CISNTWK-11

Microsoft Windows Server

Active Directory Overview

Background

- ***Directory***
  - Is a comprehensive catalog of information
    - names
    - phone numbers
    - computers
    - software
    - services
  - It is organized in a manner that makes the information easily accessible

Background

- ***Directory Services***
  - It is based on a *Directory*
  - It is a distributed database
  - It stores information about your network resources
  - It allows for accessing this information
  - It allows for searching this information using search criteria
  - It facilitates the resources location and management

What is Active Directory?

- ***Active Directory***
  - Is the implementation of *Directory Services* for Windows 2000 (or greater) Server
    - the full capabilities of Active Directory are only available with Windows 2000 (client or server) or greater
    - Active Directory requires Windows Server (s) configured as Domain Controller(s).
  - Is the central repository (database) of network resources
  - Is the functional replacement of NT 4 Domains
  - Describes
    - what information can be stored in the database
    - how it is stored in the database
    - how users can query the database to obtain specific information about network resources

Enterprise Requirements

- Enterprise *Directory Services* requirements
  - Centralization
  - Scalability
  - Reliable
  - Ease of administration
  - Integration with security
  - Integration with applications
  - Standardization and openness
    - based on “open” industry standards
    - is extensible (you can add to it)

Enterprise Requirements (continued)

- *Active Directory* meets the "enterprise" *Directory Services* requirements
  - Active Directory is centralized
  - Active Directory is scalable
  - Active Directory makes Windows networks easier to administer
  - Active Directory is built on the Windows Server security model
    - it is tightly integrated with Windows Server
    - makes use of Access Control Lists (ACLs)

Enterprise Requirements (continued)

- Active Directory implements industry standards
  - Active Directory Services is accessible programmatically through the Lightweight Directory Access Protocol (LDAP)
  - Active Directory incorporates Domain Name System (DNS) for name translation
- Active Directory is open (extensible)

Active Directory
The Logical Structure

- The following terms are used to help describe Active Directory, from “least encompassing” (lowest level) to “most encompassing” (highest level)
  - **Object**
    - the basic unit in Active Directory
    - examples include: Users, Groups, and Computers
  - **Organizational Unit**
    - a “container” of Objects
  - **Domain**
    - an administrative boundary
    - a security boundary
    - contains zero or more Organizational Units

Active Directory
The Logical Structure

- **Tree**
  - a Domain hierarchy
  - contains one or more Domains
- **Forest**
  - a collection of one or more Trees
  - they share the same Active Directory Schema, Configuration, and Global Catalog

Active Directory
The Physical Structure

- The physical structure of Active Directory is independent of the logical structure
- The physical structure consists of the following components
  - **Domain Controller**
    - houses the Active Directory database and services
    - runs on Windows Servers (2000 or better)
  - **Site**
    - a set of computers in one or more TCP/IP subnets
    - is used to facilitate the replication of the Active Directory database
    - allows client computers to access Active Directory in a “network efficient” manner

Active Directory
The Physical Structure

– Global Catalog

- a catalog of a selected set of properties from every object in an Active Directory Forest
- the Global Catalog is unique in that it is considered to be part of both the logical structure of Active Directory as well as the physical structure of Active Directory

Domain

- A Domain is collection of one or more computers
- Users, Groups, and network resources are associated with a Domain
- Domains act as security boundaries
  - Access to Domain resources require user authentication on that Domain
    - resources include directories, files, and printers
  - Users in one Domain are generally unable to access resources in another Domain unless they have a User Account in the other Domain

