Chapter 1

Device Driver Is a Software that allows communication between the computer and an input/output port or external device.

File Servers Store files created by application programs.

Network Operating System is an operating system that manages computer network resources.

Network Operating Systems not only allow communication across a network, they also allow a network administrator to organize resources, control access, and ensure that the network is operating efficiently.

A combination of software programs that instruct computers and peripherals to accept requests for services across the network and then provide those services.

Note// Sharing of network resources can be **peer-to-peer** or **client/server**.

User Manager for Domains is a Windows NT Server application program that is used to maintain individual and group user accounts.

Print Server accept print jobs sent by anyone across the network.

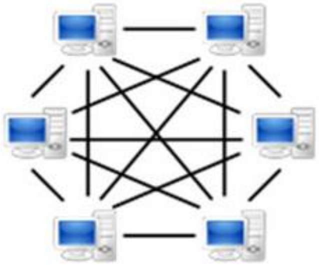
User Account An account used by Windows NT Server Operating Systems and other NOS's that provides access to the network.

Workgroup Group of devices logically networked together as a single unit.

Peer to Peer

All systems act as both users of resources and providers of resources, but no one system is dedicated to a single function.

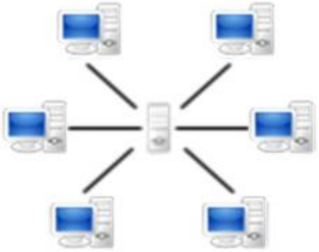
Note// In peer-to-peer networking there is a complete sharing of resources, both hardware and software.



Client Server

systems act as either users of network resources or providers of resources.

Note// Client/server networks dictate that systems are most often dedicated to a single function.

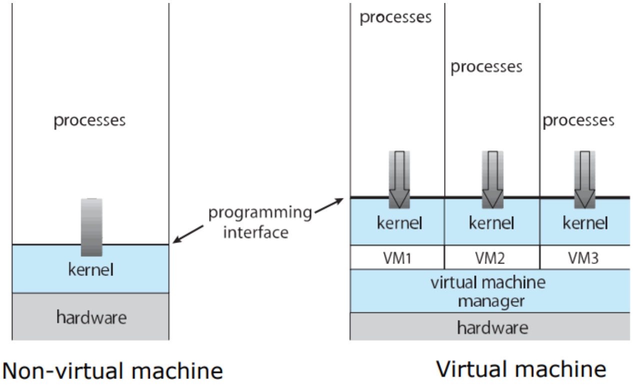


Host underlying hardware system. //The PC

Virtual Machine Manager (VMM)or hypervisor creates and runs virtual machines by providing interface that is identical to the host.

Except in the case of para virtualization.

Guest process provided with virtual copy of the host. Usually an operating system. //The VM



Type0 hypervisors Hardware-based solutions that provide support for virtual machine creation and management via firmware.

Type1 hypervisors Operating-system-like software built to provide virtualization.

Examples Vmware ESX, Joyent Smart OS, and Citrix Xen Server

Type2 hypervisors Applications that run on standard operating systems but provide VMMfeatures to guest operating systems

Examples Vmware Workstation and Fusion, Parallels Desktop, and Oracle VirtualBox

Windows for Workgroups and Windows 95

Windows for Workgroups and Windows 95 both offer peer-to-peer network protocols.

The protocols used by these operating systems allow users to share files and devices over LANs.

Note// NetBEUIsoftware identifies computer devices by name (like DNS).

Shared resources on Windows for Workgroups/95 networks are accessed by a password that protects the resource and there is **only one level of access.**

Windows NT Server

Is a Client/Server networking operating system that uses routable protocols.

Windows NT Server has **all of the advantages** mentioned for the other Windows operating systems, **plus**, it contains several other features making it more robust.

The security on Windows NT allows a network administrator to not only provide passwords for resources but also to individuals or groups.

Note// This operating system does require the use of a more powerful server computer whose sole function is to act as administrator of the NOS program.

Security Levels in Windows NT Server

1. No access
2. Read only
3. Access that allows read and write usage.
4. Access that allows you to change access permissions for network users.
5. Each user who wishes to access services on the network must have a password and a user account set up within the domain.

Domain

is a security model where the database of user accounts is stored on one or more computers known as domain controllers.

It centralizes control of the network.

The network administrator creates, deletes, and manages these accounts and passwords using the **User Manager**.

For security reasons, companies often have two servers capable of authenticating passwords.

One that acts as the **Primary Domain Controller (PDC)** and the other as the **Backup Domain Controller (BDC).**

PDC is a computer on the network that maintains a database of users and security policies for the domain.

BDC maintains a copy of the PDC database.

Domain models

1. **Single Domain Model**
   There is only one defined set of security and user accounts.
   all management functions are centralized.
2. **Master Domain Model**
   There is one master domain server that has the defined set of security and user account data of all other domain servers.
   each of these has only the specific security data for one domain.
3. **Multiple Master Domain Model**
   This Model has several master domain servers, each with their own specific domains.
   network management becomes somewhat decentralized.
4. **Multiple Trust Domain Model**
   This model is really a peer-to-peer relationship among domain servers, therefore it becomes decentralized.

Novel Netware

Is a client/server-based NOS and is not domain based but binary based. was designed for small workgroup environments.

It has evolved over time from **NetWare 2.X**.

Note// **NetWare 5.X** is aimed at **global enterprise network** environments.

NetWare is optimized for managing, sharing, translating, and synchronizing information throughout the network-computing environment.

Novell NetWare 4.X features **NetWare Directory Services (NDS)**

NDS allows a user to logon from anywhere on the network and access the same resources regardless of where the user logs on.

Note// Novell NetWare does **not** provide a computer operating system for client workstations.

Unix/Linux

UNIX is the oldest network operating system still being widely used today.

It can be used on either **peer-to-peer** or **client/server** networks.

UNIX networking is extremely **reliable**.

Networking under UNIX is based on the **TCP/IP Protocol**.

Network File System (NFS)

NFS provides hard disk sharing over TCP/IP networks.

Remote login services

Examples RLOGIN and TELNET, SSH.

Graphical user interface windowing system (X Windows)

is a completely distributed graphical user interface system.

Using X-Windows, a user can execute an application on one computer, and let that application interact with a user on a different computer using a network connection.

MACOS AppleShare

AppleShare provides network services for the Mac OS

AppleShare supports file and printer sharing over several types of physical networks by using one of the **AppleTalk** transport protocols.
AppleShare's peer-to-peer networking is used in small or moderately sized workgroup settings.

As the Internet has grown in popularity, TCP/IP software has been developed for the Apple Macintosh Computers. along with the standard TCP/IP client applications like Web Browsers and FTP file transfer clients.

Chapter 2

The term **service** describes a resource that is made available to users on the network.

The service may be **printing, accessing files**, or **running an application**.

A server can provide a **variety of network services such as**

- **File services**
- **Print services**
- **Application services** // including databases and web servers.
- **Messaging services** // in the form of e-mail and news.
- **DHCP services**
- **FTP services**
- **VPN services**

Dynamic Host Configuration Protocol (DHCP)

This service dynamically assigns an IP address to workstations that request to communicate on an IP.

File Transfer Protocol (FTP)

Used for sending and retrieving files from a server using the TCP/IP protocol.

Note// The FTP client software for downloading files is useless without the FTP server.
The FTP server, also called the FTP daemon on UNIX systems.
Note// using a web browser for file downloads has made FTP **less** common.

Virtual Private Network (VPN)

A VPN creates a tunnel by providing end-to-end encryption between the client and the VPN server to provide the connection to a private network or it could be used to access the Internet with different IP address and secure communication between the client and VPN server.

Note// Some organizations do not use VPNs because the data, although encrypted, still must travel over the highly insecure network of the Internet.

