Module 2

Analyze IP addressing: IPv4 and Ipv6

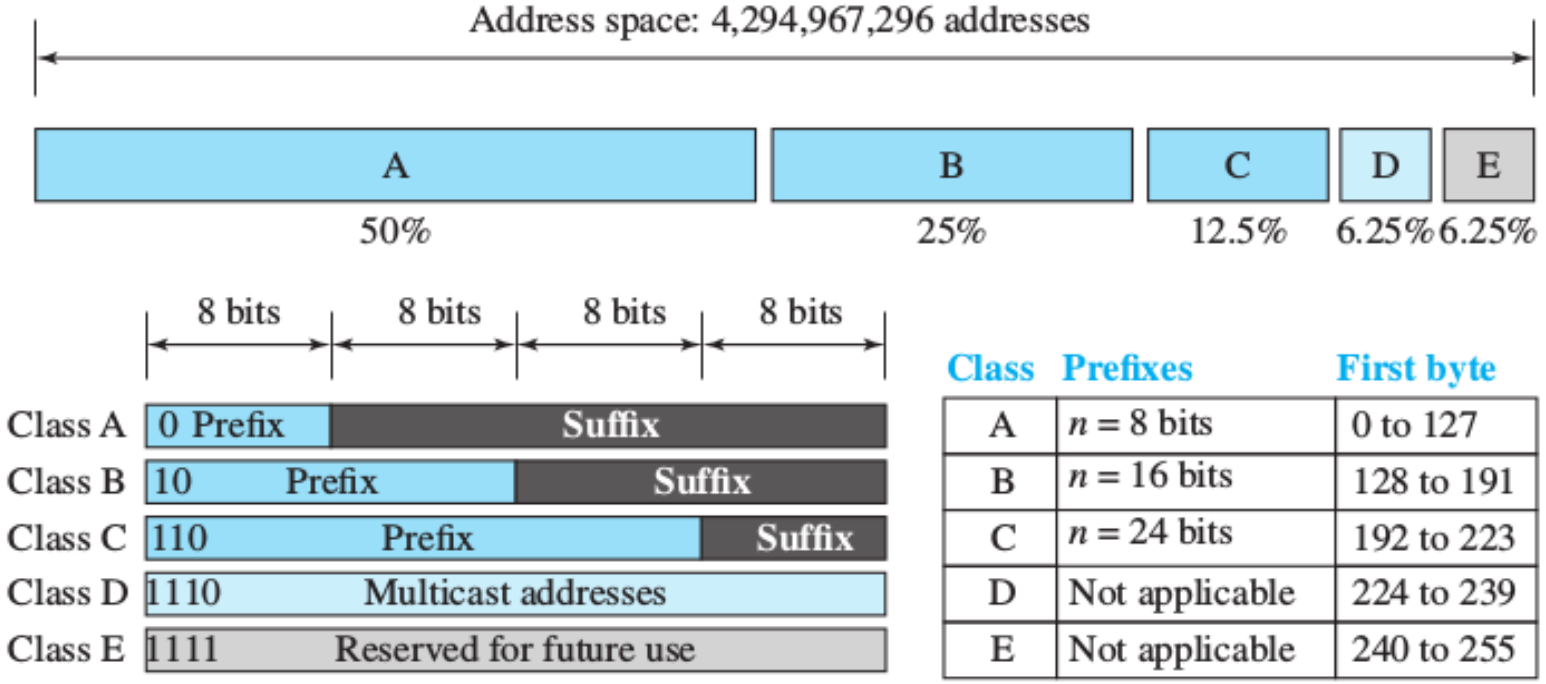
IPv4

>> 32 bits. Represented as **dotted decimal notation**. (x.x.x.x where x=0 to 255)

>> Each address is divided into two parts: Network (prefix; N bits) and host (suffix; 32-N bits).

>> Based in the number of hosts a network can handle and purpose of the IP address, the address space is divided into 5 classes: A to E; each class has a range based on first few bits (fig.).

>> Each IP address has a Network Address and a Broadcast Address. When all the host bits are zeros, that address is called the network address. When all host bits are ones it is the broadcast address of that network.



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Analyze IP addressing: IPv4

>> The first network 0.x.x.x is not used for addressing. 0.0.0.0 is the 'this host' address when the device is just booted up.

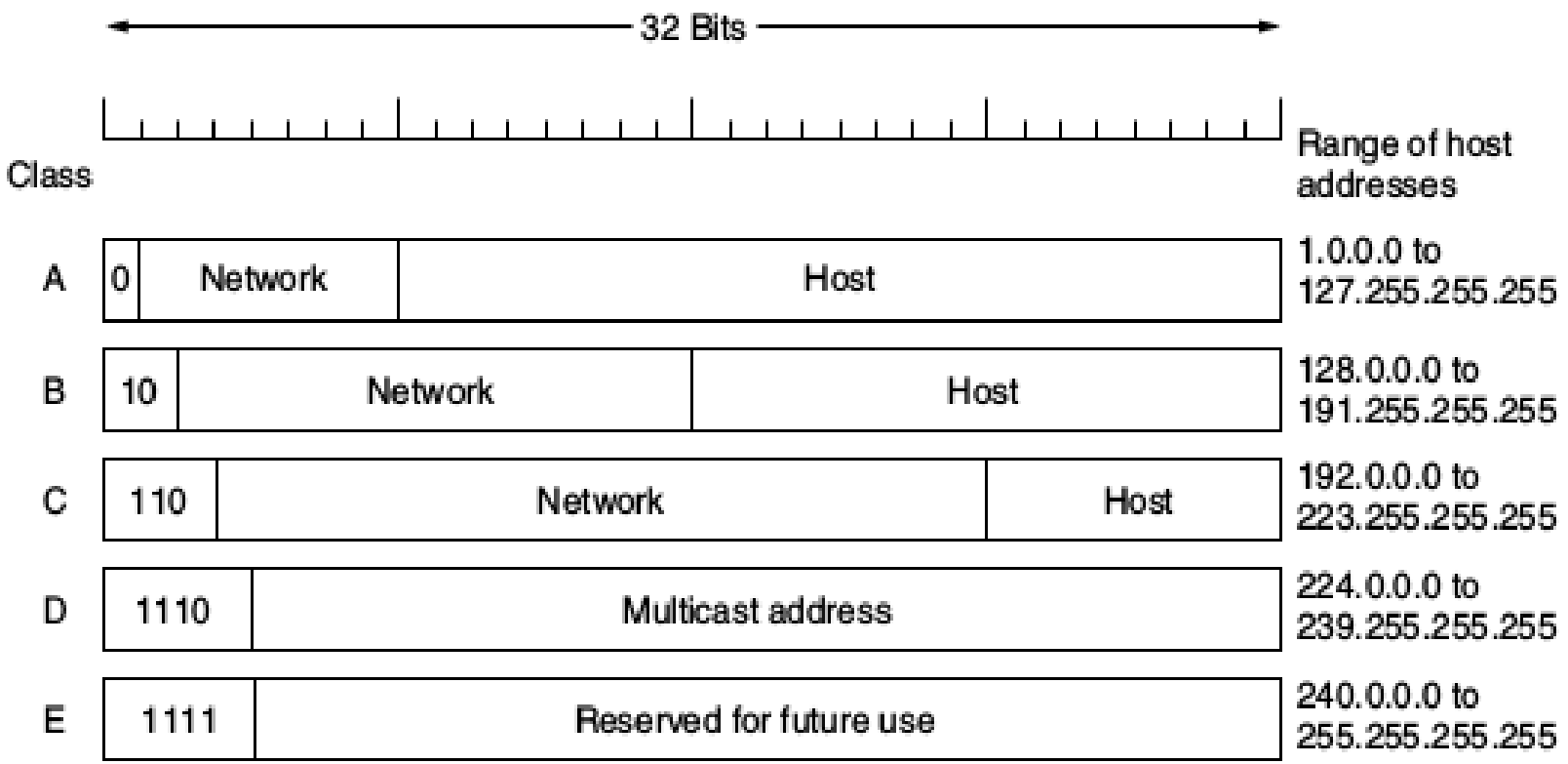
>> The network 127.x.x.x is used as loopback address to test the network card functionality.