Domain

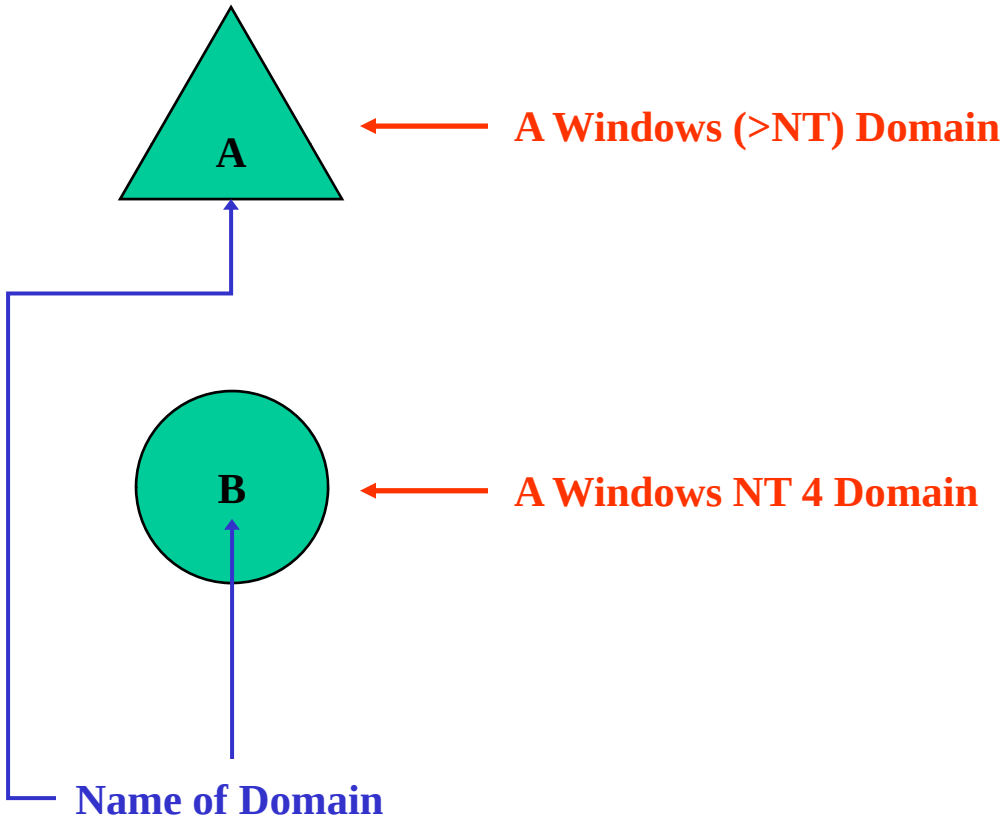
- Domains act as administrative boundaries
  - Domain A can be administered separately from Domain B
- Windows Servers and Client computers can belong to only one Domain at a time
  - Or no Domain if they are configured as a Workgroup
  - Or no domain if client OS < Windows NT Workstation

Domain (continued)

- Domains require Windows Server
  - For Windows 2003 Server
    - must be configured as a Domain Controller
  - For Windows NT server
    - one Primary Domain Controller (PDC)
    - zero or more Backup Domain Controllers (BDC)
- A “network” can support an arbitrary number of Domains