Software (NOS) that runs on a computer called a **server.**

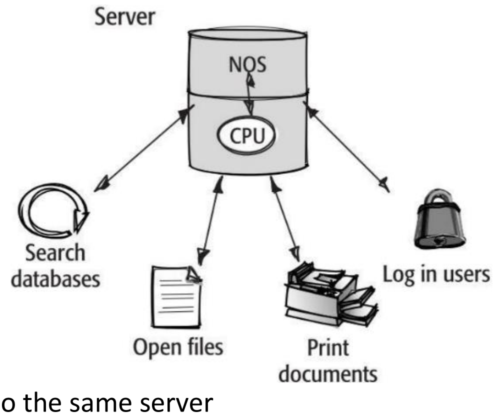
What to Look for in NOS

- **Performance.**
- **Flexibility.**
- **Security.**
- **Scalability.**

Multitasking

Is the ability to perform several tasks simultaneously.

Note// Some pieces of server software perform multitasking better than others using a process called **pre-emptive multitasking**.



Multiprocessing

Multiprocessing improves performance by allowing you to add more CPUs to the same server computer.

Note// You need to be sure your network operating system supports multiprocessing.

What to Look for in Server Hardware

- **Reliability** The server is capable of providing continuous service in the event of a critical failure or increased demand.
- **Scalability** As demand and needs grow, the server can be upgraded to accommodate growth.
- **Fault tolerance** The server minimizes the possibility of data loss by using a variety of and software to recover from faults or possibility hardware failures.

Note// The more reliable, scalable, and fault-tolerant a server is, the **more it will cost**.

These features are used to increase Fault tolerance. ↓↓

1- **Tape backup drive**
Uses software and hardware to backup data on the server.

2- **RAID (Redundant Array of Inexpensive Disks)**
A RAID configuration includes hardware and software that protects data in the event one of the hard disks stops working.

3- **Uninterruptible Power Supply (UPS)**
The UPS is a battery backup system.
In cases when power is lost, the UPS provides temporary power so that the server can be shut down properly, avoiding any loss of data.

Windows Server

is an NOS that takes the best features of Windows OS and Windows NT 4.0.

Takes some of the best features of Windows OS, such as zPlug and Play, and the well-known functions of Windows NT 4.0 was just one part of Windows

Standard, **Advanced**, and **Data Center** Each is designed to meet the particular demands of organizations.

Advantages

- Easier to manage.
- Fewer reboots.
- Plug-and-Play
- stability and uptime
- There is support to grow from a single processor server to large-scale servers.

Disadvantages

- may limit flexibility.
- high licensing costs.
- is not as stable or as fast as UNIX.
- It has high CPU, disk, and memory requirements.

UNIX

UNIX is the oldest network operating system still being widely used today.

It can be used on either **peer-to-peer** or **client/server** networks.

Note// UNIX was originally developed in the 1960s by Bell Laboratories at AT&T.

Berkeley Software Distribution UNIX (BSD UNIX or Free BSD)
Students at the University, developed BSD UNIX using the original software from AT&T.
Then they gave it away for free.

UNIX Advantages

- Very stable
- It can function as a workstation or a server.
- Very fast.
- It includes hundreds, possibly thousands, of built-in tools and applications, including programming tools.

UNIX Disadvantages

- It’s complex.
- The software can be very expensive (although BSD UNIX is free).
- Some companies sell versions of UNIX that will run only on their hardware.

Linux

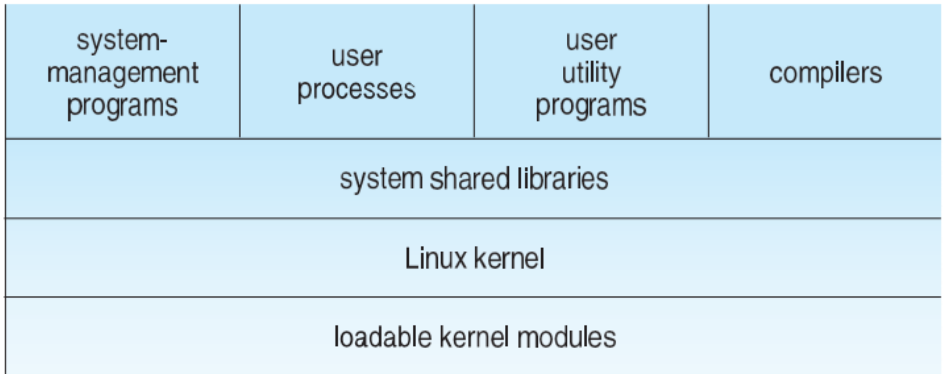
Linux is a multiuser, multitasking system with a full set of UNIX compatible tools.

Linux is a version of UNIX that was originally developed by Linus Torvalds at the University of Helsinki.

Linus made the software available for free following the concept of the **Open-Source community.**

Linux makes his code available for free to anyone who wants it, but in exchange, any changes that are made must be made available to the community.

Note// Linux runs on computers using Intel 386 or faster processors.



Advantages

- Easy to install.
- Fast.
- Reliable.
- It runs on PCs, PowerPCs, and SPARC stations.
- It’s free online.
- Hundreds of free software applications.
- bugs and security threats are fixed much faster than in any other NOS.

Disadvantages

- hundreds of commands and applications to learn.
- requires a UNIX administrator.
- Only a few companies offer dedicated tech support for Linux for a fee.
- If you are relying on Linux as your primary server, then budget for phone support and an experienced consultant.
- Linux is currently not considered a replacement for critical applications that require UNIX.

Mac OS X Server

It is UNIX with a Mac face.

The core of Mac OS X Server is based on two versions of UNIX. BSD UNIX and Mach

OS X server can run almost any version of UNIX software that runs on the Mach kernel and Free BSD.

Mac OS X Server, released in March of 1999.

Note// Apple source code, available for free Like any version of UNIX.

Mac OS X Server has several standards-based applications such as

- Standards-based DNS, FTP, and DHCP.
- Apache Web server.
- Mail Server with WebMail.
- Network File Sharing (NFS)
- Directory services such as Windows, Novell, and UNIX, using Netinfo and LDAP.

Mac OS X Server supports these additional features.

- user-friendly management tool called Server Admin.
- Seamless client support for all versions of Windows.
- Quicktime streaming server for on-demand video for the Web.
- Command-line access to all configuration features just like UNIX

Advantages

- improved server security
- It’s based on the reliable BSD UNIX and Mach software.
- It includes many standard Internet server applications, including Apache Web server.
- supports centralized management.
- Its Open Directory architecture
- A rack mount server, called Xserve, is now available and is only 1.75 inches high.

Disadvantages

- it’s less proven than other NOSs.
- does not support existing Macintosh Server applications.
- The performance is limited to the hardware options available from Apple.

Chapter 3

Distributed systems architectures

Client-server architectures

Distributed services which are called on by clients. Servers that provide services are treated differently from clients that use services.

Distributed object architectures

No distinction between clients and servers. Any object on the system may provide and use services from other objects.

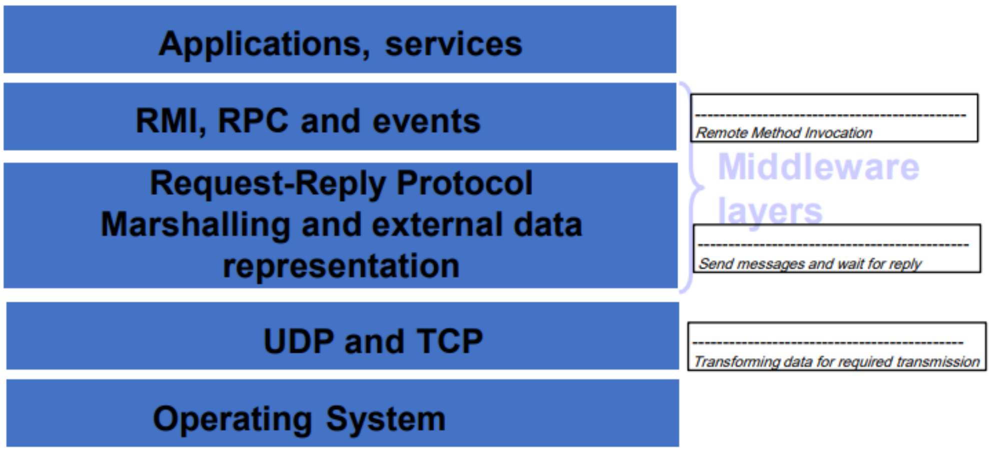
Middleware

Software that manages and supports the different components of a distributed system.