>> Class A: 128 (actually 126) networks with 16 million hosts each.

>> Class B: 16,384 networks with up to 65,536 hosts each.

>> Class C: 2 million networks (e.g., LANs) with up to 256 hosts each.

>>Class D and E addresses are not used for public / private IP addressing.



Analyze IP addressing: IPv4...

>> Each class (A,B,C) has a range of IP addresses to be used as private IP addresses (inside local networks; LANs). These are not visible to public address space and cannot be used as public IP addresses. They are;

Class A: 10.x.x.x (one network)

Class B: 172.16.x.x to 172.31.x.x (16 networks)

Class C: 192.168.x.x (256 networks with 254 hosts each)

>> A special address block 169.254.x.x is used as link local addresses which is obtained to a system when IP functionality fails (eg: DHCP failure). Microsoft termed this addressing as Automatic Private IP Addressing (APIPA).

Subnet mask

>> In order to find the network address of an IP address, the systems use a special type of address called subnet mask.

>> It is obtained by making all the network part bits to ones and host part bits to zeros. ANDing this address with the IP address will result in the exact Network Address.

>> Eg: For class C address, say 192.168.2.6, the first three bytes forms the network part. Thus 255.255.255.0 is the subnet mask of this address. ANDing this with the IP address gives 192.168.2.0 as the network address.

Analyze IP addressing: IPv4...

>> As the IPv4 addresses get exhausted and small firms may get large network addresses resulting in the wastage of IP addresses (and vice versa) Classless addressing came.

>> Here the network bits are selected based on the need and not on the class. And the number of network bits are represented as slash notations just after the IP address. Such notations are called Classles Inter Domain Routing (CIDR) notations.

eg: We have a network 192.168.2.0. With classful addressing we can have only one network, total 254 hosts. But if we need four different networks of each with say 50 hosts, we can use classless addressing. With 6 bits we can create 64 host addresses (only 62 can be used). Thus 32-6=26 bits can be in the network part. Thus 192.168.2.0/26 can be the network.

192.168.2.*00 000000* – 192.168.2.0	Network 1
192.168.2.*00 000001* – 192.168.2.1	First host
192.168.2.*00 111110* – 192.168.2.62	Last host
192.168.2.*00 111111* – 192.168.2.63	Broadcast 1
192.168.2.*01 000000* – 192.168.2.64	Network 2
192.168.2.*01 000001* – 192.168.2.65	First host
192.168.2.*01 111110* – 192.168.2.126	Last host
192.168.2.*01 111111* – 192.168.2.127	Broadcast 2
192.168.2.*10 000000* – 192.168.2.128	Network 3
192.168.2.*10 000001* – 192.168.2.129	First host
192.168.2.*10 111110* – 192.168.2.190	Last host
192.168.2.*10 111111* – 192.168.2.191	Broadcast 3
192.168.2.*11 000000* – 192.168.2.192	Network 4
192.168.2.*11 000001* – 192.168.2.193	First host
192.168.2.*11 111110* – 192.168.2.254	Last host
192.168.2.*11 111111* – 192.168.2.255	Broadcast 4

Subnet mask
255.255.255.*11 000000*
ie, 255.255.255.192

IPv6

- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with IPv4 address exhaustion.
- 128 bit length allows 2^{128} addresses.
- IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons.
- Eg: 2001:0db8:0000:0042:0000:8a2e:0370:7334
- The address can be shortened by
    - Removing leading zeroes (0042 becomes 42)
    - Replacing full-zero sections with double colon (::); but only once in an address.
- Thus the above address will become 2001:db8::42:0:8a2e:370:7334
- The loopback address, 0000:0000:0000:0000:0000:0000:0000:0001, may be abbreviated to ::1
- Similar to APIPA in IPv4, v6 also use an auto-IP called link local address. This address starts with FE80 and all other bits in the first 64 bits are zeros. The next 64 bits are obtained by inserting FF:FE in between the MAC address of the interface and seventh bit of the MAC address is flipped.
- Eg: MAC- b4:81:f4:db:d4:ee. Flipping the seventh bit: *b4* becomes *b6*. Now insert FF:FE in between f4:db. Now the last 64 bits becomes b681:f4ff:fedb:d4ee. Thus the link local address becomes fe80::b681:f4ff:fedb:d4ee

Workgroups

>> Workgroup is Microsoft's term for peer-to-peer local area network.

>> Computers running in the same workgroup may share files, printers, or Internet connection.

>> Joining a workgroup requires all participants to use a matching name. Windows' default workgroup name is WORKGROUP (or MSHOME in Windows XP).

>> Admin users can change the workgroup name from Control Panel.

>> Windows workgroups can contain many computers but work best with 15 or fewer.

>> The open source software package Samba allows Apple macOS, Linux, and other Unix-based systems to join existing Windows workgroups.

>> Each computer maintains its own database of security principles.

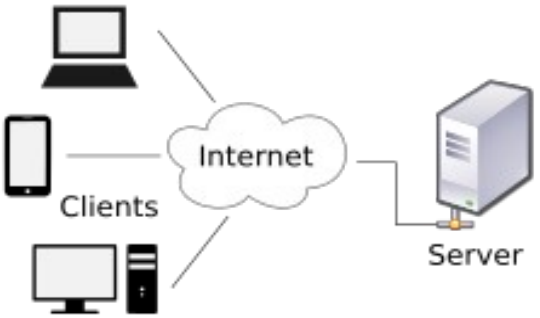
>> It is easier to set up and configure than a domain.

>> Its security measures are very weak and there is no centralized management of resources.

Client Server Architecture

>> Here a system called server provides service to other systems called clients.

>> Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system.



>> The communication is initiated by the clients.

>> The server can be a hardware, an OS or an application.

>> A client doesnot share any of its resources.

>> The client can be a full PC or a diskless node .

>> Eg for server applications: Email (by main server), network printing (by print sever), and the World Wide Web (by web server).

>> A service may be done by more than one servers; a server can provide many services too.

>> The computing power, memory and storage requirements of a server must be enough to server all clients.

>> Load-balancing and failover systems are also employed for server implementations.

>> Central administration is possible in client-server model which is not posible in peer-to-peer model (workgroup).

Domain network

>> A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers.

>> Authentication takes place on domain controllers.

>> Computers can connect to a domain via LAN, WAN or using a VPN connection.

Active Directory

>> A network directory service stores information about a computer network and offers features for retrieving and managing that information.

>> The information contains records or objects describing users and available network resources, such as servers, printers, and applications.

>> Directory service can add, modify, and delete information and also manage how its stored resources can be used and by whom.

>> The Active Directory service is Windows' directory service terminology.