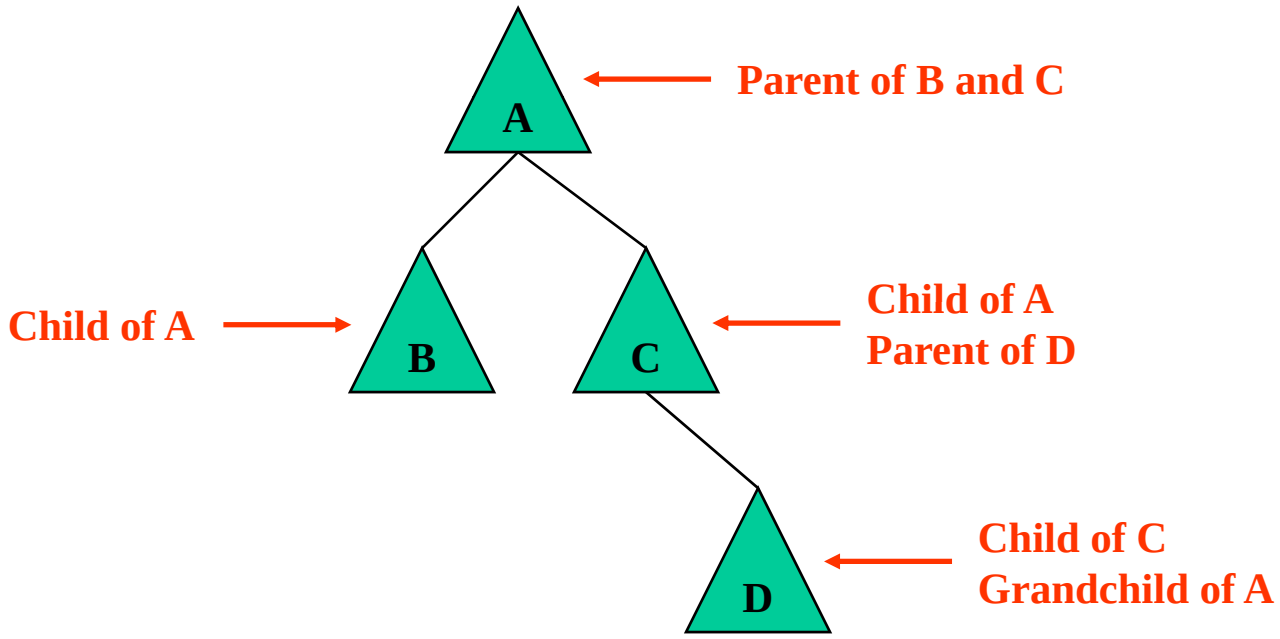
Domain Representation

- Domains are represented graphically as follows



Active Directory Domain Hierarchy

- Active Directory Domains can be organized in a parent-child relationship to form a hierarchy



Active Directory Domain Hierarchy Rules

- A child Domain can have exactly one parent
- A parent Domain can have zero or more child Domains
- **Very important**:
  - Administrators in the parent Domain **do not** automatically have administrative rights in a child Domain

Domain Name System (DNS)

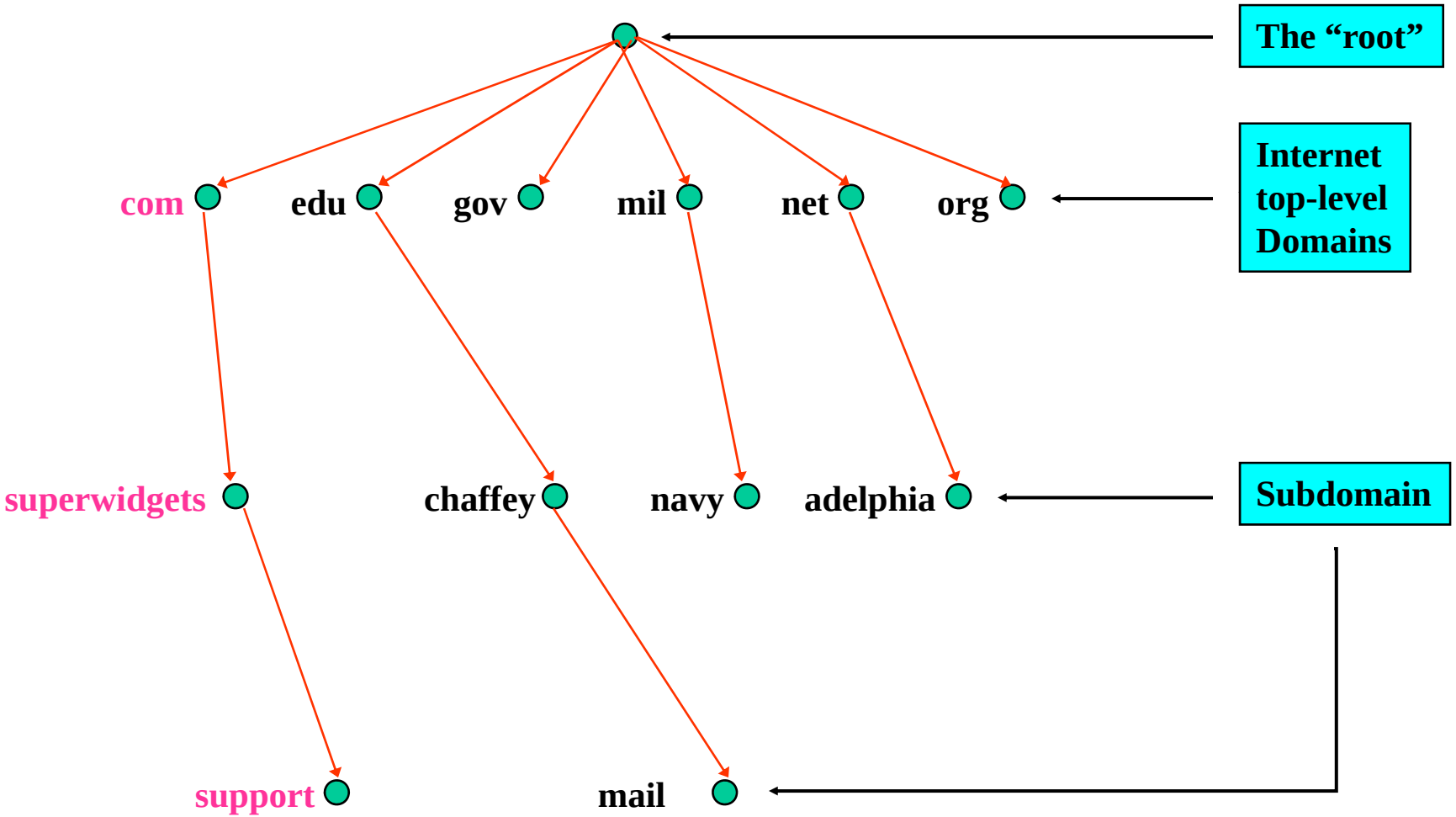
- Domain Name System (DNS) is a de facto naming system for IP based networks
- DNS is the naming service that is used to locate computers on the Internet
- DNS is used to translate “friendly” names to TCP/IP addresses
  - “IBM.COM” (DNS name) translates to “129.42.16.99” (IPv4 TCP/IP address)

