CNT 4603: System Administration
Spring 2011

Introduction To Active Directory – Part 1

Instructor : Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 4078-823-2790
http://www.cs.ucf.edu/courses/cnt4603/spr2011

Department of Electrical Engineering and Computer Science
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

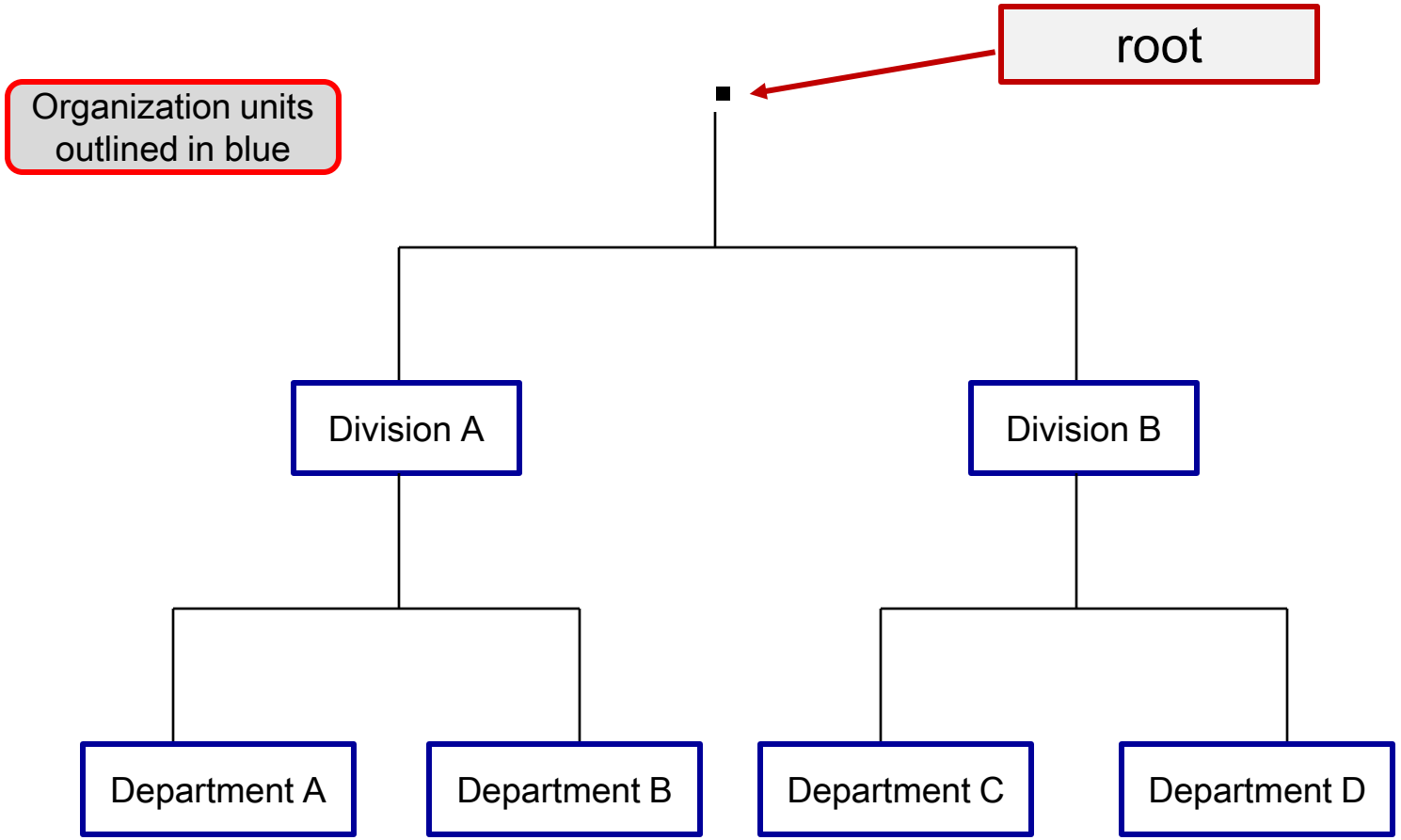
- Two of the more common directory structures in use within networks are based on object function (such as printers, servers, and storage devices) and organizational responsibility (such as marketing, accounting, and manufacturing).
- The organizational model allows you to store objects in groups, or 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.