Note// Middleware is usually off-the-shelf rather than specially written software.

Examples

- Transaction processing monitors.
- Data converters.
- Communication controllers.



Reasons for Distributed Systems

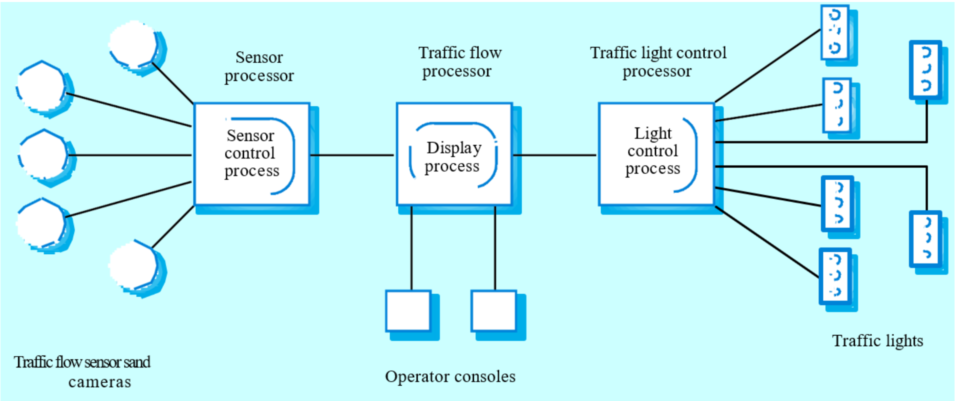
1- **Resource sharing**
Sharing files or printing at remote sites Processing information in a distributed database.
2- **Computation speedup**
Distribute sub computations among various sites stored concurrently.
3- **Load balancing**
moving jobs to more lightly loaded sites.
4- **Reliability**
Detect and recover from site failure, function transfer, reintegrate failed site.

Multiprocessor architectures

Simplest distributed system model.

Distribution of process to processor may be pre-ordered or may be under the control of a **dispatcher**.

A multiprocessor traffic control system

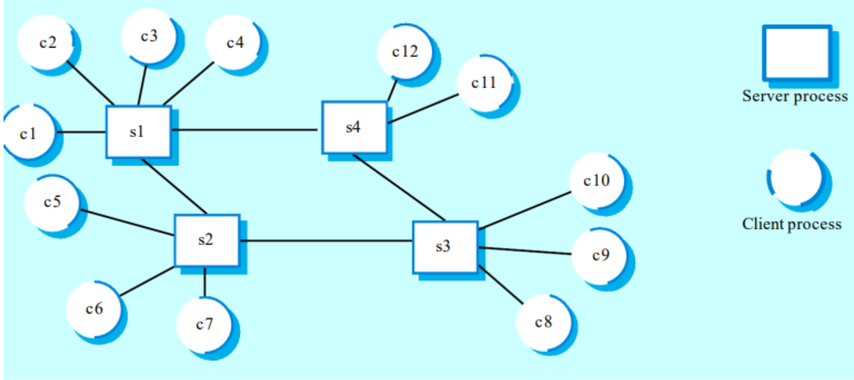


Client-server architectures

The application is modelled as a set of services that are provided by servers and a set of clients that use these services.

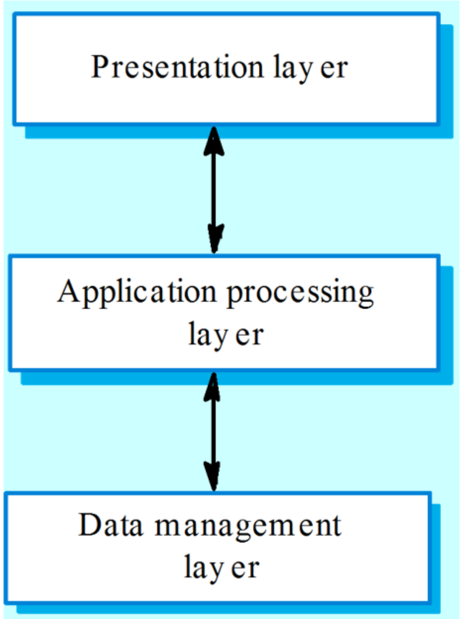
Clients and servers are logical processes.
The mapping of processors to processes is not necessarily 1:1.

Note// Clients know of servers but servers need not know of clients.



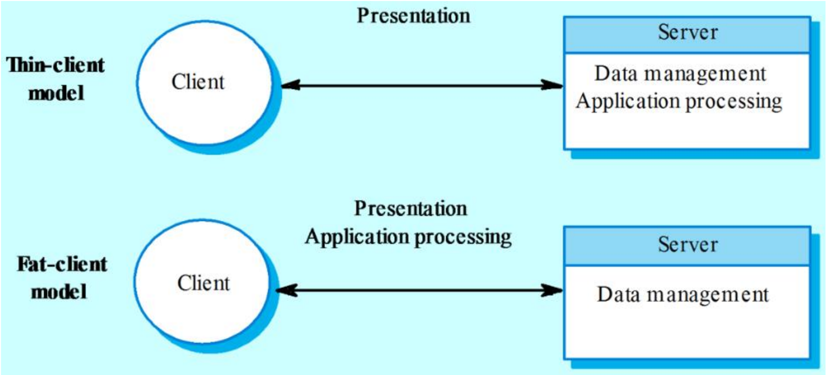
Layered application architecture

1- **Presentation layer**
   Concerned with presenting the results of a computation to system users and with collecting user inputs.
2- **Application processing layer**
   Concerned with providing application specific functionality. Ex: in a banking system, banking functions such as open account, close account, etc.
3- **Data management layer**
   Concerned with managing the system databases.



Thin and fat clients

- **Thin-client model**
  All the application processing and data management is carried out on the server.
  The client is simply responsible for running the presentation software.
- **Fat-client model**
  The server is only responsible for data management.
  The software on the client implements the application logic and the interactions with the system user.



Thin client model

Used when legacy systems are migrated to client server architectures.

A major **disadvantage** is that it places a **heavy processing load** on both the **server** and the **network**.

Fat client model

More processing is delegated to the client as the application processing is locally executed.

Most **suitable** for new C/S systems where the capabilities of the client system are known in advance.

More **complex** than a thin client model especially for management. New versions of the application have to be installed on all clients.

Chapter 4

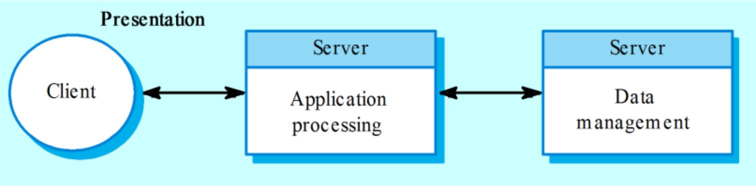
Three-tier architectures

In a three-tier architecture, each of the application architecture layers may execute on a separate processor.

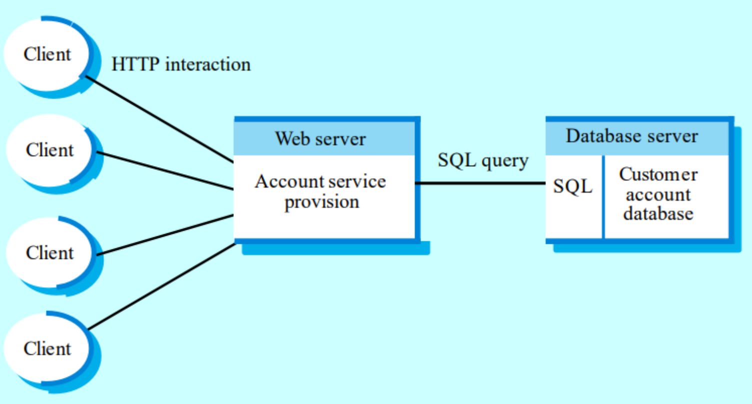
Note// It Allows for better performance than a thinclient approach and is simpler to manage than a fat-client approach.

