CNT 4603: System Administration
Spring 2013

Introduction To Active Directory

Instructor : Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 4078-823-2790
http://www.cs.ucf.edu/courses/cnt4603/spr2013

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida

Introduction To Active Directory

- One of the biggest changes in Windows 2000 over Windows NT was the addition of Active Directory (hereafter referred to as AD).
- In both Windows Server 2003 and Windows Server 2008, AD has been enhanced, making it an even more important part of the operating system.
- Active Directory provides a single reference, called a directory service, to all the objects in a network, including users, groups of users, computers, printers, policies, and permissions.
- For a user or system admin, AD provides a single hierarchical view from which to access and manage all of the network's resources.

Introduction To Active Directory

- AD utilizes Internet protocols and standards, including Kerberos, Secure Sockets Layer (SSL), and Transport Layer Security (TLS) authentication, the Lightweight Directory Access Protocol (LDAP); and the Domain Name Service (DNS).
- AD requires one or more domains in which to operate.
- A domain, as used within Windows Server 2008 (and the earlier versions), is a collection of computers that share a common set of policies, a name, and a database of their members.
- A domain must have one or more servers that serve as domain controllers and store the database, maintain the policies, and provide the authentication for domain logons.

Introduction To Active Directory

- Don’t not confuse domain as used in the context of Windows Server 2008 and that as it is used in the context of the Internet.
- A domain, as used in within the Internet, is the highest segment of an Internet domain name and identifies the type of organization; for example *.edu* for educational organizations.
- A domain name is the full Internet address used to reach one entity registered on the Internet. For example, www.cs.ucf.edu.

Introduction To Active Directory

- AD plays two different functions within a network: (1) that of a directory service containing a hierarchical listing of all the objects within the network, and (2) that of an authentication and security service that controls and provides access to network resources.
- These two roles are different in nature and focus, but they combine together to provide increased user capabilities while decreasing administrative overhead.
- At its core, Windows Server 2008 AD is a directory service that is integrated with DNS, plus a user authentication service for the Windows Server 2008 operating system.

Introduction To Active Directory

- While AD is both a directory and a directory service, the terms are not interchangeable.
- In Windows Server 2008 networking, a directory is a listing of the objects within a network.
- A hierarchical directory has a structure with a top-to-bottom configuration that allows for the logical grouping of object, such that lower-level objects are logically grouped and contained in higher-level objects for as many levels as you want.
- These groupings can be based on a number of different criteria, but the criteria should be logical and consistent throughout the directory structure. More on this later.

Introduction To Active Directory

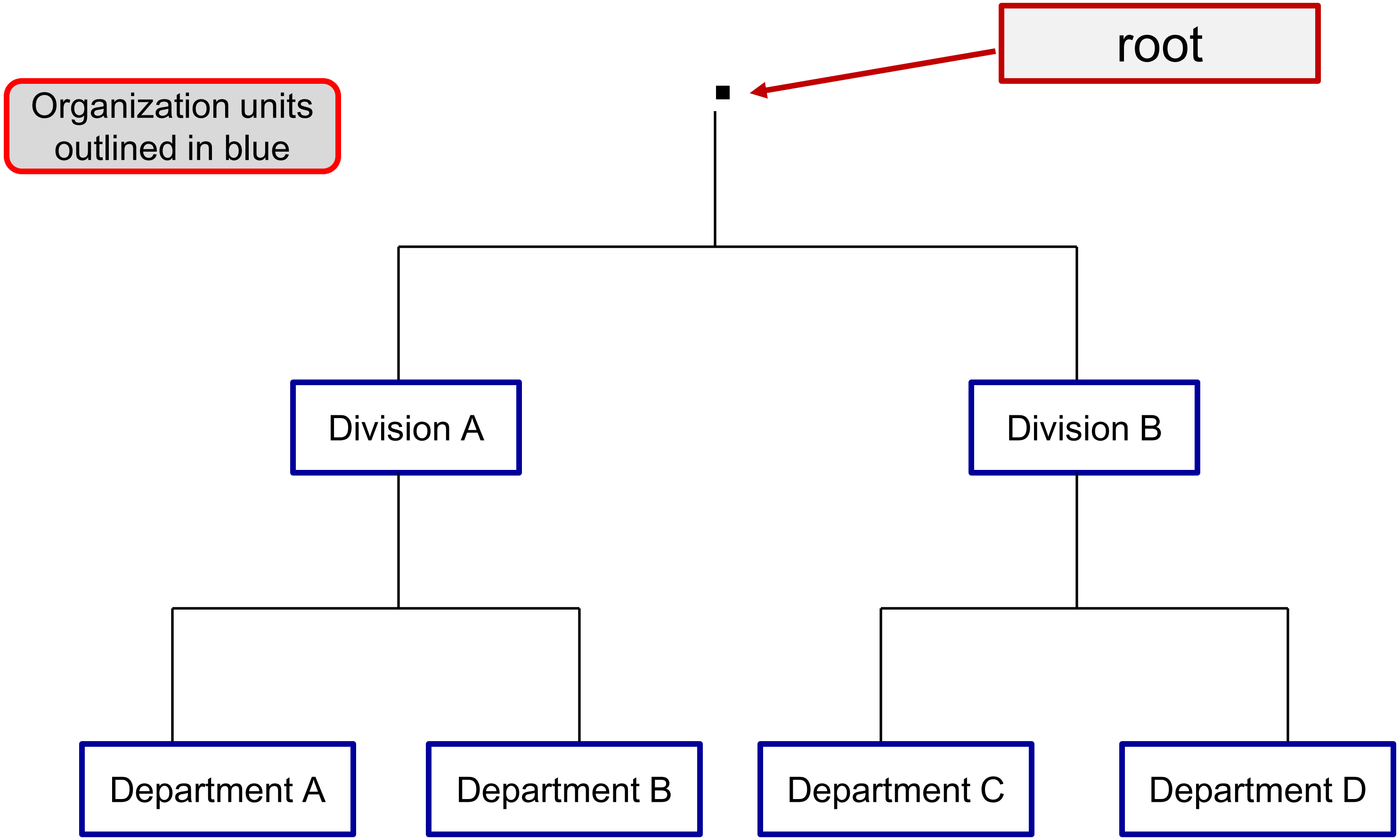
- Two of the more common directory structures in use within networks are based on object function (such as printers, servers, and storage devices) and organizational responsibility (such as marketing, accounting, and manufacturing).
- The organizational model allows you to store objects in groups, or containers, based on where they are in an organization, which might have its own structure, such as departments within divisions.
- A particular department would be the first organizational point within an organization.
- A container holding all the objects in a department is called an organizational unit (OU) and is itself grouped into higher-level OUs based on the logical structure.

Introduction To Active Directory

- After you create a group of OUs, you might find that the structure causes your directory to be cluttered and/or awkward to navigate. As a result, you may need to change your network to have more high-level OUs or more low-level OUs.
- At the top of all directories is the master OU that contains all the other OUs. This directory is referred to as the root and is normally designated by a single period.
- An example is illustrated on the nest slide.

NOTE: Active Directory, Microsoft Exchange, and Novell Directory Services (NDS) are all based on the X.500 standard, which is an internationally recognized standard used to create a directory structure. Specifically, AD is based on the newer X.509 version of the X.500 family of standards.

Introduction To Active Directory



Introduction To Active Directory

- Active Directory is just as basic as the organization illustrated by the previous slide. However, much of AD's core structure has already been mapped out by Microsoft and is consistent throughout all Windows Server 2008 implementations.
- For this reason, some of the containers, which are just OUs, have been assigned specific names and roles within AD.
- As we look at this preconfigured directory structure, don't let the terms and names confuse you. Everything is still simply a collection of objects within OUs.

