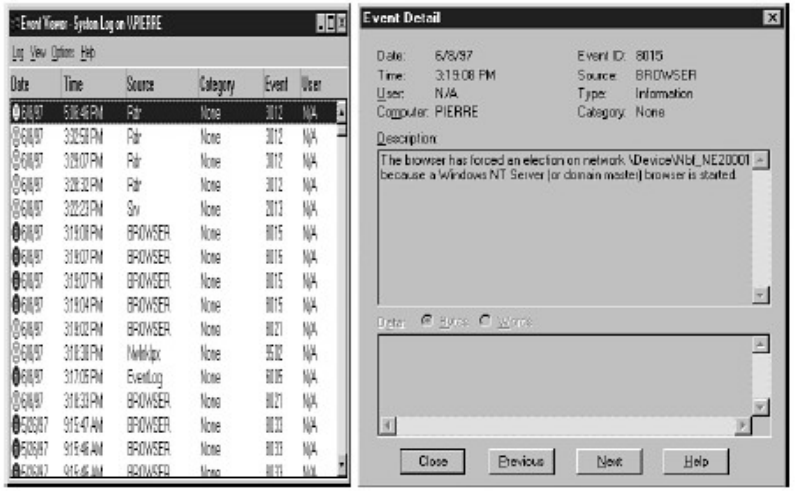
2. **Warning.** These events serve as a warning that some event that may be important has occurred. Often when services are stopped, a warning event is generated.

3. **Stop.** These events occur when something of significance, such as a detrimental event, has occurred. Often when services or hardware fail, a Stop event is generated.

4. **Success.** This event is generated within the auditing log.
   Success events are generated when an object that was audited as

Successful has occurred. You might, for example, audit the successful Logon of users.

5. **Failure.** This event is generated within the auditing log.
   Failure events are generated when an object that was audited as a Failure has occurred, such as the failure of users to log on.



❖ Microsoft Management Console(MMC) :

- MMC is the primary tool used to administer Windows Server 2003.

- In a Windows Server 2003 environment, administrator will normally be responsible for more than one server.

- A large number of pre-configured MMC are available in the Administrative Tools menu.
- A useful tool for administrators to manage Windows computers anywhere on the network
  (Remote server and clients) is **Microsoft Management Console (MMC)**

- MMC provides a customizable management framework for hosting multiple management tools (snap-ins)
- MMC with one or more snap-ins is called **console**