Domain Name System (DNS)

- DNS is based on a hierarchy, just like Windows 2003 Domains
  - This hierarchy defines a *namespace*
  - Each element of the hierarchy is separated by a dot (“.”)
- A *namespace* is a context within which the names of all “objects” are unambiguously resolvable
- The DNS *namespace* is pictured as an inverted tree, with the “root” at the top

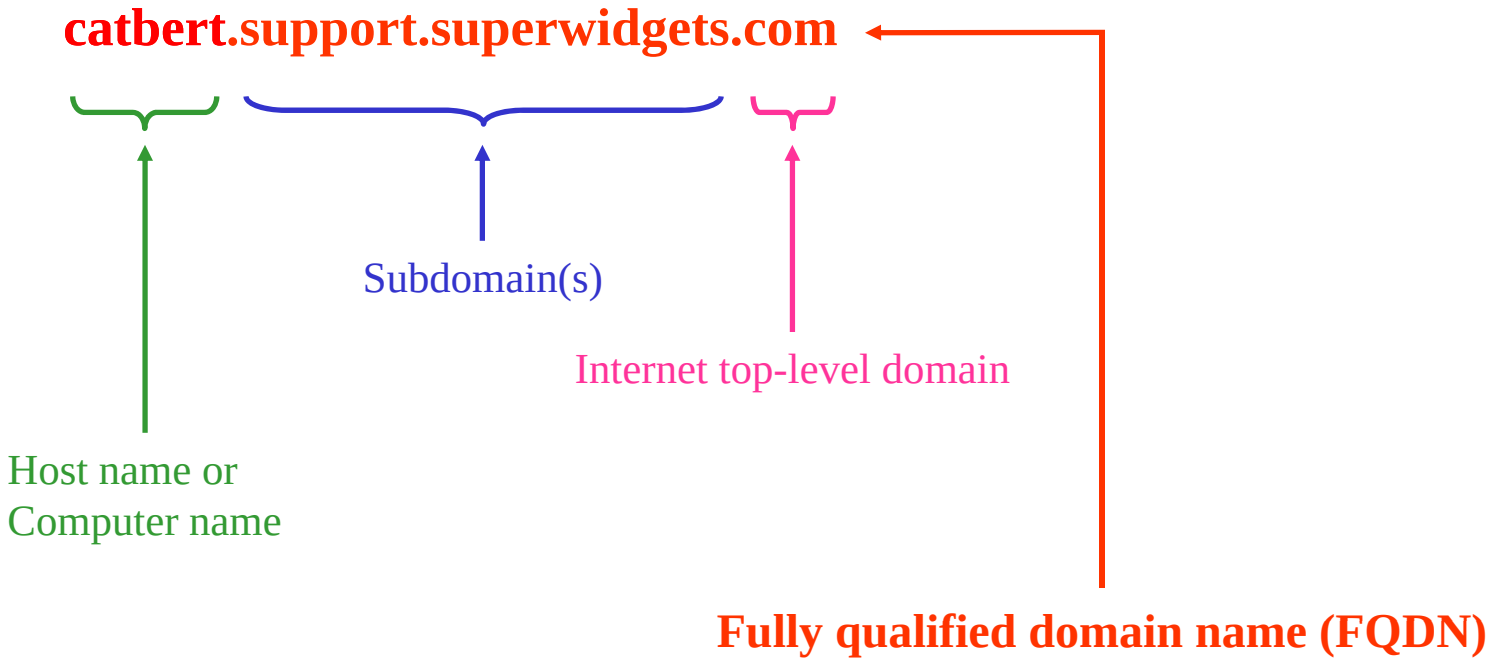
DNS Graphical Representation

- Here is an example of a DNS hierarchy



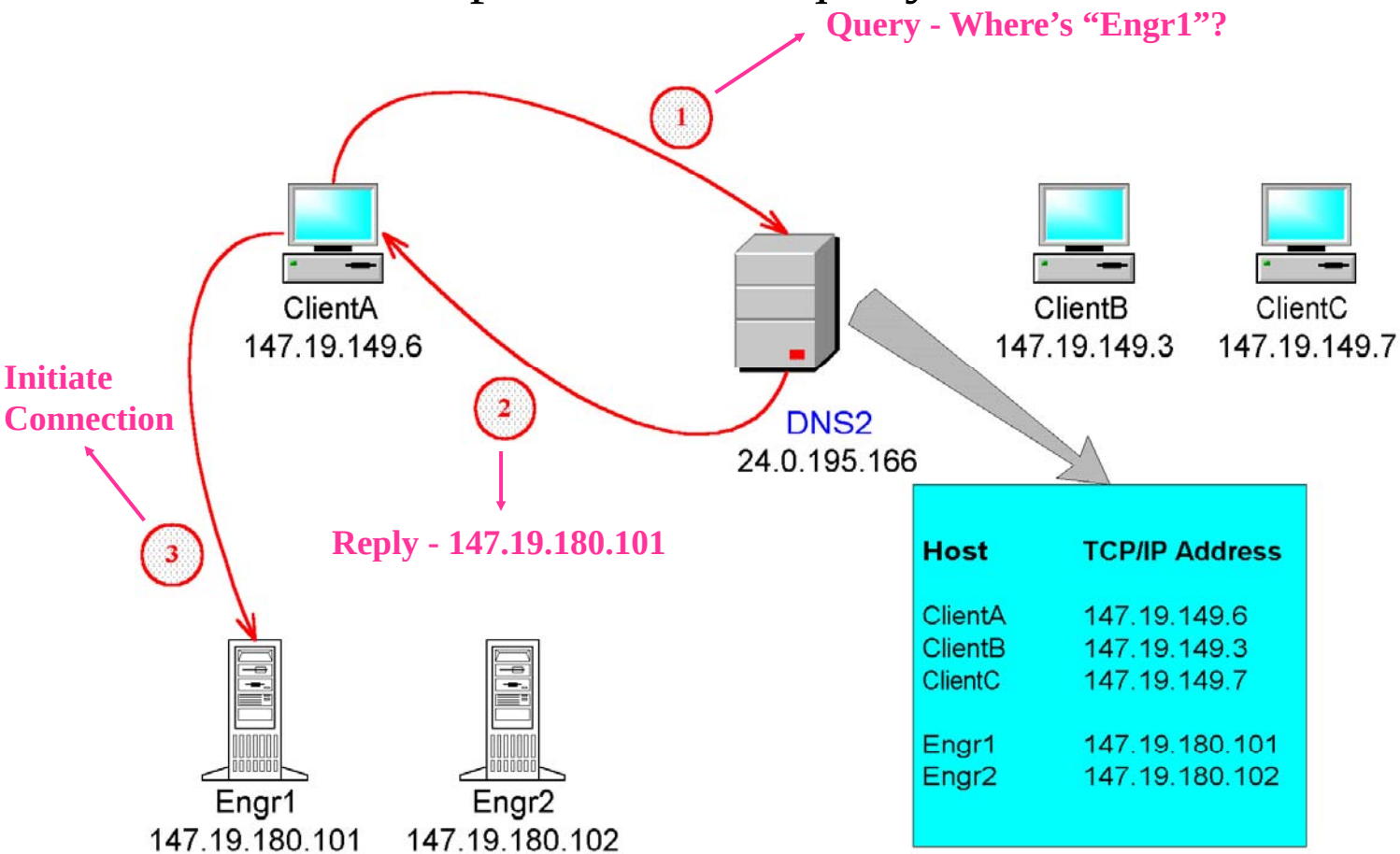
DNS Components

- Each computer in a DNS domain is uniquely identified by its fully qualified domain name (FQDN)
- Here is an example of a Windows Server DNS name:



What Does DNS Do?

- DNS is based on a client / Server model
- This is an example of a DNS query:



Active Directory and DNS

- Windows Servers uses Domain Name System (DNS) naming standards for hierarchical naming of Active Directory Domains and computers
- Windows Servers uses DNS to locate Domain Controllers and computers
  - This includes locating Active Directory on the network

Active Directory and DNS

- A Windows 2003/NT Domain is not the same as a "domain" as used by DNS
  - DNS domains and Active Directory Domains use identical naming standards for different namespaces
  - Each stores different data and therefore manages different objects
    - DNS is a "name resolution" mechanism
    - Windows Server Domains are administrative and security boundaries

Trusts

- A “Trust” is a relationship between two Domains that allows for resource sharing between the two Domains
- Trust relationships between Domains support the following capabilities
  - Permitting Domain A Users to logon to Domain B
    - with Windows (>NT), this is also supported in reverse
  - Permitting Domain B Users to access resources in Domain A