Note// A **more scalable** architecture - as demands increase, extra servers can be added.

A 3-tier C/S architecture



An internet banking system



Distributed object architectures

Each distributable entity is an object that provides services to other objects and receives services from other objects.

Note// Object communication is through a **middleware** system called an **object request broker**.

Note// There is no distinction in a distributed object architectures between clients and servers.

Note// distributed object architectures are more complex to design than C/S systems.

Distributed Operating Systems

Users not aware of multiplicity of machines.

Access to remote resources similar to access to local resources

- **Data Migration**
  transfer data by transferring entire file,or transferring only those portions of the file necessary for the immediate task.
- **Computation Migration**
  transfer the computation, rather than the data, across the system.
  - Via remote procedure calls (RPCs)
  - Via messaging system
- **Process Migration**
  execute an entire process, or parts of it, at different sites.

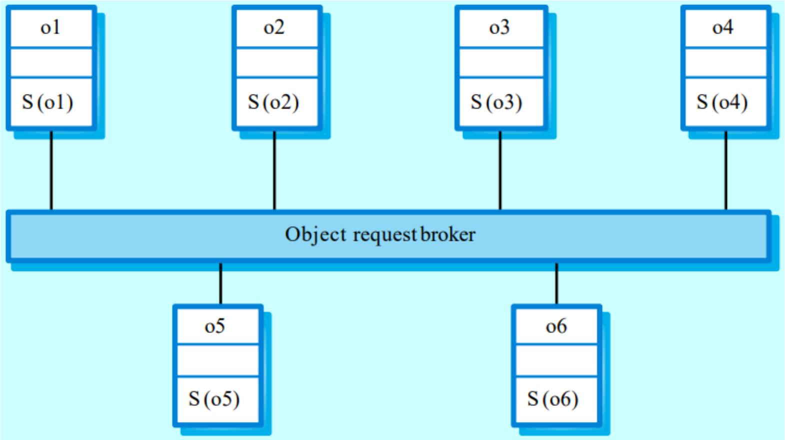
- **Load balancing**
  distribute processes across the network to reduce the workload.
- **Computation speedup**
  sub-processes can run concurrently on different sites.
- **Hardware preference**
  process execution may require specialized processor.
- **Software preference**
  required software may be available only at a particular site.
- **Data access**
  run process remotely, rather than transfer data locally.

Design Issues of Distributed Systems

We investigate three design questions

1. **Robustness**
   Can the distributed system withstand failures?
2. **Transparency**
   Can the distributed system be transparent to the user both in terms of where files are stored and user mobility?
3. **Scalability**
   Can the distributed system be scalable to allow the addition of more computation power, storage, or users?

Distributed object architecture



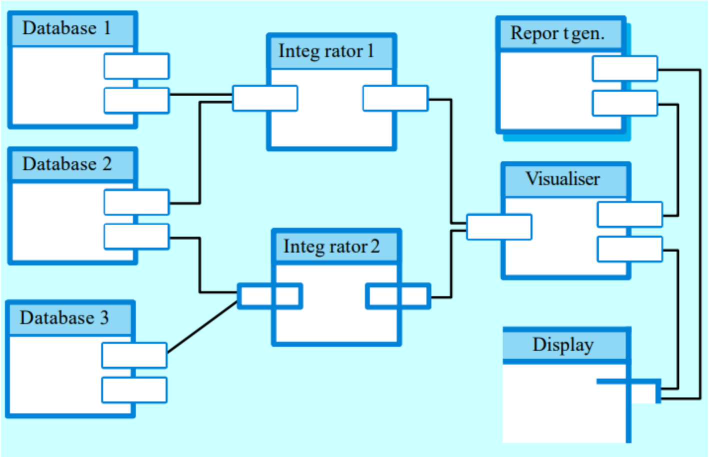
Advantages of distributed object architecture

- It allows the **system designer to delay decisions** about where and how services should be provided.
- It is a **very open system architecture** that allows new resources to be added to it as required.
- The system is **flexible** and **scalable**.
- It is possible to reconfigure the system **dynamically** with objects migrating across the network as required.

Uses of distributed object architecture

logical model that allows you to structure and organize the system as a flexible approach in which objects are communicating through a **common communication framework.**

A data mining system



Data mining system

It allows the number of databases that are accessed to be increased without disrupting the system.

Note// It allows **new types of relationships** to be mined by adding **new integrator objects**.

CORBA (Common Object Request Broker Architecture)

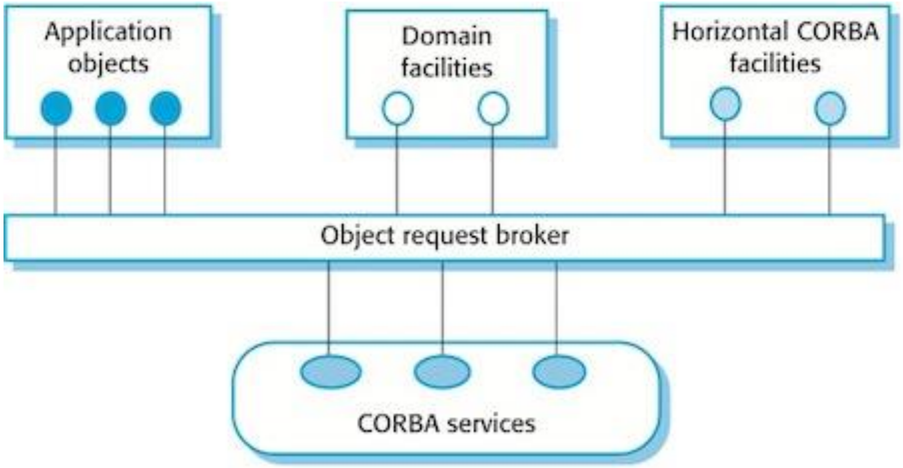
It is a middleware to manage communications between distributed objects.

Note// CORBA is an international standard for an Object Request Broker

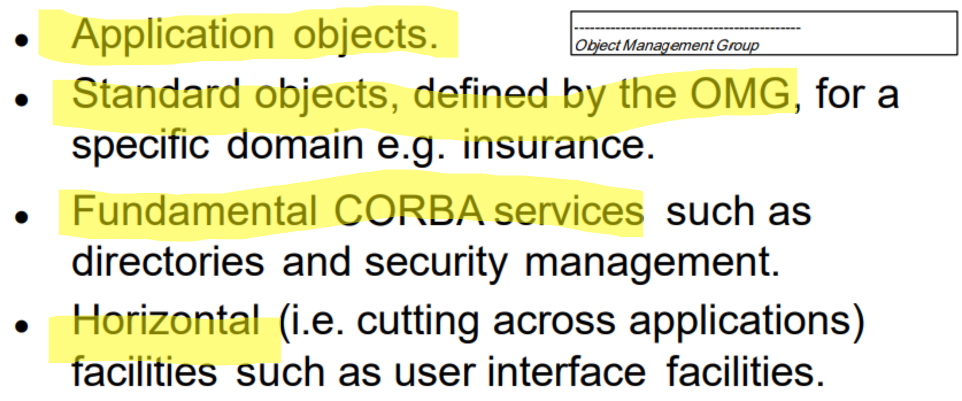
Middleware for distributed computing is required at 2 levels:

1. **At the logical communication level**
   the middleware **allows** objects on different computers **to exchange data and control information.**
2. **At the component level**
   the middleware provides a basis for **developing compatible components.**

CORBA application structure



Application structure



- Application objects.
- Standard objects, defined by the OMG, for a specific domain e.g. insurance.
- Fundamental CORBA services such as directories and security management.
- Horizontal (i.e. cutting across applications) facilities such as user interface facilities.

Object Management Group

CORBA standards

- An object model for application objects
  A CORBA object is an encapsulation of state with a well-defined, language-neutral interface defined in an **IDL (interface definition language).**
- An object request broker that manages requests for object services.
- A set of general object services of use to many distributed applications.
- A set of common components built on top of these services.