Active Directory Features

1) **Hierarchical organization:** enables administrators to organize users and network resources to reflect the organization of the environment in which it is used.
2) **Centralized but distributed database:** All network data is centrally located, but it can be distributed among many servers for fast, easy access to information from any location. *Automatic replication* of information also provides *load balancing* and *fault tolerance*.
3) **Scalability:** Advanced indexing technology provides high-performance data access even if there are million objects.
4) **Security:** *Fine-grained access controls* enable administrators to control access to each directory object and its properties. Active Directory also supports secure authentication protocols to maximize compatibility with Internet applications and other systems.
5) **Flexibility:** Active Directory is installed with some predefined objects, such as user accounts and groups, but their properties can be modified, and new objects can be added for a customized solution.
6) **Policy-based administration:** Administrators can define policies to ensure a secure and consistent environment for users.

Active Directory Structure

There are two aspects of Active Directory's structure:

1) Physical structure
2) Logical structure

Active Directory's Physical Structure

>> Consists of *sites* and servers configured as *domain controllers*.

Site

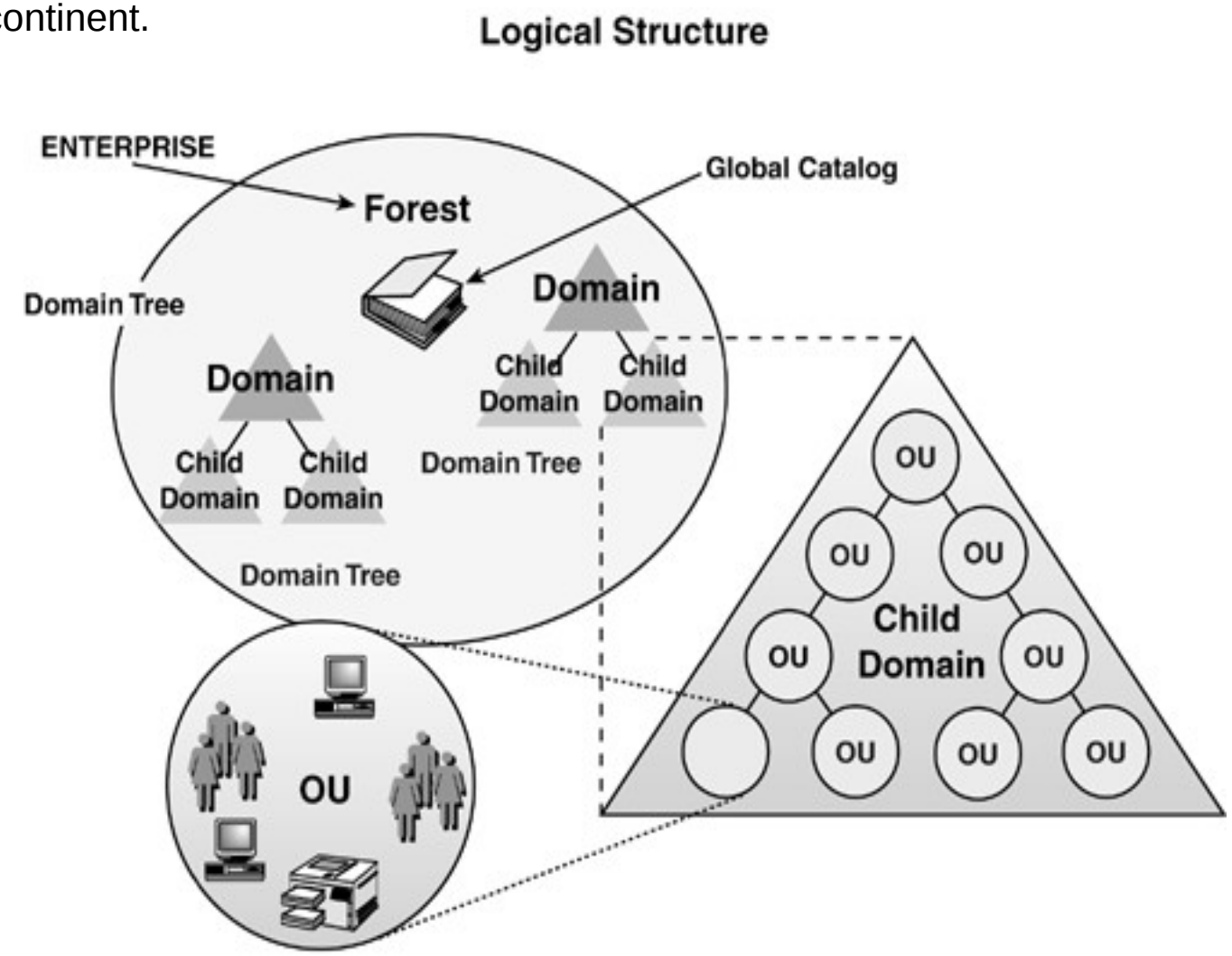
- A site is one or more IP subnets connected by high-speed LAN technology (eg: a small office with no branches).
- It is a physical location in which domain controllers communicate and replicate information regularly.
- A business with a branch office in another part of the city connected to the main office through a slow WAN link usually has two sites; but they come under the same domain.
- Advantages of sites: to control the frequency of Active Directory replication and to assign policies based on physical location.

Domain Controller (DC)

- DC is a computer running Windows Server with the Active Directory Domain Services role installed.
- Active Directory domain can consist of many domain controllers, each domain controller can service only one domain.
- DC is responsible for the following functions:
  1) Storing a copy of the domain data and replicating changes to that data to all other domain controllers throughout the domain.
  2) Providing data search and retrieval functions for users attempting to locate objects in the directory.
  3) Providing authentication and authorization services for users who log on to the domain and attempt to access network resources.