    - with Windows (>NT), this is also supported in reverse

Trusts

- Trusts are between Domains
  - Trusts are **not** established between computers
- Once a Trust is established, **all** the users participate in the Trust
  - Individual users cannot be excluded from a Trust relationship

Trusts (continued)

Approaches for accessing resources in another Domain without a Trust

- Enable the Guest Account on the Domain "owning" the resource
  - generally a poor approach - you lose any accountability

Approaches for accessing resources in another Domain without a Trust

- Add the same User Account with the same password on the other Domain
  - this generally undermines the notion of Domains in Windows Server
  - Windows Server will always try to authenticate with your Account name and password
    - this is a built-in behavior
    - this allows for “transparent” access to any (>Windows 98) computer
      - in any Domain or any Workgroup
  - this approach scales poorly
  - issues arise when the password expires on the originating Domain
    - there is generally no provision for keeping them synchronized

Trusts (continued)

Approaches for accessing resources in another Domain without a Trust

- You don't - the resources are kept separate (this is the "default" behavior)

Active Directory Objects

- The basic unit in Active Directory is an *Object*
- An *Object* is a distinct, named set of attributes that represents something concrete
- An *Object* consists of
  - A name
  - A “type”
  - One or more attributes

Active Directory Objects

- Common *Objects* in Active Directory include
  - User
  - Group
  - Computer
  - Printer
  - Shared Folder

Active Directory Tree

- Active Directory Domains are created in an inverted tree structure, with the root at the top
  - An Active Directory tree must have a contiguous namespace