CORBA objects

CORBA objects are comparable, in principle, to objects in C++ and Java.

Note// They **MUST** have a separate interface definition that is expressed using a common language (IDL) similar to C++.

Note// There is a mapping from this **IDL** to programming languages (C++, Java, etc.).

Therefore, objects written in different languages can communicate with each other.

CORBA services

- **Naming and trading services**
  These allow objects to discover and refer to other objects on the network.
- **Notification services**
  These allow objects to notify other objects that an event has occurred.
- **Transaction services**
  These support atomic transactions and rollback on failure.

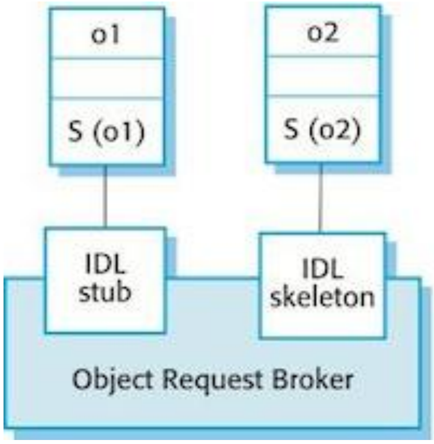
ORB (Object Request Broker)

The ORB handles object communications. It knows of all objects in the system and their interfaces.

Note// Using an ORB, the calling object binds an IDL stub that defines the interface of the called object.

Calling this stub results in calls to the ORB which then calls the required object through a published IDL skeleton that links the interface to the service implementation.

ORB-based object communications



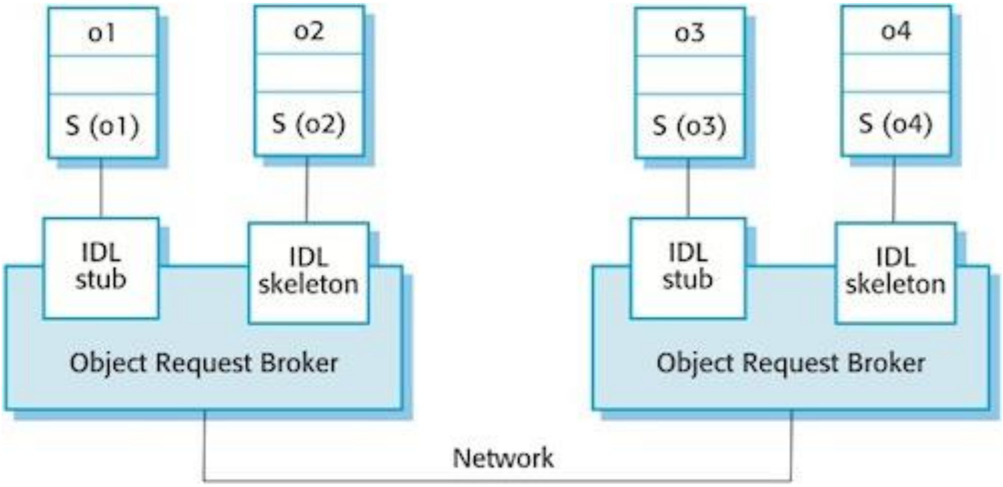
Inter-ORB communications

Inter-ORB communications are used for distributed object calls.

ORBs handle communications between objects executing on the same machine.

Note// ORBs are not usually separate programs but are a set of objects in a library that are linked with an application when it is developed.

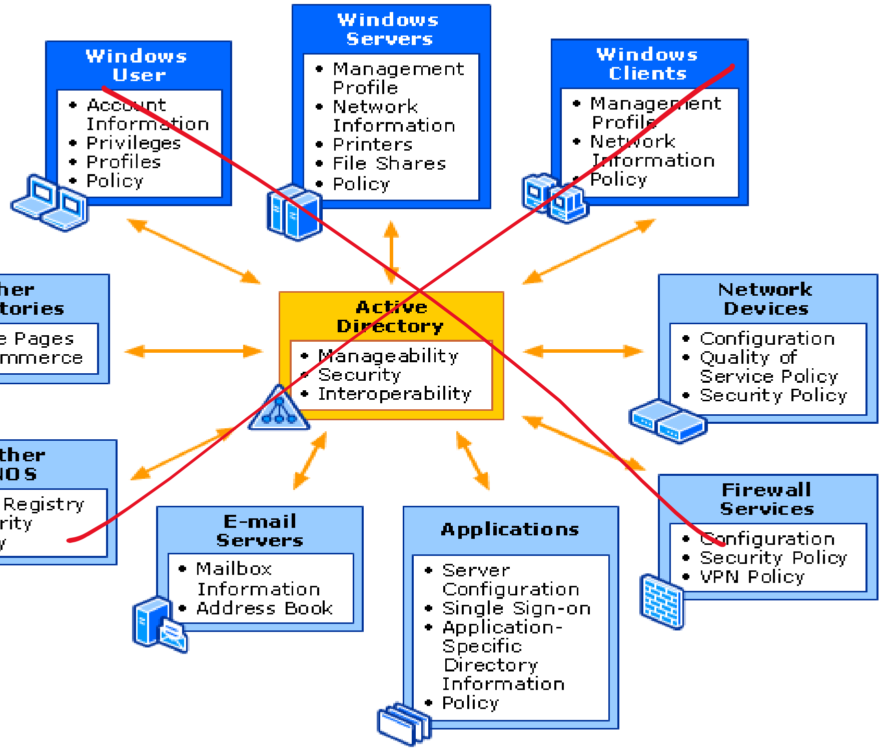
Note// Several ORBs may be available and **each computer** in a distributed system will **have its own ORB**.



Chapter 5

Active Directory service

An extensible and scalable directory service that uses a namespace based on the DNS.



///↓///

System Components

Layered system of modules operating at specific privilege layers Kernel and user mode of course

Virtual Trust Levels (VTLs) option implemented by Hyper-V virtualization.

Normal World(VTL0) and **Secure World(VTL1)** Within each world are user and kernel modes.

Secure world has a secure kernel and executive and a collection of **trustlets (trusted/secure processes)**

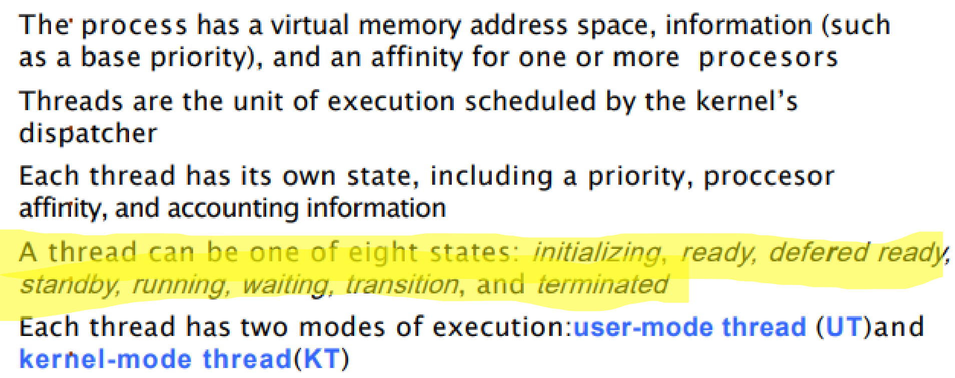
Bottom most layer runs in special processor mode (VMX Root Mode on Intel) including Hyper-V hypervisor, creating hardware-based normal-tosecure-world boundary.