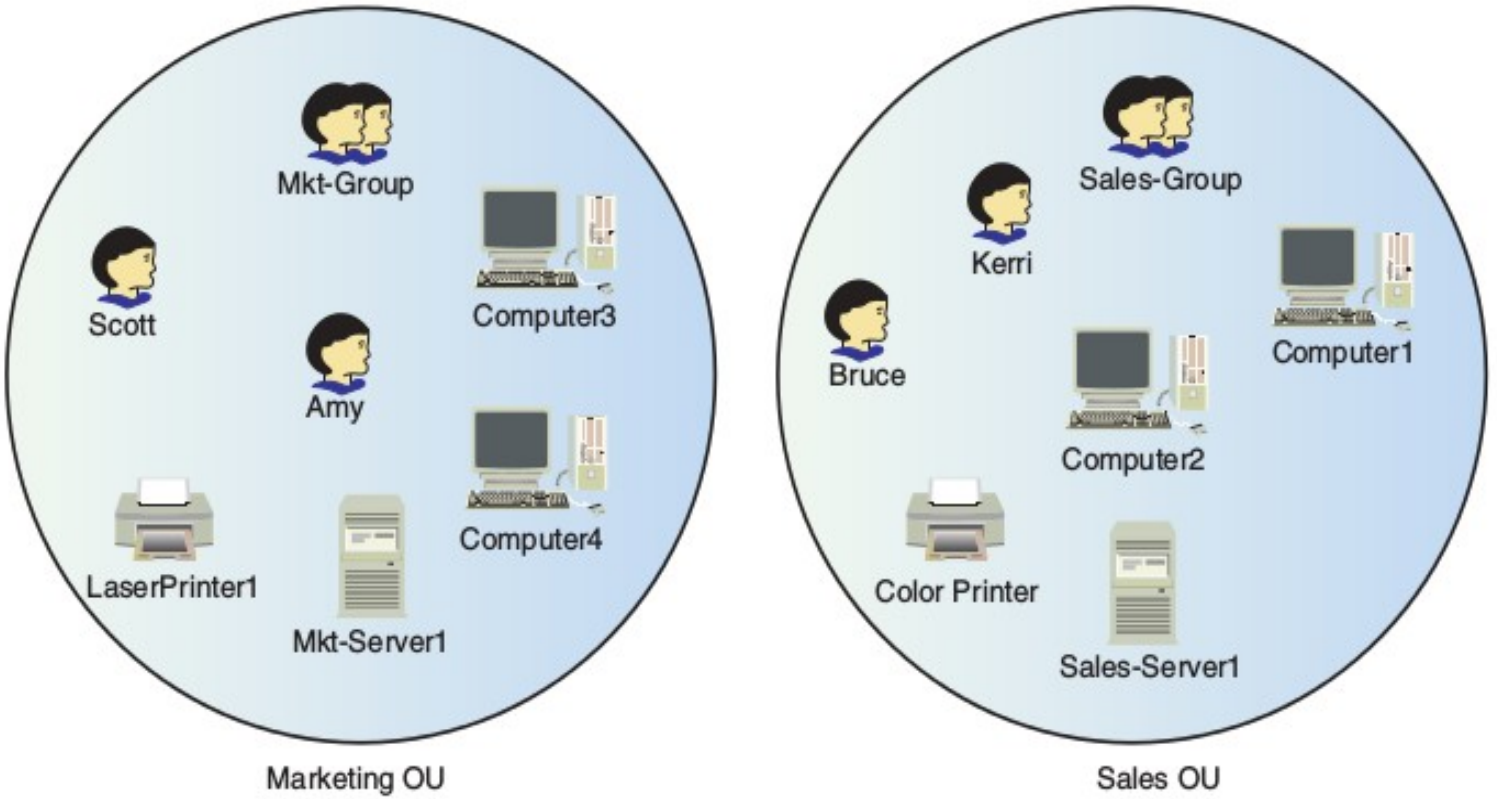
Logical Structure

- Makes the Active Directory structure seems like the organization in which it runs.
- Four components:
  1) Organizational units (OUs) 2) Domains
  3) Trees 4) Forests
- To use a geographical analogy, an OU represents a city, a domain is the state, a tree is the country, and a forest is the continent.



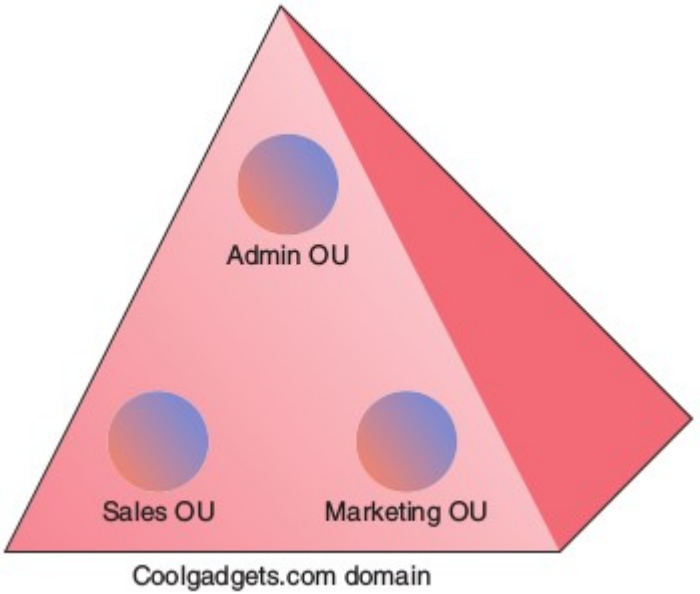
Organizational Unit (OU)

- It is an Active Directory container used to organize a network's users and resources into logical administrative units.
- Contains Active Directory objects, such as user accounts, groups, computer accounts, printers, shared folders, applications, servers, and domain controllers.
- For example, a corporation might create an OU for each department.
- OUs can be nested as many levels as necessary.
- OUs can represent policy boundaries, in which different sets of policies can be applied to objects.