Introduction To Active Directory

- The “service” in directory service adds to the server features that are not otherwise available. Primarily, a directory service provides access to a directory of information, as well as to services that provide information about the location, access methods, and access rights for the objects within the directory service tree.
- This means that a user can access a single directory and then be directly connected to a variety of other servers and services that all appear to be coming from the original directory.
- Most of the rest of this set of notes is devoted to examining the different kinds of objects and methods of access that AD can provide both users and system administrators.

Integration With DNS

- Much of AD's structure and services, as well as the namespace that it uses, are based on DNS (Domain Name System).

- Namespace is the addressing scheme that is used to locate objects on the network. Both AD and the Internet use a hierarchical namespace separated by periods.

- Exactly how AD uses DNS we'll get to, but first we need to see the structure and workings of DNS and how it is used to build the AD foundation.

Integration With DNS

- All servers and services on the Internet are given an Internet Protocol (IP) numerical address, and all Internet traffic uses this IP number to reach its destination.
- IP numbers change, and may host multiple services at the same time. In addition, most people have a hard time remembering large, arbitrary numbers such as IP addresses.
- IP addresses are decimal-based descriptions of binary numbers without a discernable pattern.
- DNS services were created to allow servers and other objects on the network to be given a name, which translates to an IP number. For example, a user-friendly name such as *cs.ucf.edu* might be translated or resolved to an IP address such as 132.170.0.0, which the network can then use to locate the desired resource.

Integration With DNS

- DNS servers use hierarchical directory structures, just like the illustration on slide 9. At the core of DNS servers are root domains with a root directory, which is described by a single period.
- The first groups of OUs below the root are the various types of domains that can exist, for example, *com*, *net*, *org*, *gov*, *edu*, and so on.
- Over 250 of these top-level domains are controlled within the United States by InterNIC, an arm of the U.S. Department of Commerce, and run by a private, non-profit corporation named the Internet Corporation for Assigned Names and Numbers (ICANN), which controls a number of root servers that contain a listing of all the entries within each subdomain.

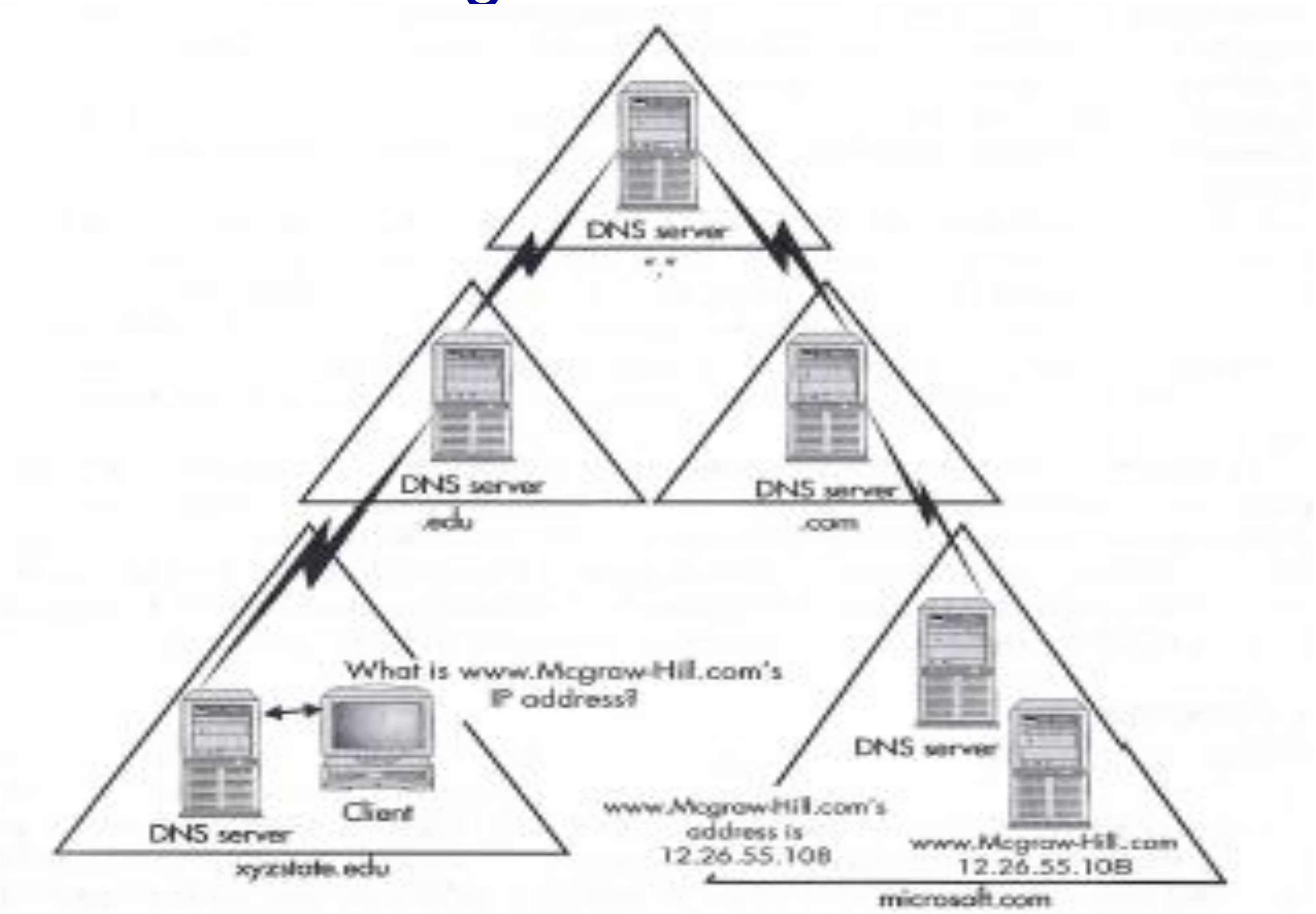
Integration With DNS

- The next group of OUs following the *".coms"* consists of domain names, such as *microsoft.com*, *ucf.edu*, etc.. These domains are registered and administered by the organization or individuals who own them.

- A number of companies have contracted with InterNIC/ICANN to register new domain names added to the Internet; you can see an alphabetical listing of those companies at http://www.internic.com/alpha.html.

- A domain name such as *ucf.edu*, can contain both additional OUs, called subdomains, and actual server objects. For example, *cs.ucf.edu* is a server in the Computer Science department within the *ucf* domain. A server name, such as this, that contains all OUs between itself and the root is called a fully qualified domain name (FQDN).

Integration With DNS


DNS server
"."
DNS server
.edu
DNS server
.com
What is www.Mcgraw-Hill.com's IP address?
DNS server
Client
xyzstate.edu
DNS server
www.Mcgraw-Hill.com's address is 12.26.55.108
www.Mcgraw-Hill.com 12.26.55.108
microsoft.com

Active Directory And Domains

- AD and DNS share the same central OU, called a domain.
- A domain is a central authentication and directory service that contains all the information for a group of computers.
- In Microsoft Server 2008 AD, the domains can scale to virtually any size (NT placed a 40,000 object limit on a domain structure). Also domains can form transitive two-way trusts with other domains in the network (more later on this).
- The close integration between AD and DNS might lead you to think that they are one and the same thing, however, this is not true.
- In actuality, DNS and AD are separate directory services that are using the same names for different namespaces. Each directory contains different objects, and different information about the objects in its own database. However, those object names, as well as the directory structure, are often identical.

Active Directory And Domains

- Every Windows Server 2008 computer has a FQDN. This is a combination of its own computer name and the domain name of the domain in which it currently resides.
- For example, Windows Server 2008 computers in the McGraw-Hill domain may very well have a computer name equal to *computername*.mcgraw-hill.com. However, that same computer may in fact be a member of the subdomain of editorial.mcgraw-hill.com. In this case, the FQDN would actually be *computername*.editorial.mcgraw-hill.com.