System Components — Kernel

- Foundation for the executive and the subsystems
- Never paged out of memory; execution is never preempted

  Four main responsibilities:
  - Thread scheduling
  - Interupt and exception handling
  - low–level processor synchronization
  - recovery after a power failure
- Kernel is object–oriented ,uses two sets of objects
  - *Dispatcher objects* control dispatching and synchronization (events, mutants, mutexes, semaphores, threads and timers)
  - *Control objects* (asynchronous procedure cals,interupts, power notify, power status, process and profile objects)
- Virtual Secure Mode (VSM)Enclaves allow valid signed third–party code to perform crypto calculations

Kernel — Process and Threads



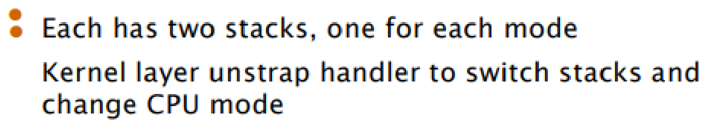
The process has a virtual memory address space, information (such as a base priority), and an affinity for one or more procesors

Threads are the unit of execution scheduled by the kernel's dispatcher

Each thread has its own state, including a priority, proccesor affinity, and accounting information

A thread can be one of eight states: *initializing, ready, defered ready, standby, running, waiting, transition*, and *terminated*

Each thread has two modes of execution:user-mode thread (UT)and kernel-mode thread(KT)



- Each has two stacks, one for each mode

  Kernel layer unstrap handler to switch stacks and change CPU mode

Kernel — Scheduling

Scheduling can occur when a thread enters the ready or wait state

Real-time threads are given preferential access to the CPU; but 10 does not guarante that a real-time thread will start to execute within any particular time limit (**This is known as soft realtime**)

//↑//

IntelliMirror

mirroring of user data and environment settings as well as central management of software installation and maintenance.

Security Architecture

smart cards, public and private encryption keys, and security protocols.

Terminal Services

allow you to remotely log on to and manage other Windows Server systems.

Windows Script Host

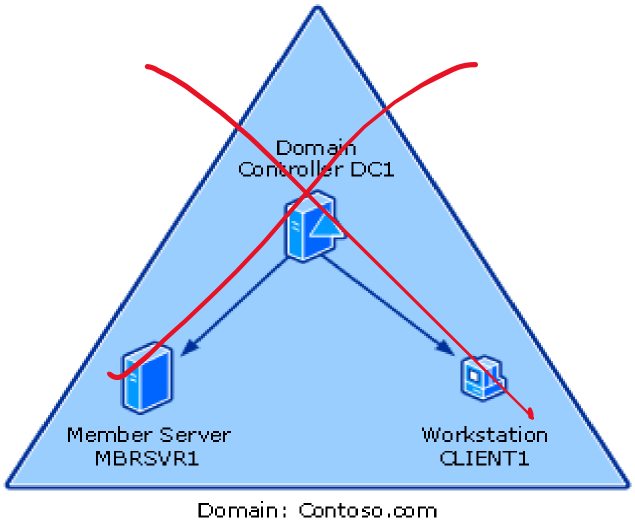
scripting environment for automating common administration tasks

Domain Controllers and Member Servers

Note// When you install Windows Server on a new system, you can configure the server to be **member server**, a **domain controller**, or a **stand alone server**.

- **Member servers**
  part of a domain but don't store directory information.
- **Domain controllers**
  are distinguished from member servers because
  - **they store directory information.**
  - And **provide authentication and directory services** for the domain.
- **Stand-alone servers**
  aren't a part of a domain And have their own user database.

Domain Controller



Windows Server doesn't designate **primary or backup domain controllers**.

It supports a **multimaster replication model**.

In this model any domain controller can process directory changes and then replicate those changes to other domain controllers automatically.

This differs from the **Windows NT single master replication model.**

In which the primary domain controller stores a master copy and backup controllers store backup copies of the master.

Note// Domains that use Active Directory are referred to as **Active Directory domains**.

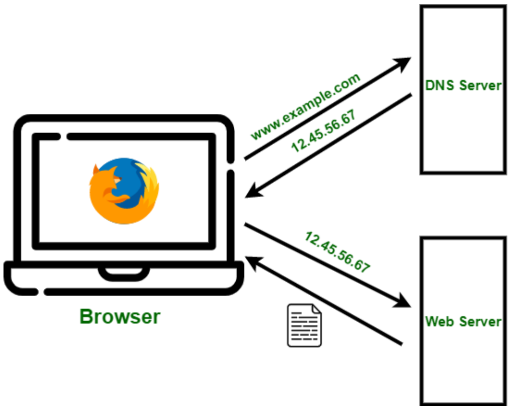
Note// **Active Directory domains** can function with **only one domain controller**.

Server Roles

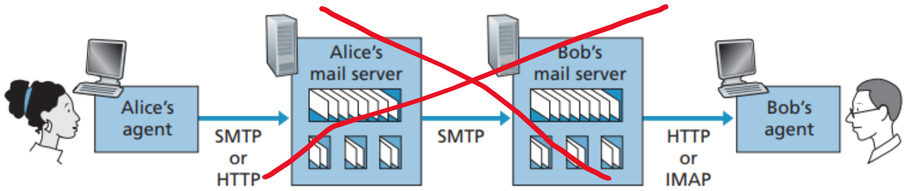
Note// Any server can support one or more of the following server roles.

- **Application server**
  provides XML Webservices, Web applications, and distributed applications.
  Note// When you configure a server with this role – IIS, COM+, and the Microsoft .NET Framework are installed automatically.

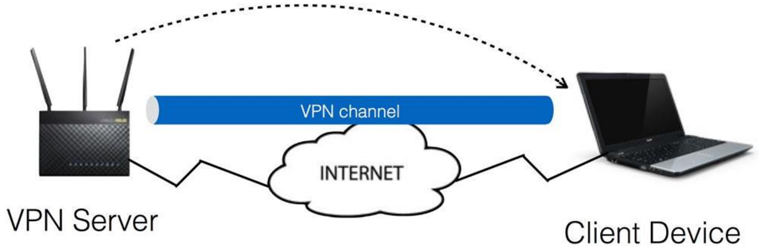
- **DNS server**
  A server that runs DNS resolves computer names to IP addresses and vice versa.
  Note// This option installs DNS and starts the DNS Server Wizard.



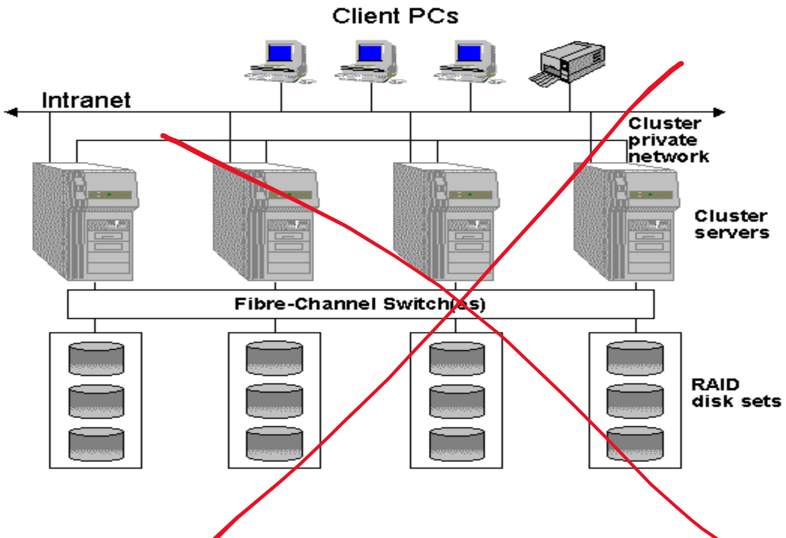
- **Mail server (POP3, SMTP)**
  A server that provides basic Post Office Protocol3 (POP3), Simple Mail Transfer Protocol (SMTP) mail services. so that POP3 mail clients can send and receive mail in the domain.



- **Remote access / VPN server**
  A server that routes network traffic and manages dial-up networking or VPN.
  Note// This option starts the Routing and Remote Access Setup Wizard.



- **Server cluster node**
  A server that operates as part of a group of servers working together called a cluster.



- **Streaming media server**
  A server that provides streaming media content to other systems on the network or the Internet.
- **Terminal Server**
  A server that processes tasks for multiple client computers running in terminal services mode.
- **WINS Server**
  A server that runs Windows Internet Name Service (WINS)
  resolves NetBIOS names to IP addresses and vice versa.