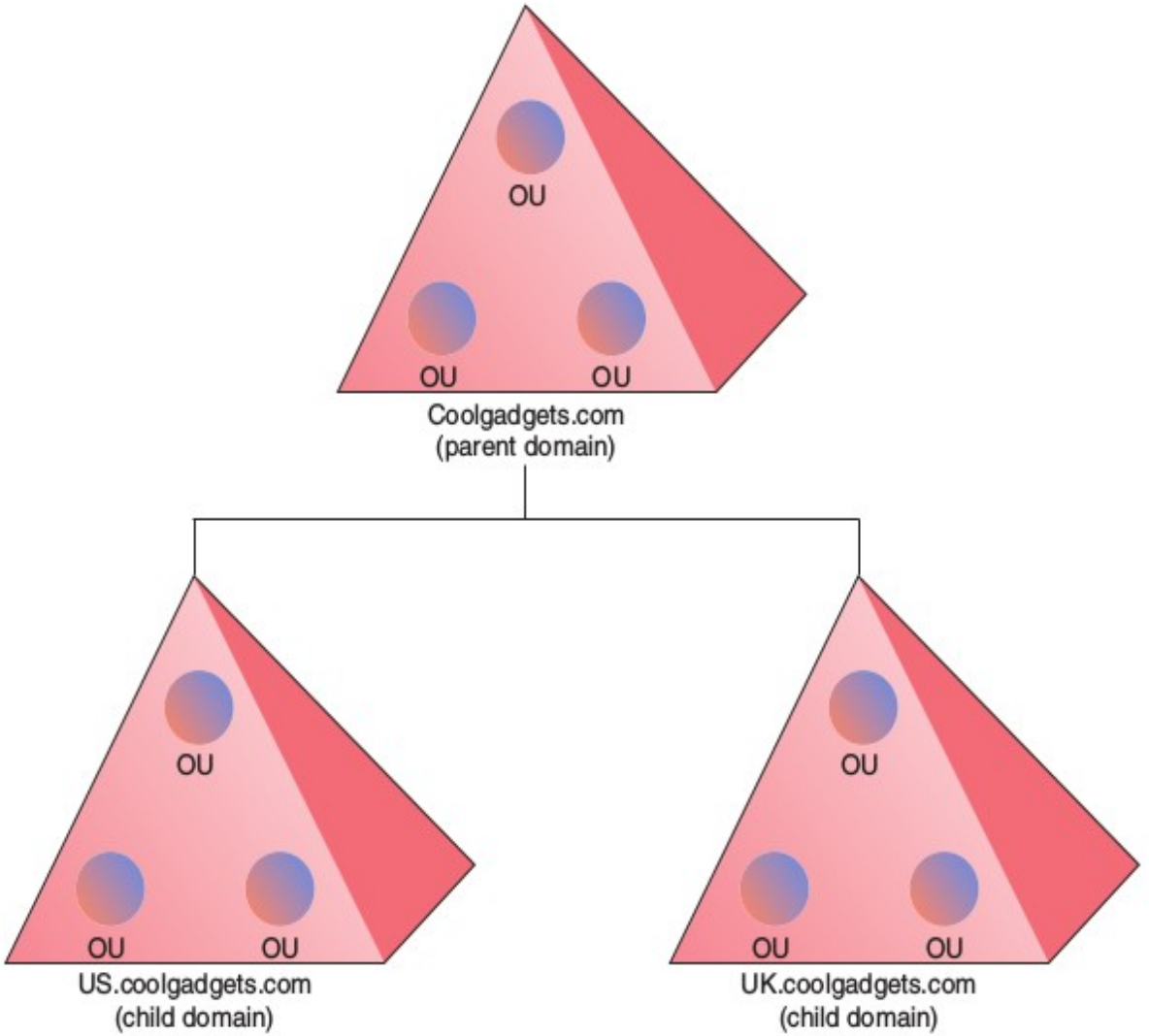
Domain

- The core structural unit of an Active Directory.
- Contains OUs, users, groups, etc.
- Represents administrative, security, and policy boundaries.
- A small to medium company usually has one domain with a single administrative group.
- A large company or a company with several locations might benefit from having multiple domains to separate administration or accommodate widely differing network policies.
- For example, a company 'coolgadgets.com' has two branches in US and UK, might want to divide administrative responsibilities into domains based on location, such as US.coolgadgets.com and UK.coolgadgets.com domains, each with a separate administrative group and set of policies.



Tree

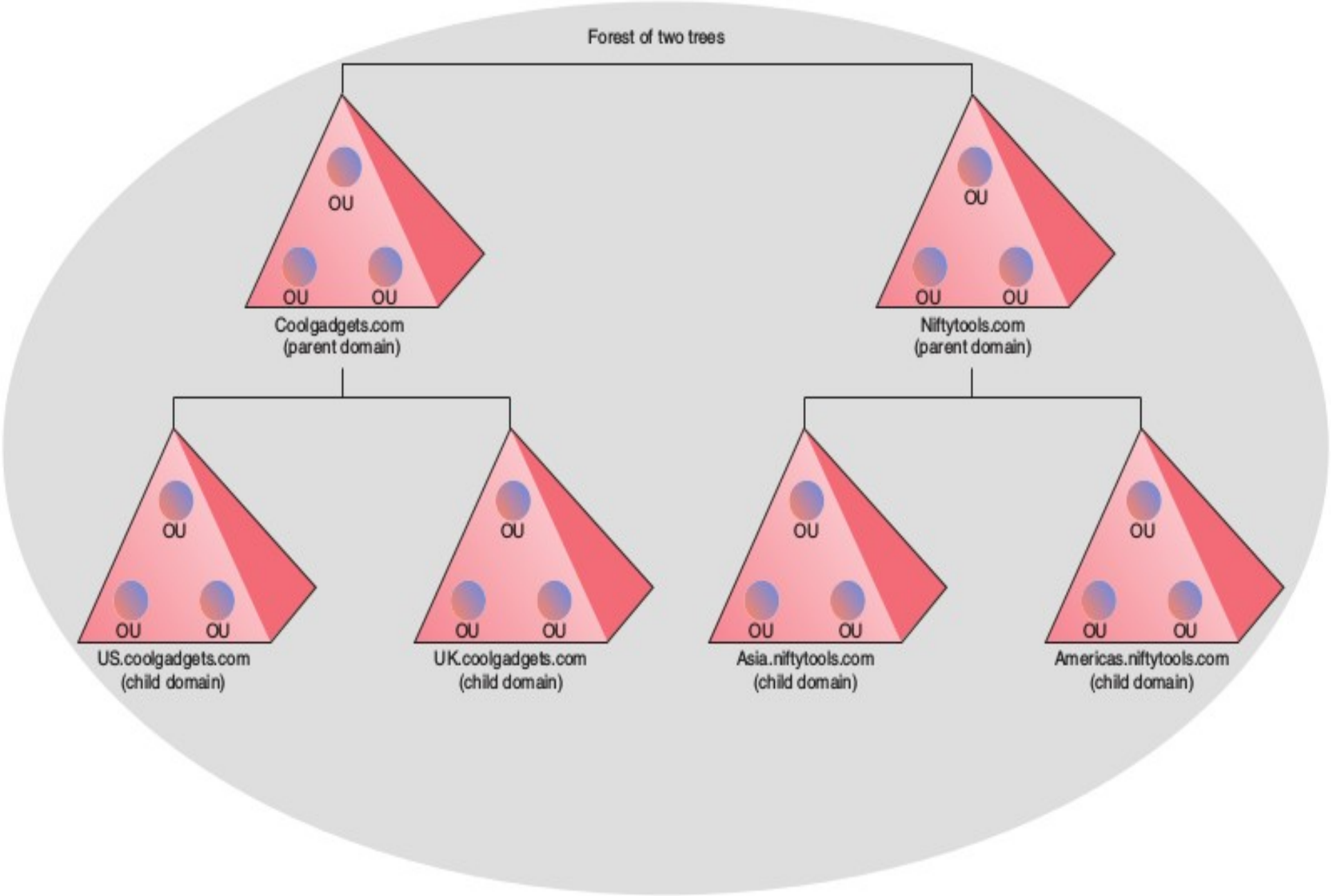
- A tree is a grouping of domains that share a common naming structure.
- A tree consists of a parent domain and possibly one or more child domains that have the same second-level and top-level domain names as the parent domain.
- For example, US.coolgadgets.com and UK.coolgadgets.com are both child domains of the parent domain coolgadgets.com.
- The tree can have several levels.



Forest

- It is a collection of one or more trees.
- A forest can consist of a single tree with a single domain, or it can contain several trees, each with a hierarchy of parent and child domains.
- Each tree in a forest has a different naming structure, so although one tree might have coolgadgets.com as the parent, another tree in the forest might have niftytools.com as its parent domain.
- A forest's main purpose is to provide a common Active Directory environment, in which all domains in all trees can communicate with one another and share information yet allow independent operation and administration of each domain.

Forest


Forest of two trees
OU
OU
OU
Coolgadgets.com
(parent domain)
OU
OU
OU
Niftytools.com
(parent domain)
OU
OU
OU
US.coolgadgets.com
(child domain)
OU
OU
OU
UK.coolgadgets.com
(child domain)
OU
OU
OU
Asia.niftytools.com
(child domain)
OU
OU
OU
Americas.niftytools.com
(child domain)