DNS Directories

- A DNS directory doesn't really store objects in its database. Rather, DNS stores domains, the access information for each domain, and the access information for the objects (such as the servers and printers) within the domain.
- The access information is normally just the FQDN and the related IP address.
- All queries for an object's IP address will match the FQDN in the request to the FQDN index in the DNS directory and return (resolve to) the IP address.
- In some cases, the access information (or resolve reference) simply points to another object (or resource) within the same or a different DNS domain.

Active Directory Services

- AD services contain a lot more information that what is available in DNS directories, even though the names and structure are nearly identical. AD resolves all information requests for objects within its database using LDAP queries.
- The AD server is able to provide a varied amount of information about each object within its database. The information the AD can provide includes, but isn't limited to, the following:
  - Username
  - Contact information, such as physical address, phone numbers, and email addresses
  - Administrative contacts
  - Access permissions
  - Ownerships
  - Object attributes, such as object name features; for example, Color Laser Jet Printer, 20 sheets/minute, duplex printing.

Active Directory Services

- Although DNS does not require AD, AD requires a DNS server to be in place and functioning correctly on the network before a user will be able to find the AD server.

- Windows Server 2003 moved entirely to Internet standards for its network OS, a trend continued with Server 2008. This requires a method of locating network services other than using the NetBIOS broadcast technique employed by Windows NT. This was accomplished using a new DNS domain type known as dynamic DNS (DDNS) domains.

- A DDNS domain, which is integrated into AD, allows all domain controllers to use the same database, which is automatically updated as new Windows Server computers are added and removed from the network.

Active Directory Services

- The DDNS domain also allows DNS to function with networks based on DHCP (Dynamic Host Configuration Protocol), where the IP addresses of the network objects are constantly changing.
- Besides providing the name resolution for the network, DDNS domains also contain a listing of all the domains and domain controllers throughout the network. This means that as new Windows Server systems are added to a network, they will query the DDNS servers to get the name and connection information, including IP addresses, of the domain controllers they are closest to.

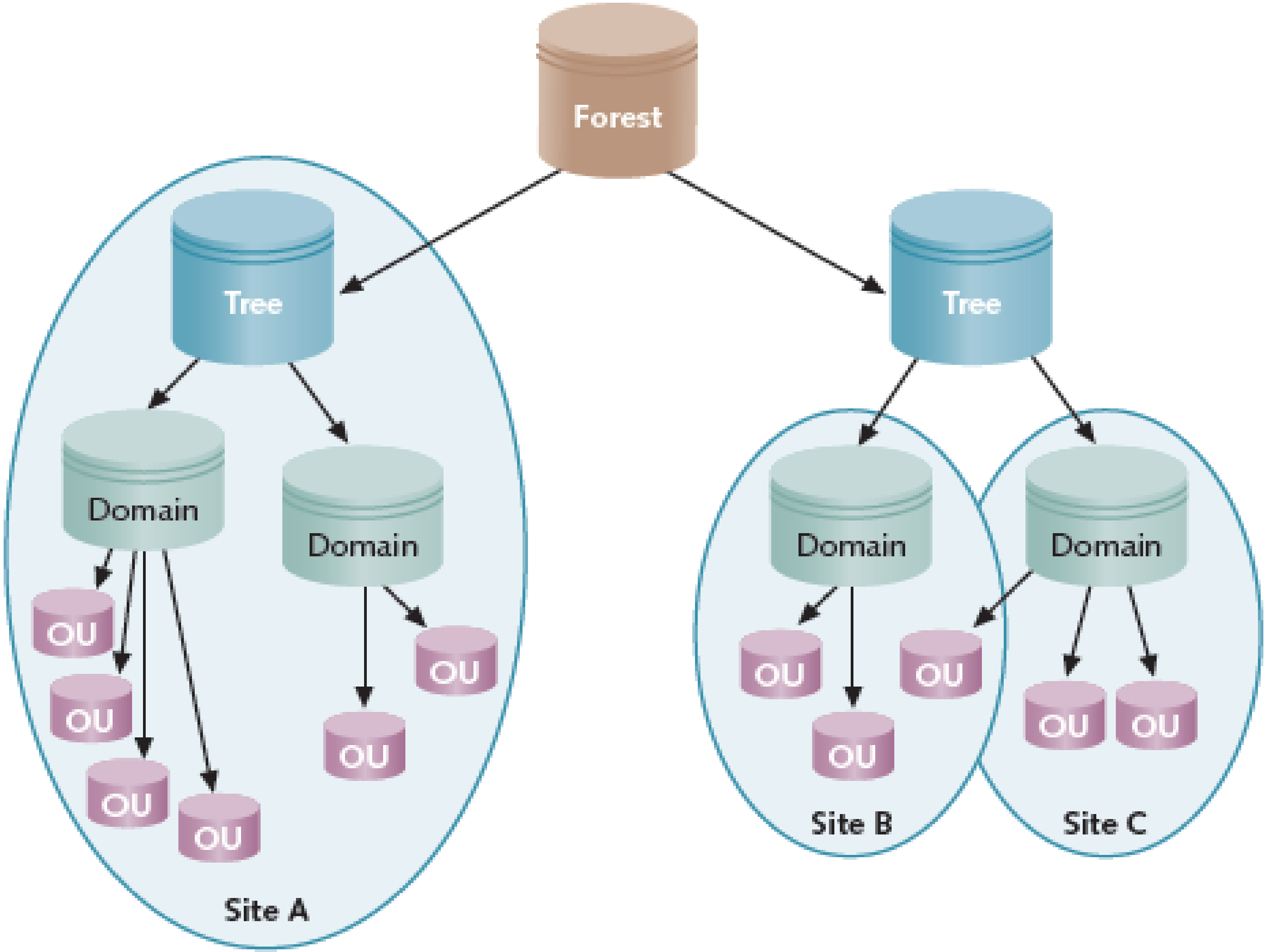
Active Directory And The Global DNS Namespace

- AD domains are designed and intended to exist within the naming schemes of the global DNS domain operated through the Internet. This means that, by design, the DNS domain of your network would also match the AD domain-naming scheme.

Containers In Active Directory

- As we just saw, AD has a treelike structure which is based on the X.500 standard for directory structures.
- In a normal directory structures, folders contain subfolders and within subfolders there can be more subfolders to an arbitrary depth.
- Just as files are the basic element that are grouped in a hierarchy of folders and subfolders, objects are the basic elements of AD and are grouped into a hierarchy of containers.
- Containers in AD include forests, trees, domains, OUs, and sites.

Containers In Active Directory



Active Directory - Forests

- At the highest level in an AD design is the forest.
- A forest consists of one or more AD trees that are in a common relationship and that have the following characteristics.
  - The trees can use a disjointed namespace.
  - All trees use the same schema.
  - All trees use the same global catalog.
  - Domains enable administration of commonly associated objects, such as accounts and other resources, within a forest.
  - Two-way transitive trusts (resources that are equally shared) are automatically configured between domains within a single forest.