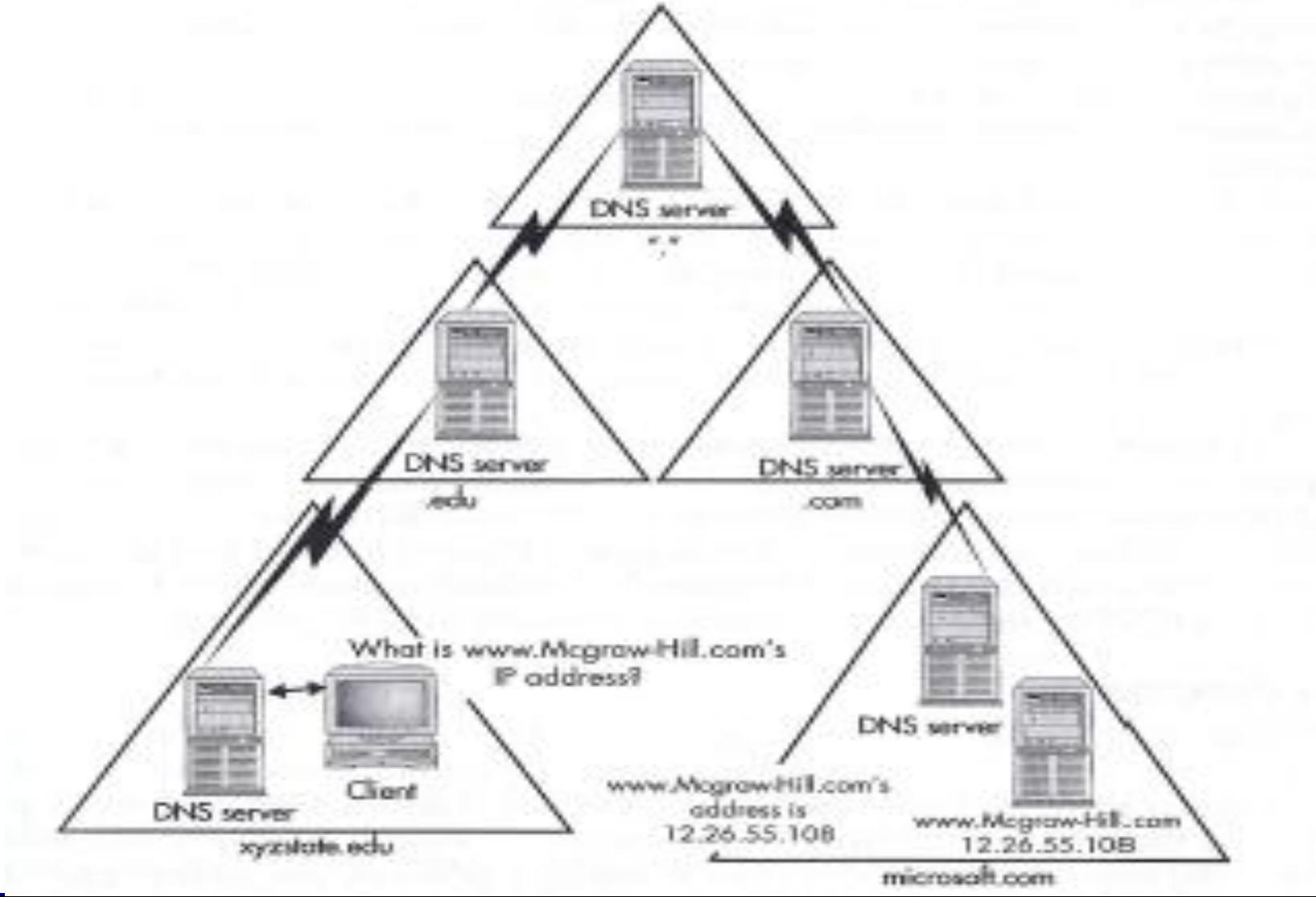
Integration With DNS

- 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



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.