Frequently Used Tools

- **Control Panel**
  A collection of tools for managing system configuration.
- **Graphical administrative tools**
  The key tools for managing network computers and their resources.
  Note// You can access these tools by selecting them individually on the Administrative Tools submenu.
- **Administrative wizards Tools**
  designed to automate key administrative tasks.
  Note// Unlike in Windows NT, there's no central place for accessing wizards.
- **Command-line utilities**
  You can launch most administrative utilities from the command line.

Control Panel Utilities

1. **Add Hardware**
   Starts the Add Hardware Wizard, which you can use to install and troubleshoot hardware.
2. **Add Or Remove Programs**
   Used to install programs and to safely uninstallprograms.
   Note// Also used to modify Windows Server 2003 setup components.
3. **Date And Time**
   Used to view or set a system's date, time, and time zone.
4. **Display**
   Used to configure backgrounds, screen savers, video display mode, and video settings.
5. **Folder Options**
   Used to set a wide variety of folder and file options
6. **Licensing**
   On a workstation you use this utility to manage licenses on a local system.
7. **Network Connections**
   Used to view network identity information to add network components and to establish network connections.
8. **Printers And Faxes**
   Provides quick access to the Printers And Faxes folder
9. **Scheduled Tasks**
   Allows you to view and add scheduled tasks.
   Note// You can schedule tasks on a one-time or recurring basis to handle common administrative jobs.
10. **System**
    Used to display and manage system properties
    - Startup/shutdown
    - environment
    - hardware profiles
    - user profiles

Command-Line Utilities

1. **ARP**
   Displays and manages the IP-to-Physical mappings.
2. **AT**
   Schedules programs to run automatically.
3. **DNSCMD**
   Displays and manages the configuration of DNS services.
4. **FTP**
   Starts the built-in FTP client.
5. **HOSTNAME**
   Displays the computer name of the local system.
6. **IPCONFIG**
   Displays the TCP/IP properties for network adapters installed on the system.
7. **NBTSTAT**
   Displays current connections for NetBIOS over TCP/IP.
8. **NET**
   Displays a family of useful networking commands.
9. **NETSH**
   Displays configuration of local and remote computers.
10. **NETSTAT**
    Displays TCP/IP connections and protocol statistics.
11. **NSLOOKUP**
    Checks the status of a host or IP address when used with DNS.
12. **PATHPING**
    Traces network paths and displays packet loss information.
13. **PING**
    Tests the connection.
14. **ROUTE**
    Manages the routing tables on the system.
15. **TRACERT**
    During testing, determines the network path taken to a remote host.

NET Tools

1. **NET SEND**
   Sends messages to users.
2. **NET START**
   Starts a service on the system.
3. **NET STOP**
   Stops a service on the system.
4. **NET TIME**
   Displays the current system time.
5. **NET USE**
   Connects and disconnects from a shared resource.
6. **NET VIEW**
   Displays a list of network resources.

Chapter 6

Physical and Logical Devices (Managing and Maintaining)

A large part of managing and maintaining **any network environment involves**:

- network hardware is configured and functioning correctly.

A **network administrator** will be **responsible** for:

- installing and configuring server hardware devices
- managing server disks
- generally ensuring that devices are performing optimally.

Key tools that are used to **manage server hardware** and related settings include:

- Control Panel applets
- Device Manager
- Computer Management MMC.

A **proactive approach** to network management and maintenance will help to

- ensure that server hardware problems are minimized.
- there will still be times when problems occur without warning.
- network administrator be able to identify the problem.
- using the various tools provided to minimize the potential impact to network users.

Managing Users, Computers, and Groups

One of the most **common day-to-day tasks** encountered by **a network administrator** is:

- the administration of user accounts.
- New user accounts need to be created.
- existing settings may need to be changed.
- users will invariably forget their passwords from time to time.
- management and maintenance of user accounts.
- can consume a great deal of time and energy for any administrator.

To help **alleviate some of this burden**, Windows Server Active Directory includes

- **A variety of new tools and features**
  that allow an administrator to automate and simplify many account related tasks.
  For example, the primary user administration tool, Active Directory
- **Users and Computers, now supports**
  drag-and-drop functionality to make moving objects easier.
- **Windows Server supports**
  a number of different group types and scopes.
  Groups can be created for the purpose of assigning network rights and permissions to multiple users, As well as to create distribution lists for e-mail.

Once **network objects are created** and settings are configured

- an administrator is still responsible for troubleshooting related problems as they arise.
- administrator must be familiar with the authentication process
- administrator must be familiar with the different policy settings
- One of the most common tasksfor a network administrator involves resetting forgotten user passwords.

Access to Resources (Managing and Maintaining)

The primary reason for implementing a network is to allow users to share resources.

An administrator not only needs to ensure that resources are accessible to users but also that **they are properly secured**.

Windows Server provides two main **methods** of **securing resources**

1. **shared folder permissions**
   Shared folder permissions are only applicable when a user tries to access a resource over a network.
2. **NTFS permissions**
   Note// NTFS (New Technology File System)
   NTFS permissions apply both locally and remotely.

In Windows Server, resources are made available to network users via a technique known as **sharing**.

Terminal Services

Terminal Services allows a user to connect to a central server and access applications as though working from the user desktop.

Note// This is a popular method of granting users access to certain applications without the need to deploy those applications to all desktops.

Note// Terminal Services is one of Windows Server services.

Server Environment (Managing and Maintaining)

A network administrator needs to be familiar with a wide variety of software tools and concepts.

aimed not only at management, but also the monitoring of resources.

tools to monitor and troubleshoot a server environment.

1. **Event Viewer**
   Event Viewer handles
   - the primary event logging
   - creating entries when any event occurs.
   - When an error occurs, Event Viewer should be the main tool accessed by a network administrator to gather information.
2. **System Monitor**
   System Monitor tool allows an administrator to gather
   - current performance information
   - that can be compared against the baseline of normal performance.

Both tools are key utilities in helping an administrator identify problem areas or performance issues.

Note// Timely application of software patches and security updates is another key maintenance task for the network administrator.

Microsoft has released a tool known as **Software Update Services (SUS)**

for managing updates in a centralized manner.

An administrator should be familiar with the **disk quota** feature of Windows Server

which allows an administrator to control the amount of disk space allocated and available to each user.

Microsoft Management Console (MMC)

provides an administration framework that allows different tools (known as **snapins**) to be added in custom configurations for different management and maintenance tasks.

Disaster Recovery (Managing and Implementing)

This focus area concentrates on tasks that ensure both **data and system settings are properly backed up.**

and then available in cases like the **failure** of a server or the **accidental deletion** of files.

Windows Backup

An administrator should be familiar with both **backing up** and **restoring** System State information using the Windows Backup tool.

Note// Windows Backup is the backup tool provided with Windows Server.

Automated System Recovery

Allows administrator to create a floppy disk to which critical configuration information will be copied.

Allowing a server OS to be restored using disk and the Windows Server installation media.

Another new and important feature in Windows Server is **Shadow Copies of Shared Folders**.

Note// Automated System Recovery is a new feature in Windows Server

Shadow Copies of Shared Folders

is a feature that maintains previous versions of files on a server in a manner accessible to individual users.

In the event that the current copy of a file has been deleted or overwritten, Shadow Copies of Shared Folders allows a user to restore a previous version of the file without having to contact an administrator.

Active Directory

Active Directory provides the following services and features to the network environment:

- A **central point** for storing, organizing, managing, and controlling network objects.
  such as users, computers, and groups
- **A single point of administration of objects.**
  such as users, groups, computers, and Active Directory-published resources, – such as printers or shared folders
- **Logon and authentication**
- **Delegation of administration**
  to allow for decentralized administration of Active Directory objects

Active Directory database

The Active Directory database is stored in a domain controller.

- Each domain controller on the network has a writeable copy of the directory database.
- changes are replicated to all of the other domain controllers. // This process is called **multimaster replication**
- **multimaster replication** provides a form of fault-tolerance. If a **single server fails**, **Active Directory does not fail.**
  because replicated copies of the database are available from other servers within the network.

Active Directory uses the Domain Name Service (DNS) to maintain domain-naming structures and locate network resources.