Active Directory - Forests

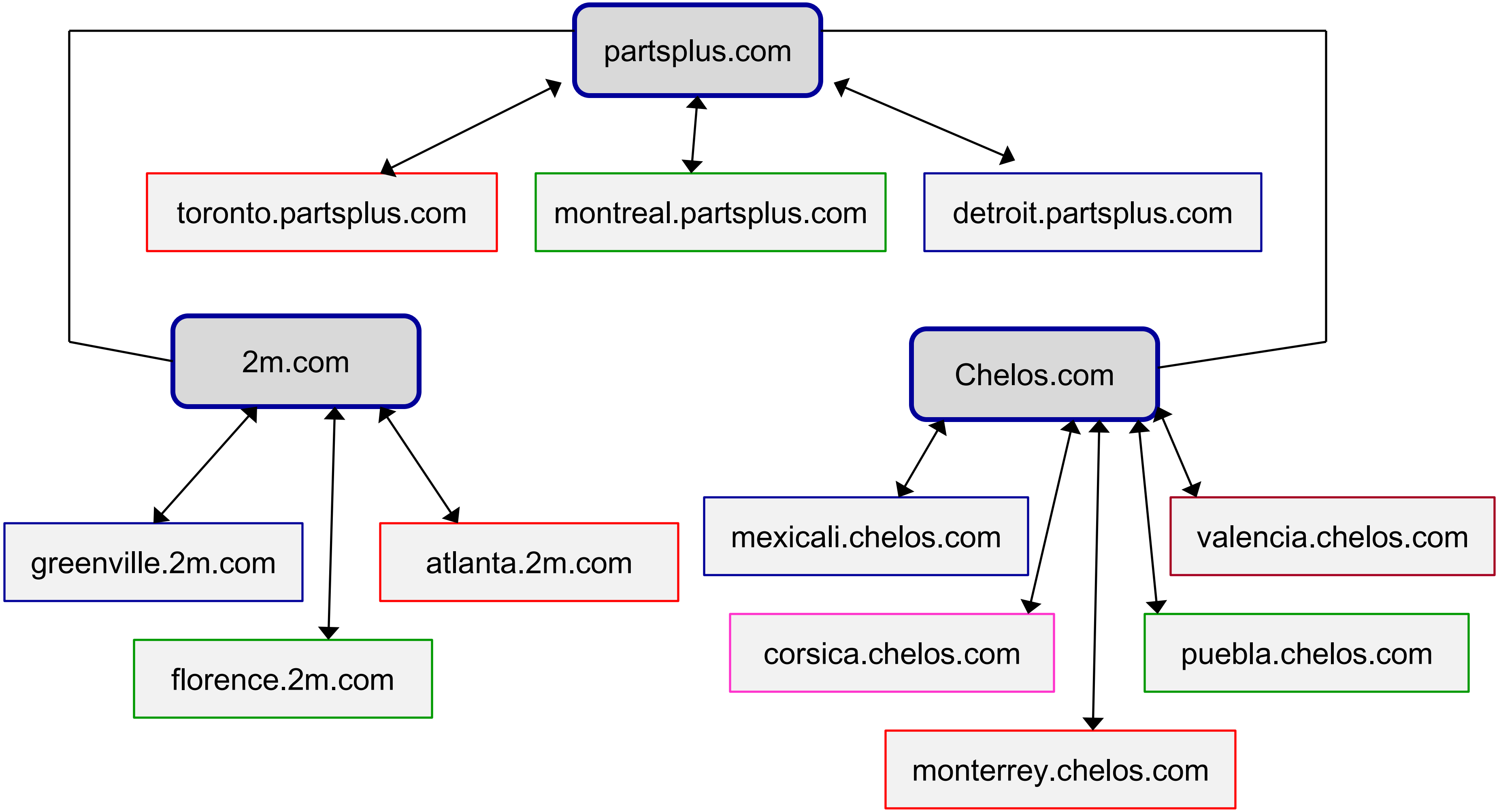
- A forest provides a means to relate trees that use a contiguous namespace in domains within each tree but that have disjointed namespaces in relationship to each other.

- Consider the following scenario: an international automotive parts company that is really a conglomerate of three different companies, each with a different brand name. The parent company is PartsPlus, located in Toronto. PartsPlus manufactures alternators, coils and other electrical parts at plants in Toronto, Montreal, and Detroit, and has a tree structure for domains that are part of partsplus.com.

- Another company owned by PartsPlus is Marty & Mikes (2m.com) makes radiators in two South Carolina cities, Florence and Greenville, and radiator fluid in Atlanta.

Active Directory - Forests

- A third member company, Chelos (chelos.com) makes engine parts and starter motors in Mexico City, Corsica, Monterrey, and Puebla, all in Mexico – and also has a manufacturing site in Valencia, Venezuela.
- In this situation, it makes sense to have a contiguous tree structure for each of the three related companies and to join the trees in a forest of disjointed name spaces.
- This is illustrated in the figure on page 7.


partsplus.com
toronto.partsplus.com
montreal.partsplus.com
detroit.partsplus.com
2m.com
Chelos.com
greenville.2m.com
atlanta.2m.com
florence.2m.com
mexicali.chelos.com
valencia.chelos.com
corsica.chelos.com
puebla.chelos.com
monterrey.chelos.com

A Forest

Active Directory - Forests

- The advantage of joining trees into a forest is that all domains share the same schema and global catalog.
- A schema is set up at the root domain (which is partsplus.com in the previous example), and the root domain is home to the master schema server.
- At least one DC (domain controller) functions as a global catalog server. However, in the previous example it would be likely that you would plan to have a global catalog server located at each geographic location (domain).

Active Directory - Forests

- Windows Server 2008 AD recognizes three types of forest functional levels.
- The forest functional level refers to the AD functions supported forest-wide.
- The functional levels are:
- *Windows 2000 native forest functional level* – provides AD functions compatible with a network that has a combination of Windows 2000 Server, Windows 2003 Server, and Windows 2008 Server domain controllers.
- *Windows Server 2003 forest functional level* – intended for Windows Server 2003 and 2008 domain controllers only and enables more forest management functions, such as more options for creating trust relationships between forests, domain renaming, Read-Only Domain Controllers, cross-forest authentication of users, and enhanced replication of AD.

Active Directory - Forests

- *Windows Server 2008 forest functional level* – contains only Windows Server 2008 domain controllers. Currently this level has no more functional features that in the Windows Server 2003 forest functional level, although there is room for new features that can be added later. This level is also included for compatibility with the domain functional levels we’ll see later.