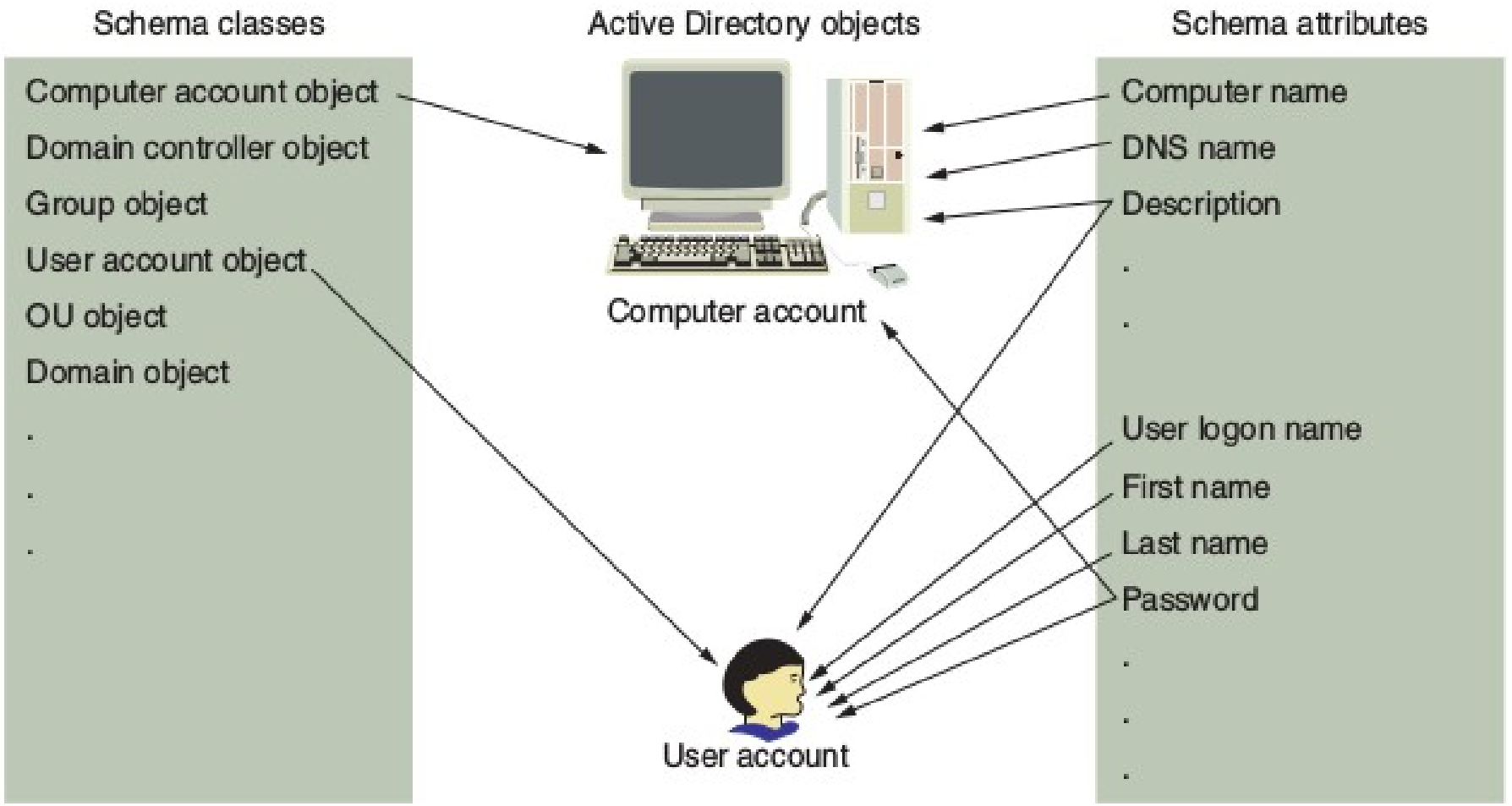
Active Directory's contents and the functions it performs in a network are defined by the schema, objects, and Group Policy Objects (GPOs).

Objects

- All information in the Active Directory database is organized as objects.
- An object is a grouping of information that describes a network resource, such as a shared printer, or an organizing structure, such as a domain or OU.

Schema

- The schema defines the type, organization, and structure of data stored in the Active Directory database and is shared by all domains in an Active Directory forest.
- The information the schema defines is divided into two categories: schema classes and schema attributes.
- Schema classes define the types of objects that can be stored in Active Directory, such as user or computer accounts.
- Schema attributes define what type of information is stored in each object, such as First name, Last name, and Password for a user account object.



Schema classes, schema attributes, and Active Directory objects

Active Directory Container Objects

- Contains other objects.
- Used to organize and manage users and resources in a network.
- Also act as administrative and security boundaries or a way to group objects for applying policies.
- Three container objects are used in Active Directory Users and Computers: OU, folder, and domain.

- Organizational Units (OU)
  - In Active Directory Users and Computers, an OU is represented by a folder with a book inside.
  - When Active Directory is first installed, a single OU called Domain Controllers is created and contains a computer object representing the domain controller.
  - When a new DC is installed in the domain, a new computer object representing it is placed in the Domain Controllers OU by default.
- Folder Objects
  - When Active Directory is installed, four folder objects are created: *Builtin, Computers, Users* and *ForeignSecurityPrincipals*.
  - You can't create new folder objects, nor can you apply group policies to folder objects.
- Domain Objects
  - Domains contain OU, folder container objects, leaf objects such as users, groups, and so forth.

Active Directory Leaf Objects

- A leaf object doesn't contain other objects.
- Usually represents a security account (users, groups, and computers), network resource (servers, domain controllers, file shares, printers), or GPO.

User Accounts:

- Contains information about a network user.
- When a user account is created, the administrator enters at least the user's name, logon name, password, office location, job title, department, etc.
- The user account object contains information such as group memberships, account restrictions (allowed logon hours and account expiration date, for example), profile path, and dial-in permissions.
- The main purpose of a user account is to allow a user to log on to a Windows computer or an Active Directory domain to access computer and domain resources.
- On login, when the user gives the logon name and password, authentication confirms a user's identity, and the account is then assigned permissions and rights that authorize the user to access resources and perform certain tasks on the computer or domain.
- There are three types of user accounts: local user accounts, domain user accounts, and built-in user accounts.

User Accounts...

- A local user account is defined on a local computer and is authorized to access resources only on that specific computer. Local user accounts are mainly used on stand-alone computers or in a workgroup network with computers that aren't part of an Active Directory domain.
- A domain user account is created in Active Directory and provides a single logon for users to access all resources in the domain for which they have been authorized.
- Windows creates two built-in user accounts automatically: *Administrator* and *Guest*. They can be local user accounts or domain user accounts, depending on the computer where they're created. On client systems, they are local to the systems and on servers with Active Directory, they are part of domain.

Groups

- A group object represents a collection of users with common permissions or rights requirements on a computer or domain.
- Helps when the same permissions and rights are to be given to a number of users.
- *Permissions* define which resources users can access and what level of access they have (Eg: open and read a certain document but not to change it).
- A *right* specifies what types of actions a user can perform on a computer or network (a user might have the right to log on to and log off a computer but not shut down the computer).
- When a user is moved away from a group, the user loses all rights and permissions assigned to that group.

Computer Accounts

- A computer account object represents a computer that's a domain controller or domain member.
- Used to identify, authenticate, and manage computers in the domain.
- Computer accounts are created automatically when Active Directory is installed on a server or when a server or workstation becomes a domain member.
- Administrators can also create computer accounts manually if automatic account creation is undesirable.
- By default, domain controller computer accounts are placed in the Domain Controllers OU, and domain member computer accounts are placed in the Computers folder.
- Like user accounts, computer accounts have a logon name and password, but a computer account password is managed by Active Directory instead of an administrator.
- A computer must have a computer account in Active Directory for users to log on to that computer with their domain user accounts.

Other Leaf Objects:

- Contact: A person who is associated with the company but is not a network user. Used purely for informational purposes.
- Printer: Represents a shared printer in the domain.
- Shared folder: Represents a shared folder on a computer in the network.

Group Scope and Group Type

- Each group has a scope that identifies the extent to which the group is applied in the domain tree or forest.
- There are three different scopes: universal, global, and domain local.

1) Groups with universal scope can have groups and accounts from any domain in the domain tree or forest as their members and can be granted permissions in any domain in the domain tree or forest. Groups with universal scope are referred to as universal groups.