Active Directory Objects

Active Directory stores a variety of objects within the directory database.

An object represents network resources. such as users, groups, computers, and printers.

Note// When an object is created in Active Directory, various **attributes** are assigned to it to provide information about the object.

Active Directory Schema

All of the objects and attributes that are available in Active Directory are defined in the Active Directory schema.

Note// This means that there is only one schema for a given Active Directory implementation and it is replicated among all domain controllers within the network.

The **Active Directory schema consists of two main definitions**:

1. **Object classes**
   Object classes define the types of objects that can be created within Active Directory.
   such as user objects and printer objects.
2. **Attributes**
   Attributes are created and stored separately in the schema and can be used with multiple object classes to maintain consistency.

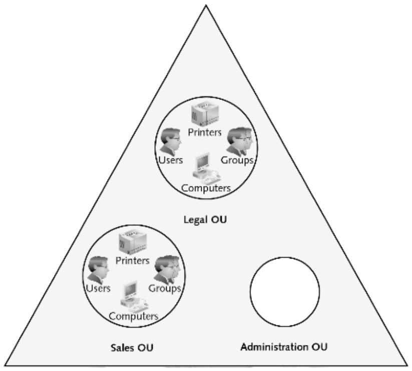
Note// The Active Directory database stores and replicates the schema partition to all domain controllers in an Active Directory environment.

Active Directory Logical Structure and Components

The **logical components** that make up an Active Directory structure include:

1. Domains and Organizational Units (OU)

- A Windows Server **domain** is a logically structured organization of objects.
  such as users, computers, groups, and printers that are part of a network
  share a common directory database.
  Note// Each domain has a unique name and is organized in levels administered as a unit with common rules and procedures.
- **Organizational unit (OU)** is a logical container used to organize objects within a single domain.
  Objects such as users, groups, computers
  and other OUs can be stored in an OU container.
  Another main advantage of using an OU structure is the ability to delegate administrative control over OUs.



2. Trees and Forests

A **tree** is a hierarchical collection of domains that share a contiguous DNS namespace.

Reasons for creating multiple domains within an organization include the following:

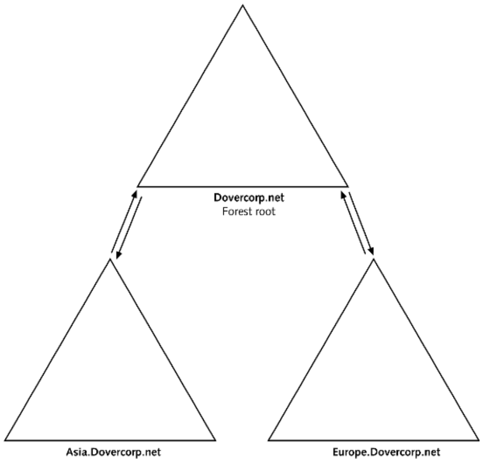
- Divisions within the company may be **administered on a geographic basis**.
  - To make administration easier
  - a separate domain is created for each division.
- **Different password policies** are needed between divisions within an organization.
- An **large number of objects** need to be defined.
- **Replication performance** needs to be improved.

Note// The first Active Directory domain created in an organization is called the **forest root domain.**

When multiple domains are needed, they are **connected to the forest root** to form either a **single tree** or **multiple trees.**

Note// Whenever a child domain is created, a two-way, **transitive trust relationship** is automatically created between the **child** and **parent domains**.

A **transitive trust** means that all other trusted domains implicitly trust one another.



A **forest** is a collection of trees. that do not share a contiguous DNS naming structure.

3. Global Catalog

A global catalog is an index and partial replica of the objects and attributes most frequently used throughout the entire Active Directory structure.

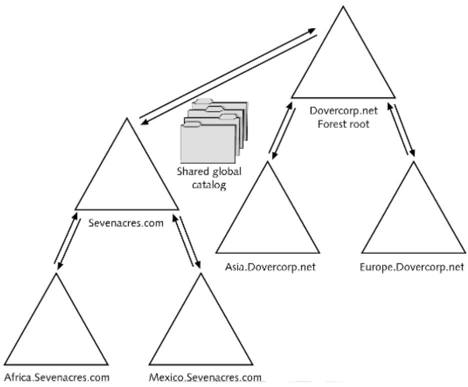
Some of the common attributes that are stored in a global catalog include:

- a user's first and last names, logon name, and e-mail address.

Note// A global catalog is replicated to any server within the forest that is configured to be a global catalog server.

A global catalog is used primarily for 4 main functions:

1) To **enable users to find Active Directory information** from anywhere in the forest.
2) To **provide universal group membership information** to facilitate logging on to the network.
3) To supply authentication services when a user from another domain logs on using a **User Principal Name (UPN).**
   A UPN is a representation of a user's logon credentials in the form user@domain.com.
4) Global catalog servers also host the **Exchange Global Address List(GAL).**



Active Directory Communications Standards

When users need to access Active Directory the **Lightweight Directory Access Protocol (LDAP)** is used to query or update the Active Directory database directly.

Just as a DNS name contains a specific naming convention (Example mansourhaneen.com) **LDAP** also follows a specific naming convention.

LDAP naming paths are used when referring to objects stored within the Active Directory.

- **Distinguished name**
  Every object in Active Directory has a unique **distinguished name (DN).**
- **Relative distinguished name**
  A portion of the distinguished name that uniquely identifies the object within the container is referred to as the **relative distinguished name (RDN).**

For example, the distinguished name

- OU=Marketing, DC=Dovercorp, DC=Net would have a relative distinguished name of OU=Marketing.
- For the distinguished name **CN=Moira** Cowan, OU=Marketing, DC=Dovercorp, DC=Net, the **relative distinguished name would be CN=Moira**

Active Directory Physical Structure

The Active Directory physical structure relates to the actual connectivity of the physical network itself.

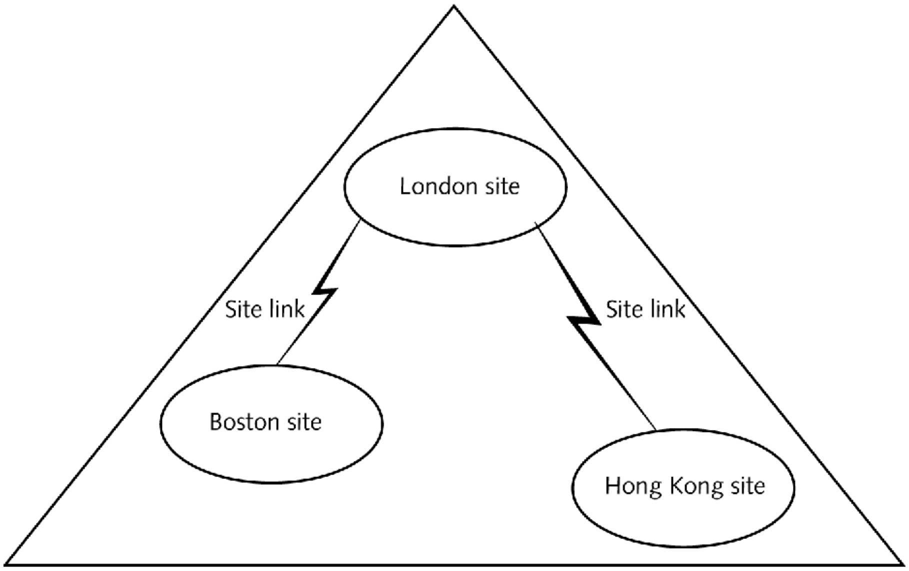
Because the Active Directory database is stored on multiple servers, You need to make sure that any modification database to the is replicated as quickly as possible between domain controllers.

You can control Active Directory replication and authentication traffic by configuring **sites** and **site links**.

Active Directory site is a combination of one or more Internet Protocol (IP) subnets connected by a high-speed connection.

A **site link** is a configurable object that represents a connection between sites.

Site links created using the Active Directory Sites and Services **snap-in** are the **core of Active Directory replication.**


London site
Site link
Site link
Boston site
Hong Kong site