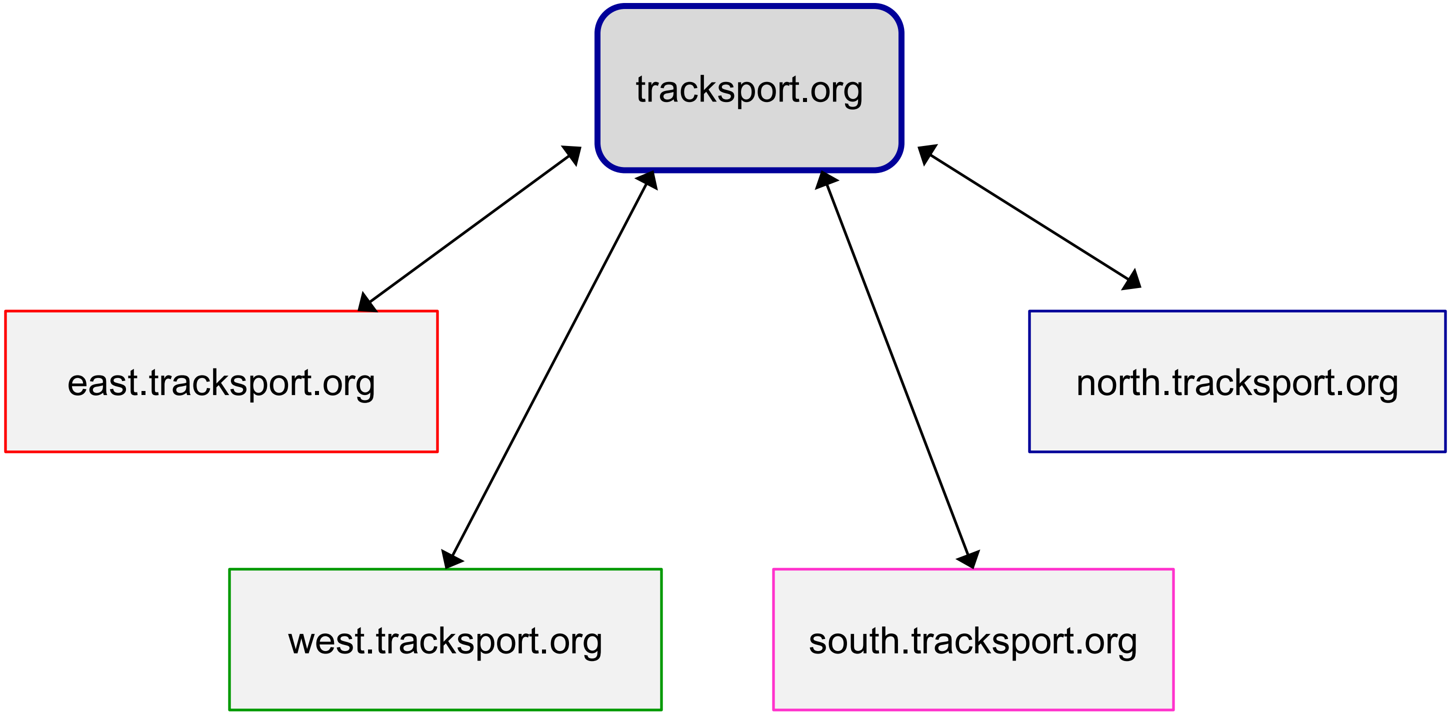
Active Directory - Trees

- A tree contains one or more domains that are in a common relationship, and has the following characteristics.
  - Domains are represented in a contiguous namespace and can be in a hierarchy.
  - Two-way trust relationships exist between parent domains and child domains, essentially creating a trust path.
  - All domains in a single tree use the same schema for all types of common objects.
  - All domains use the same global catalog.

Active Directory - Trees

- The domains in a tree typically have a hierarchical structure, such as a root domain at the top and other domains under the root (similar to a parent-child relationship).
- Consider the following example: tracksport.org might be the root domain and have four domains under the root to form one tree: east.tracksport.org, west.tracksport.org, north.tracksport.org, and south.tracksport.org, as shown on page 13.
- These domains use the contiguous namespace format in that the child domains each inherit a portion of their namespace from the parent domain.

Active Directory - Trees



A Tree

Active Directory - Trees

- The domains within a tree are in what is called a Kerberos transitive trust relationship, which consists of two-way trusts between parent domains and child domains.
- A transitive trust means that if A and B have a trust and B and C have a trust, the A and C automatically have a trust as well.
  - This transitive property comes from first-order predicate logic and inference axioms. The transitive axiom states that if A implies B and B implies C, then A also implies C. Example: if CNT 4603 meets on Monday, and Monday is today, then by implication, CNT 4603 meets today.

Active Directory - Trees

- A trusted domain is one that is granted access to resources, whereas a trusting domain is the one granting the access.
- In a two-way trust, members of each domain can have access to the resources of the other. In other words, either domain can play the role of both a trusted domain and also that of a trusting domain.

Windows Server 2008 (and Server 2003) also have a forest trust. In a forest trust, a Kerberos transitive trust relationship exists between the root domains in Windows Server 2008 forests, resulting in trust relationships between all domains in the forest.

Active Directory - Trees

- Because of the trust relationship between parent and child domains, any one domain can have access to the resources of all the others.
- The security in the two-way trust relationships is based on Kerberos techniques, using a combination of protocol-based and encryption-based security techniques between clients and servers.
- A new domain joining a tree has an instant trust relationship with all the other member domains through the trust relationship that is established with its parent domain, which makes all objects in the other domains available to the new one.

Active Directory - Trees

- All domains within a single tree (as well as all trees in a single forest) share the same schema defining all the object types that can be stored within AD.
- Further, all domains in a tree also share the same global catalog and a portion of their namespace.
- In addition, a child domain contains part of the namespace of the parent domain.

Active Directory - Domain

- Microsoft views a domain as a logical partition within an AD forest.
- A domain is a grouping of objects that typically exist as a primary container within AD.
- The basic functions of a domain are as follows:
  - To provide an AD “partition” in which to house objects, such as accounts and groups, that have a common relationship, particularly in terms of management and security.
  - To establish a set of information to be replicated from one DC to another.
  - To expedite management of a set of objects.

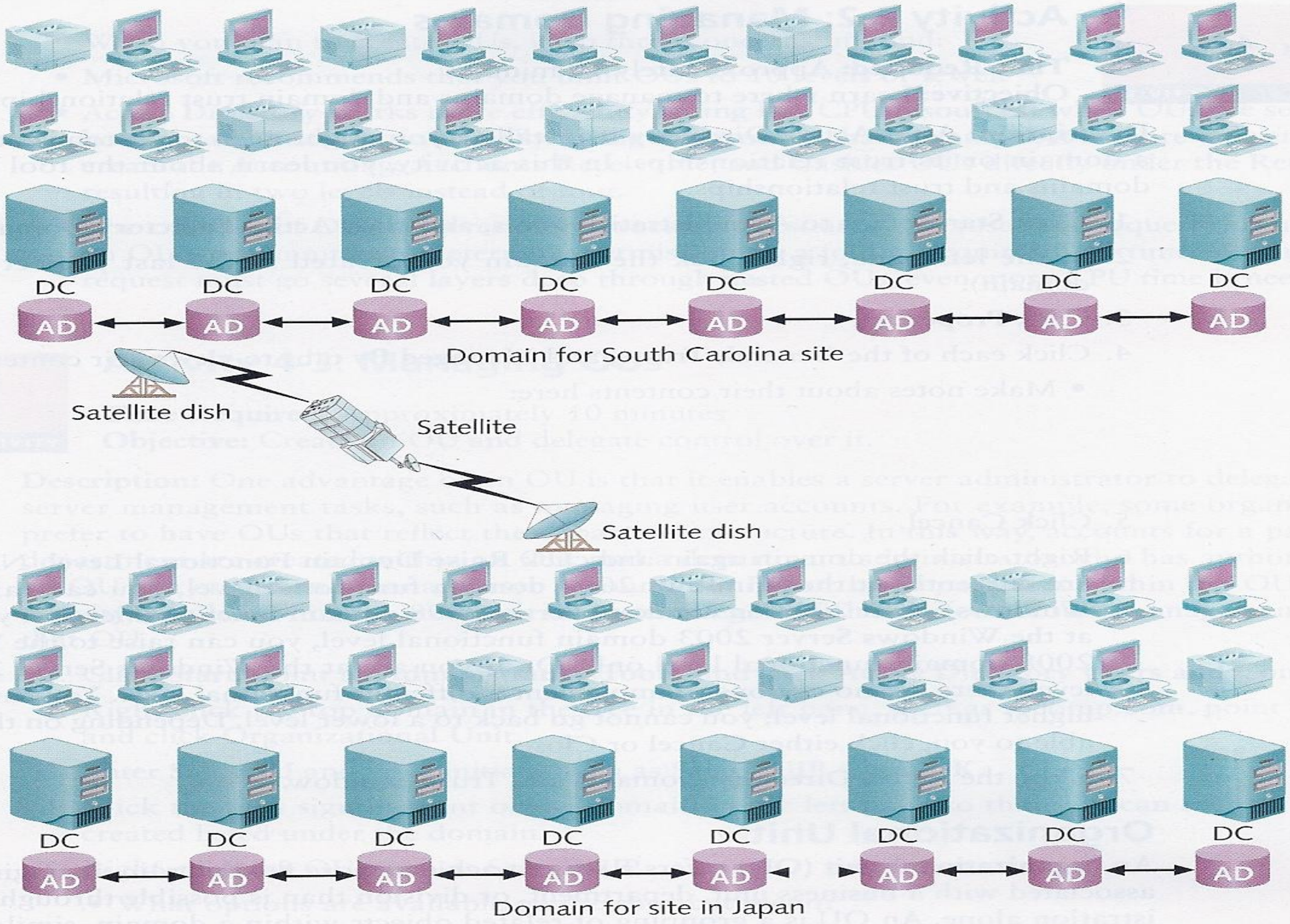
Active Directory - Domain

- When you use a server-based networking model to verify who to log on to the network, there is at least one domain.
  - For example, if you are planning an AD for a small organization of 34 employees who have workstations connected to a network that has one or two Windows Server 2008 server, then one domain is sufficient for that organization.
- The domain functions as a partition within which to group all of the network objects consisting of servers, user account, shared printers, and shared folders and files.