2) Groups with global scope can have groups and accounts only from the domain in which the group is defined and can be granted permissions in *any domain* in the forest. Groups with a global scope are referred to as global groups. These are default scopes for newly created groups.

3) Groups with domain local scope can have groups and accounts from a domain as their members and can be used to grant permissions only within that domain. Groups with a domain local scope are referred to as domain local groups.

Group Policy Object (GPO)

- It is a list of settings that administrators use to configure user and computer operating environments remotely.
- Group policies can specify security settings, deploy software, configure a user's desktop, etc.
- They can be configured to affect an entire domain, a site, and, most commonly, users or computers in an OU.
- The objects a GPO affects are said to be within that GPO's scope.
- GPOs don't apply to group objects.
- When Active Directory is installed, two GPOs are created and linked to two containers:
  1) Default Domain Policy—This GPO settings affect all users and computers in the domain.
  2) Default Domain Controllers Policy—This GPO settings affect all domain controllers in the domain.

Global Catalog Servers

- The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest.
- The global catalog is stored on domain controllers that have been designated as global catalog servers.
- It is distributed through multimaster replication.
- Searches that are directed to the global catalog are faster.

Child Domain

- The domain at the top of the forest (the first one to be created) is called the *ROOT domain*. A domain in the same forest but not a child of the root domain is an *additional domain* in the same forest. A domain which "hangs off" either of these two is a Child Domain.
- Sample Pattern:

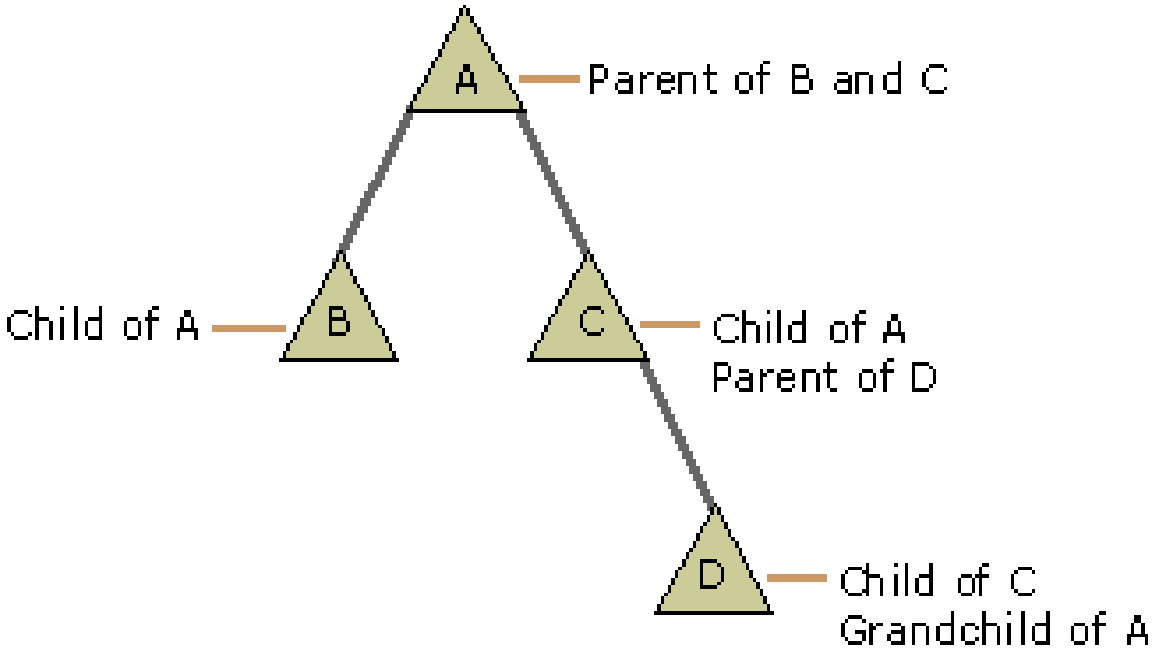
  root.forest.com - the root domain.

  rootsbrother.forest.com - additional domain in same forest.

  child.root.forest.com - a child domain of ROOT.

  child.rootsbrother.forest.com - a child domain of ROOTSBROTHER.

- A child can be the parent of one or more child domains. Thus forms a hierarchy (called **Tree**).



Additional Domain Controller (ADC)

- It is another DC in an existing domain.
- This DC is called Additional Domain Controller (ADC) which replicates all the data from the primary domain controller (PDC) including global catalog and runs DNS services too.
- Used to balance the load among existing domain controllers.
- Also provides fault-tolerance that in case primary AD DC is down, additional AD DC can be used for authentications without any business discontinuity.
- Generally the PDC DNS server address is set as the preferred DNS for ADC too (a forest root domain DC), and can give its own IP address is given as alternate DNS server address.
- Steps to install ADC

  1) Install ADDS and DNS from Server Roles and Background Intelligent Transfer Service (BITS) from Features. (Keeps other selected services as such).
  2) Start 'Promote this server to a Domain Controller' option.
  3) In Deployment Configuration, click 'Add a DC to an existing domain' option and type domain name for which it will become an ADC.
  4) Every other things are default as such.

- After installation, the server will restart and will replicate the databases from PDC.

Trust Relationships

- Active Directory Trust relationship is a logical link which allows a domain to access another domain, or a forest to access another forest.
- When there are trust relationships between domains, the authentication mechanism for each domain trusts the authentication mechanism for all other trusted domains.
- If a user or application is authenticated by one domain, its authentication is accepted by all other domains that trust the authenticating domain.
- Trusts which are created automatically are called as Implicit Trusts. (eg: trusts between parent and child) and the trusts which are created manually are called as Explicit Trusts.
- Active Directory Trusts can be either transitive or non-transitive.
    - Transitive trusts: When Domain1 trusts Domain2, and Domain2 trusts Domain3, Domain1 would also trust Domain3.
    - Non-transitive trust: The defined trust relationship ends with the two domains between which the particular trust is created.
- Active Directory Trusts can be one-way or two-way.
    - Based on the direction of trusts.
    - One-way trusts can be *incoming trust* or *outgoing trust*.
    - Two way trust is when a domain A trusts B and B trusts A.
    - Both the above can be transitive or non-transitive.