Active Directory - Domain

- In a midsized or larger organization, you might use more than one domain. This would be especially true if the business units are separated by large distances and you want to limit the amount of DC replication over expensive WAN links or to manage the objects differently between locations, such as through different account or security policies.

- Consider the following example: a company builds tractors in South Carolina and has a parts manufacturing division in Japan. Each site has a large enterprise network of Windows Server 2008 servers, and the sites are linked together in a WAN by an expensive satellite connection. When you calculate the cost of replicating DCs over the satellite link, you cannot justify it in terms of the increased traffic that will delay other virtual daily business communications. In this situation it makes sense to create two separate domains, one for each site, as shown on the next page.


DC
AD
Domain for South Carolina site
Satellite dish
Satellite
Satellite dish
DC
AD
Domain for site in Japan

Active Directory - Domain

- Windows Server 2008 AD recognizes three domain functional levels, which refers to the Windows Server OS on domain controllers and the domain-specific functions they support.

- The domain functional levels are:

- *Windows 2000 domain functional level* – provides AD functions compatible with a network that has a combination of Windows 2000 Server, Windows 2003 Server, and Windows 2008 Server domain controllers. This level supports universal groups, which were not previously supported in Windows NT Server, converting types of groups, and nesting groups.

- *Windows Server 2003 domain functional level* – intended for Windows Server 2003 and 2008 domain controllers only and enables more domain management functions, such as delegating management of AD object, time stamps for logons, use of Authorization Manager policies in AD, and other features not available in Windows Server 2000 domain controllers.

Active Directory - Domain

- *Windows Server 2008 domain functional level* – contains only Windows Server 2008 domain controllers, and offers new features such as default incorporation of the Distributed File System (DFS), with better security, enhanced security for Kerberos authentication, Advanced Encryption Standard (AES) encryption servers, and enhanced user account password policies, including fine-grained password policies.

Active Directory – Organizational Unit

- An organizational unit (OU) offers a way to achieve more flexibility in managing the resources associated with a business unit, department, or division than is possible through domain administrations alone.
- An OU is a grouping of related objects within a domain, similar to the idea of having subfolders within a folder.
- OUs can be used to reflect the structure of the organization without having to completely restructure the domain(s) when that structure changes.
- OUs allow the grouping of objects so that they can be administered using the same group policies, such as security and desktop setup.

Active Directory – Organizational Unit

- OUs also make it possible for server administration to be delegated or decentralized.
  - For example, in a software development company in which the employees are divided into 15 project teams, the user accounts, shared files, shared printers, and other shared resources of each team can be defined as objects in separate OUs. There would be 1 domain for the entire company and 15 OUs within that domain, all defined in AD.
  - With this arrangement, file and folder objects can be defined to specific OUs for security, and the management of user accounts can be delegated to each group leader (OU administrator).

Active Directory – Organizational Unit

- OUs can also be nested within OUs, as subfolders are nested in subfolders, so that you can create them several layers deep.
  - For example, you might have one OU under the Retail Sales OU for the Accounting Department, and OU under the Accounting Department for the Accounts Receivable Group, and an OU under Accounts Receivable for the Cashiers, thus creating four layers of OUs.
- The problem with this approach is that creating OUs many layers deep can get as confusing as creating subfolders several layers deep. It is confusing for the server administrator to track layered OUs, and it is laborious for AD to search through each layer.

Active Directory – Organizational Unit

- When you plan to create OUs, keep three things in mind:

1. Microsoft recommends that you limit OUs to 10 levels or fewer.

2. AD works more efficiently (using less CPU resources) when OUs are set up horizontally instead of vertically. For example, it is more efficient to create the Accounting, Accounts Receivable, and Cashier OUs directly under the Retail OU, resulting in two levels instead of four.

3. The creation of OUs, involves more processing resources because each request through an OU (for example, to determine the permission of a folder) requires CPU time. When that request must go several layers deep through nested OUs, even more CPU time is needed.

Active Directory – Site

- A site is a TCP/IP –based concept (container) within AD that is linked to IP subnets and has the following functions:
  - Reflects one or more interconnected subnets, usually having good network connectivity.
  - Reflects the physical aspect of the network.
  - Is used for DC replication.
  - Is used to enable a client to access the DC that is physically closest.
  - Is composed of only two types of objects, servers and configuration objects.

Active Directory – Site

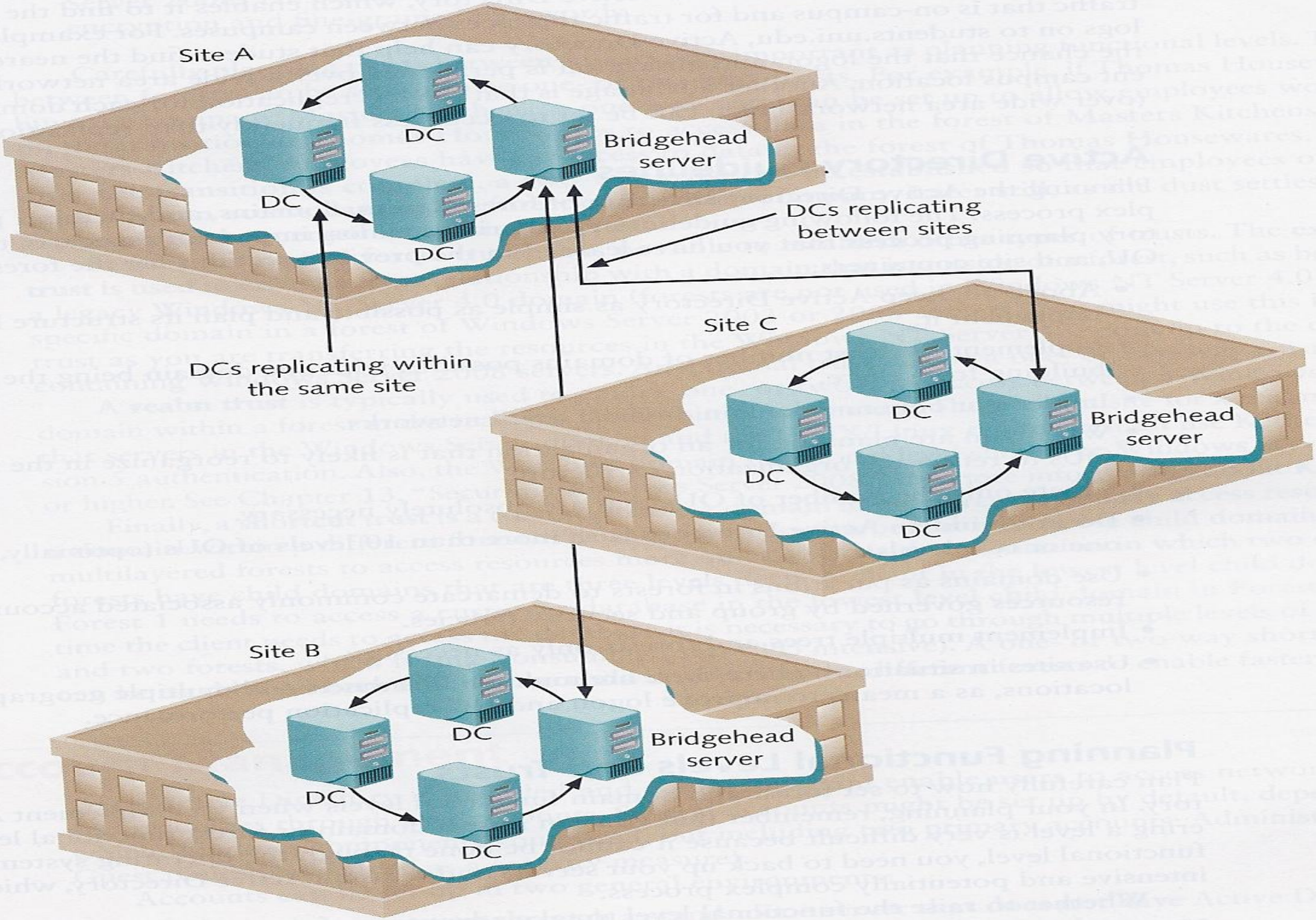
- Sites are based on connectivity and replication functions.
- You might think of sites as a way of grouping AD objects by physical location so AD can identify the fastest communication paths between clients and servers and between DCs.
- The physical representation of the network to AD is accomplished by defining subnets that are interconnected. For this reason, one site may be contained within a single OU or a single domain, or a site may span multiple OUs and domains, depending on how subnets are setup.
- The most typical boundary for a site consists of the LAN topology and subnet boundaries rather than the OU and domain boundaries.

Active Directory – Site

- There are two important reasons to define a site.
- First, by defining site locations based on IP subnets, you enable a client to access network servers using the most efficient route.
- In the partsplus.com example (see pages 5-7), it is faster for a client in Toronto to be authenticated by a Toronto global catalog server than for a client to go through Detroit or Mexico City.
- Second, DC replication is the most efficient when AD has information about which DCs are in which locations.
- Within a site, each DC replicates forest, tree, domain, and OU naming structures, configuration naming elements, such as computers and printers, and schema information.

Active Directory – Site

- One advantage of creating a site is that it sets up redundant paths between DCs so that if one path is down, there is a second path that can be used for replication.
- This redundancy is in a logical ring format, which means that replication goes from DC to DC around a ring until each DC is replicated.
- If a DC is down along the main route, the AD uses site information to send replication information in the opposite direction around the ring.
- Whenever a new DC is added or an old one removed, AD reconfigures the ring to make sure there are two replication paths available from each DC.
- Between sites, replication is coordinated through one server, called a bridgehead server, located at each site. See next page.


Site A
DC
DC
DC
Bridgehead server
DCs replicating between sites
DCs replicating within the same site
Site C
DC
DC
DC
Bridgehead server
Site B
DC
DC
DC
Bridgehead server

Active Directory – Site

- When you replicate between sites, the replication occurs only between two bridgehead servers.
- The bridgehead server is a DC that is designated to have the role of exchanging replication information.
- Only one bridgehead server is set up per site, so the network traffic per site is kept to a minimum. Otherwise, having multiple DCs replicating with partners across sites could take up considerable bandwidth.

Active Directory Guidelines

- Planning the AD structure of forests, trees, domains, and OUs is a potentially complex process. The following guidelines summarize the most important aspects of the AD planning process.
- Above all, keep AD as simple as possible and plan its structure before you implement it.
- Implement the least number of domains possible, with one domain being the ideal and building from there.
- Implement only one domain on most small networks.
- When you are planning for an organization that is likely to reorganize in the future, use OUs to reflect the organization’s structure.

Active Directory Guidelines

- Create only the number of OUs that are absolutely necessary.
- Do not build an AD with more than 10 levels of OUs (optimally, no more than one or two levels).
- Use domains as partitions in forests to demarcate commonly associated accounts and resources governed by group and security policies.
- Implement multiple trees and forests only as necessary.
- Use sites in situations where there are multiple IP subnets and multiple geographic locations, as a means to improve logon and DC replication performance.

More Active Directory Basics

- AD is a directory service that houses information about all network resources such as printers, user accounts, groups of user accounts, security policies, and other information.
- As a directory service, AD (Active Directory Domain Services – or AD DS) is responsible for providing a central listing of resources and ways to quickly find and access specific resources as well as providing a way to manage network resources.
- Writable copies of information in AD are contained in one or more domain controllers (DCs), which are servers that have the AD DS server role installed.
- Servers on a network managed by AD that do not have AD installed are called member servers (and are not domain controllers).

More Active Directory Basics

- Microsoft recommends that are least two DCs should be present in any organization using AD. This is to ensure that if one DC goes down, the other is still available to service user account requests to log on and access resources.
- In AD, a domain is a fundamental component or container that holds information about all network resources that are grouped within it – servers, printers, and other physical resources, users, and user groups.
- A domain is usually a high-level representation of how an organization is structured. Common structures reflect geographic locations or corporate division hierarchies.

More Active Directory Basics

- Every resource is called an object and is associated with some domain.
- When you set up a new user account or a network printer, for example, it becomes an object within a domain.
- In Windows Server 2008, every DC is equal to every other DC in that it contains the full range of information that composes an AD.
- If information on one AD changes, such as the creation of a new user account, it is replicated automatically (see page 53) to all other DCs, in a process known as multimaster replication.

"The trouble with quotes on the internet is that one can never be sure if they are genuine" - Abraham Lincoln

More Active Directory Basics

- In Windows Server 2008 the system administrator can set replication of an AD to occur at a preset interval instead of automatically upon the occurrence of an update in some DC.
- You can also determine how much of AD is replicated each time it is copied from one DC to another.
- AD is designed to make replication efficient so that it transports as little as possible over the network, saving network resources.

More Active Directory Basics

- AD in Windows Server 2008 can:
  - Replicate individual properties instead of entire accounts, which means that a single property can be changed without replicating information for the entire account.
  - Replication can be done based on the speed of the network link, such as replicating more frequently over a LAN than over a WAN.

More Active Directory Basics

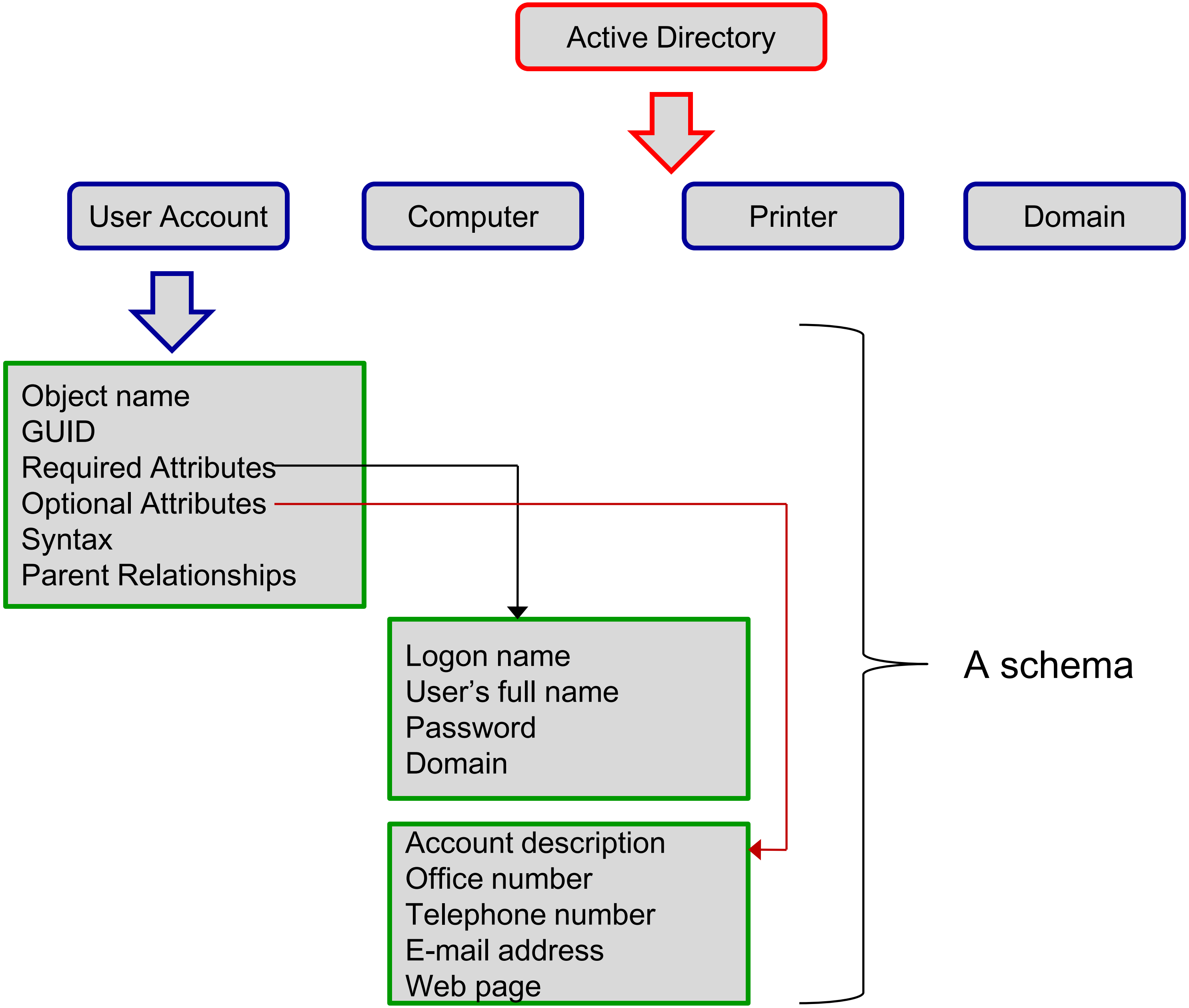
- The AD schema defines the objects and the information pertaining to those objects that can be stored in AD.
- Each kind of object in AD is defined through the schema, which is like a small database of information associated with that object, including the object class and its attributes.
- Schema information for objects in a domain is replicated on every DC.