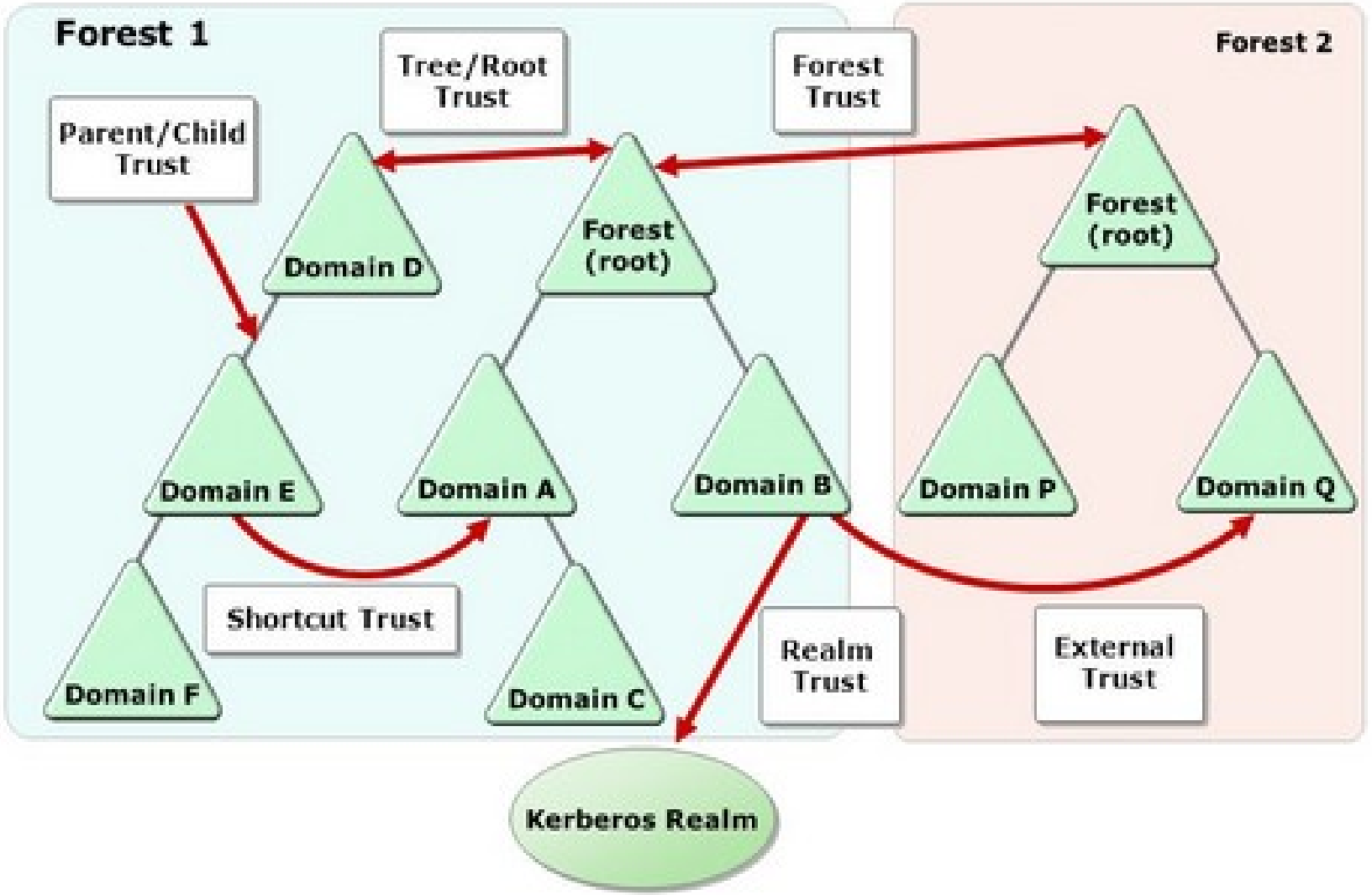
Trust Relationships...

- Users in a *trusted* domain have access to resources in the *trusting* domain, subject to the access controls that are applied in the trusting domain.
- If B is the trusting domain and A is the trusted domain, B-->A indicates that domain B trusts domain A. (The same trust relationship can be illustrated as A<--B, that is, A is trusted by B).
- In B-->A, users in A can be authenticated to access resources in B, but users in B can't access the resources of A.
- When a new domain joins a domain tree as a child, a parent-child trust relationship is defined automatically that establishes a two-way, transitive trust relationship (A<---->B).
- Types of Trust:

    1) Tree-root trust
    2) Parent-child trust
    3) Shortcut trust
    4) Realm trust
    5) External trust
    6) Forest trust

Tree-root trust

- Automatically/implicitly created when a new tree root domain is added to a forest.
- It is transitive and two way.



Parent-child trust:

- Implicitly established when new child domains are added to a domain tree.
- Two-way, transitive trust relationship.
- Since part of the same domain, both have common contiguous DNS namespace.
- When a new domain is added to the tree, trust relationships are created with each domain in the tree.
- Network resources in the tree’s individual domains can be accessed by all other domains in the tree.

Shortcut trust:

- Created between two domains in different trees but within the same forest.
- An administrator explicitly creates a shortcut trust and is either a one way transitive trust or two way transitive trust.
- Shortcut trust is usually created when users want to speed up or enhance authentication performance between two domains in different trees but within the same forest.

Realm trust:

- An administrator explicitly creates realm trust and it can be defined as either a transitive or non-transitive trust.
- It can also either be a one way or two way trust.
- Realm trust enables users to create a trust relationship between a Windows Server Active Directory domain and a non-Windows Kerberos version 5 realm.

External trust

- An administrator explicitly defines the external trust to enable trust between domains that are located in different forests.
- External trust is always non-transitive but can be either one-way trusts or two-way trusts.
- Created when users need to access network resources in a domain that resides in a different forest and forest trust cannot be created between the two domains.

Forest trust:

- An Administrator explicitly created Forest trust to enable trust between two Active Directory forests.
- Forest trust is transitive in nature and can either be one-way or two-way.
- Users would be able to access Active Directory objects between all domains of these forests.

Securing files and folders

- Permissions can be applied to files, folders and drives formatted with NTFS file system. Permissions once applied is effective for both network users and local users.
- Permissions enable the owner of each secured object, such as a file, folder or an Active Directory object, to control who can perform an operation or a set of operations on the object or object property. (Hence this type of access control is called discretionary access control – DAC).
- You can assign permissions on objects to the following:
  - Groups, users, and special identities in the domain
  - Groups and users in the domain and any trusted domains
  - Local groups and users on the computer where the object resides

Explicit vs. Inherited Permissions

- There are two types of permissions, explicit permissions and inherited permissions:
  - Explicit permissions are those that are set by default when the object is created or by user action.
  - Inherited permissions are those that are propagated to a child object from a parent object. Inherited permissions ease the task of managing permissions.

- Ownerships: The owner is the creator of the object. The owner controls how permissions are set on the object and to whom permissions are granted.

- There are two types of permissions: Shared permissions and Security permissions.
- Both are applicable for folders.
- Only security permissions are applicable for files.
- **Shared Permissions:**
  - Shared folder permissions are in effect only when users are remote to the shared data.
  - Shared permissions can be placed only on the folder and not on individual files.
  - shared permissions are additive, so users receive the highest level of permissions granted by the groups of which they are members.
  - The Deny permission overrides any group permission, and an individual permission overrides a group Deny.
  - The default shared permission is Administrators = Full Control .
  - The standard permissions are:
    - Full control – enables users to “read”, “change” as well as edit permissions and take ownership of files.
    - Change – means that user can read/execute/write/delete folders/files within share.
    - Read – allows users to view the folder’s contents.

Security Permissions

- Allow or deny actions on files and folders by other users who log on to the same system.
- Deny permissions are involved, they always override Allow permissions.
- The common permissions on files and folders are;

Permission name	Folder	File
Full control	The user has full control to the folder and can add, change, move and delete items. The user can also add and remove permissions on the folder as well as for any subfolders.	The user has full control to the file and can change, move or delete it. The user can also add and remove permissions on the file.
Modify	A combination of Read and Write permissions. A user also has the ability to delete files within that folder. He can also view the contents of subfolders.	A user is able to modify the contents of the selected file.
Read & execute	Users are allowed to read the contents of files in the folder or execute programs inside the folder.	Users are allowed to read the contents of the file or execute the program.
List folder contents	Allows the user to view the contents of the selected folder. The user is not allowed to read a file's contents or execute a file.	NA
Read	The user can read the contents of a folder.	The user can read the contents of a file.
Write	A user can create files and folders. This does not grant a user with the ability to read any existing information.	A user can create a file.