More Active Directory Basics

- A user account is one class of objects in AD that is defined through schema elements unique to that class.
- The user account class as a whole has the following schema characteristics:
  - A unique object name
  - A globally unique identifier (GUID), which is a unique number associated with the object name.
  - Required attributes – must be defined for each object.
  - Optional attributes – optional definition for any object.
  - A syntax (format) to determine how attributes are defined.
  - Pointers to parent entities, such as to a parent domain.

More Active Directory Basics

- Examples of required user account attributes are:
  - Logon name
  - User’s full name
  - Password
  - Domain
- Examples of optional user account attributes are:
  - Account description
  - Account holder’s office number or address
  - Account holder’s telephone number
  - Account holder’s email address
  - Account holder’s web page
- An example schema for user accounts is shown on the next page.



Active Directory

User Account

Computer

Printer

Domain

Object name
GUID
Required Attributes
Optional Attributes
Syntax
Parent Relationships

Logon name
User's full name
Password
Domain

Account description
Office number
Telephone number
E-mail address
Web page

A schema

More Active Directory Basics

- To some extent, the optional attributes may be influenced by the security policies that the server administrator sets in AD for a class of objects. We'll see more about security policies in AD later.
- Each attribute is automatically given a version number and date when it is created or changed.
- This information enables AD to know when an attribute value, such as a password, is changed, and update only that value on all DCs.
- When you install Windows Server 2008 for the first time on a network server, designating it as a DC, you also create several object classes automatically.
- The default object classes include domain, user account, group, shared drive, shared folder, computer, and printer.

More Active Directory Basics

- The global catalog stores information about every object within a forest.
- The first DC configured in a forest becomes the global catalog server.
- The global catalog server will store a full replica of every object within its own domain and a partial replica of each object within every domain in the forest.
- The partial replica for each object contains those attributes most commonly used to search for objects.

More Active Directory Basics

- The global catalog serves the following purposes:
  - Authenticating users when the log on.
  - Providing lookup and access to all resources in all domains.
  - Providing replication of key AD elements.
  - Keeping a copy of the most used attributes for each object for quick access.
- The global catalog server enables forest-wide searches of data.
- Because it contains attributes pertaining to every object within a forest, users can query this server to locate an object, as opposed to having to perform an extensive search.

More Active Directory Basics

- The global catalog server also can be used for network logons.
- When a user logs on to the network, the global catalog server is contacted for universal group membership information pertaining to the user’s account (universal groups will be covered later in the course).
- In a Windows 2000 domain, if the global catalog was unavailable, the user could only log on to the local computer. In Windows Server 2003 and 2008, if the global catalog is unavailable for group membership information, the user can log on to the network with cached credentials.

More Active Directory Basics

- Cached credentials means that a record is kept in server cache if a user has successfully logged on previously.
- Authentication, when the user logs off and subsequently logs on again, can be performed by checking the cached credentials, instead of the global catalog.
- However, when a user is logging on for the first time and there is no cached credential for that user, if the global catalog is unavailable, access will be provided only to the local computer.

More Active Directory Basics

- By default, the first DC in the forest is automatically designated as the global catalog server. The system administrator has the option of configuring another DC to be a global server as well as designating multiple DCs as global catalog servers.
- There must be at least one global catalog server in a forest.
- In most cases, it also makes sense to place one global catalog server in every site.
- If an organization utilizes email servers, such as for Microsoft Exchange, one global catalog server for every four mailbox servers is recommended . Since global catalog servers can generate heavy network traffic, configuring every DC to be a global catalog server is too much!

Planning Functional Levels and Trusts

- Careful planning about how to set forest and domain functional levels when you implement AD should be performed.
- In the planning, you should remember that it is easier to raise a domain or forest functional level, but lowering a level is very difficult since it cannot be done through the operating system.
- To lower a functional level, you will need to backup the servers and reinstall AD, which is a lengthy and potentially complex task.
- Whether to raise the functional level to take advantage of newer features should be weighed against the versions of servers that must be supported and the anticipated changes within an organization.

Planning Functional Levels and Trusts

- For example, one branch of an organization might have all Windows Server 2008 DCs, but another branch of the organization might have Windows Sever 2003 DCs.
- In this sort of situation, the domains and forests would be kept at the Windows Server 2003 domain and forest functional levels.
- If your organization is currently at the Windows Server 2000 domain and forest functional levels, and there is some likelihood of a merger with another organizations, it would be best to remain at the current functional levels until you are certain about the functional levels already in use at the other organization. In this case, you don't want to raise to the Server 2008 levels and later discover that the other organization has a Server 2003 domain, which would require reinstalling AD.

Planning Functional Levels and Trusts

- On the other hand, if you are in a relatively small organization with no intention of a merger and have upgraded all of your servers to Windows Server 2008, it would be best to raise the forest and domain levels to Windows Server 2008 level.
- This would enable you to take advantage of all the new features, such as better encryption and fine-grained passwords.

Planning Functional Levels and Trusts

- Carefully planning trusts between forests is as important as planning functional level.
- Trusts between forests can be set up to be one- or two- way trusts.
- For example, if Organization A buys Organization B, a one-way trust can be set up to allow employees working on the transition at A to access data in the forest of B, but employees at B would have no access to data in the forest of A.
- Later after the transition is complete, a two-way trust can be established so that employees of each organization can access data in the forest of the other.
- Later still, as the dust from the merger settles, both forests might be merged into a single forest.

Planning Functional Levels and Trusts

- AD also provides other types of trusts.
- An external trust is used to create a trust relationship with a domain that is outside of a forest.
- A realm trust is typically used to enable one- or two- way access between a Windows Server domain within a forest and a realm of Unix/Linux computers. The prerequisite for a realm trust is that the servers in the Windows Server domain and the Unix/Linux realm must all use Kerberos version 5 authentication. Also the Windows domain functional level must be at the 2003 or higher level.

Planning Functional Levels and Trusts

- A shortcut trust is a trust to enable a domain in one forest to quickly access resources in a domain within a different forest.
- The shortcut trust is ideal to enable child domains within multilayered forests to access resources more quickly.
- Consider a situation in which two different forests have child domains that are three levels deep. A client in the lowest level child domain in Forest 1 needs to access a customer database in the lowest level child domain in Forest 2. Each time the client needs to access the database it is necessary to go through multiple levels of domains and two forests, which is time consuming (and CPU intensive). A one- or two-way shortcut trust can be established between the two child domains in different forests to enable faster access.