Active Directory Tree

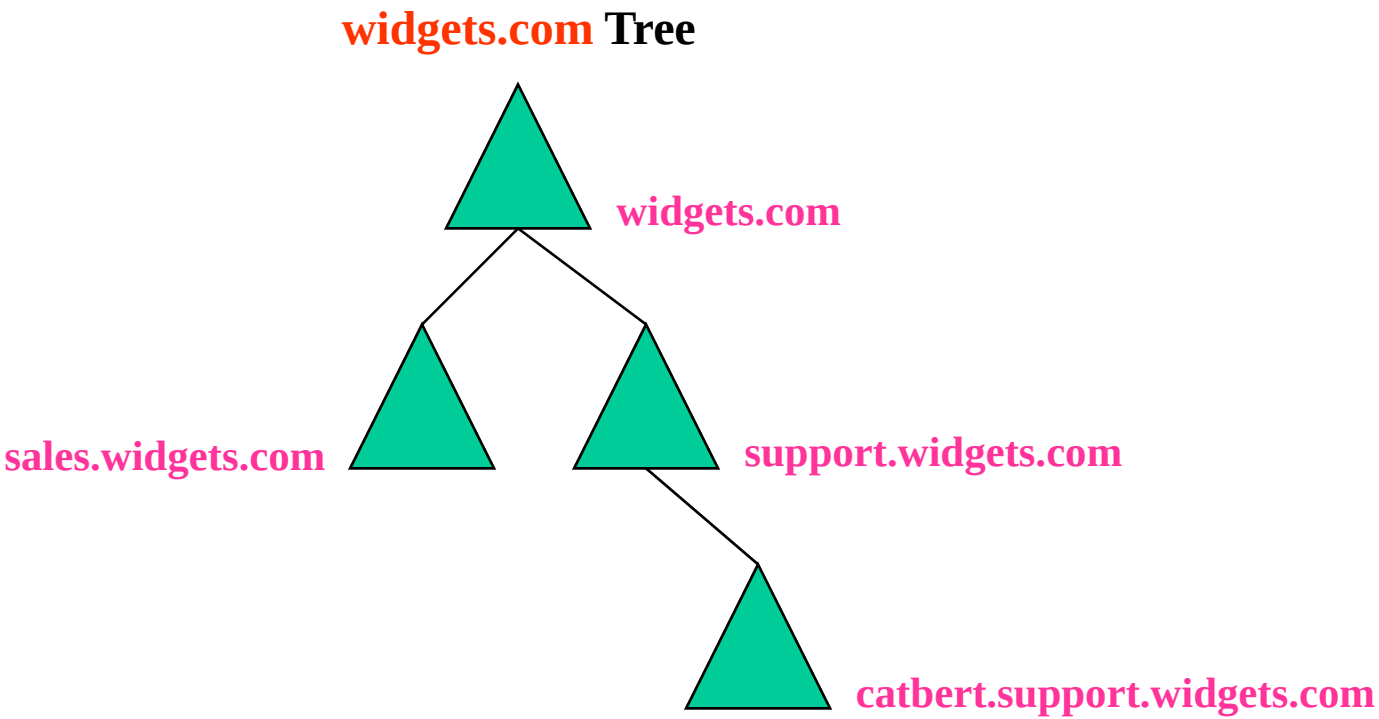
- The Windows Server Domain hierarchy is based on *Trust* relationships, each one being implicitly linked by inter-domain Trust relationships
  - All the Domains in a domain tree trust one another implicitly
  - The Trusts are transitive
    - if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C
  - The Trusts are bi-directional (with NT 4, this is referred to as a “two way” trust)
    - Domain A trusts Domain B
    - Domain B trusts Domain A

Active Directory Tree

- This allows users to logon to the Domain tree from any computer that is a member of the Domain tree
  - The computer could be a member of Domain A and their User Account could be a member of Domain B
- This also allows access to resources in any Domain within the Domain tree

Active Directory Tree Example

- Here is an example of a Domain Tree



Active Directory Forest

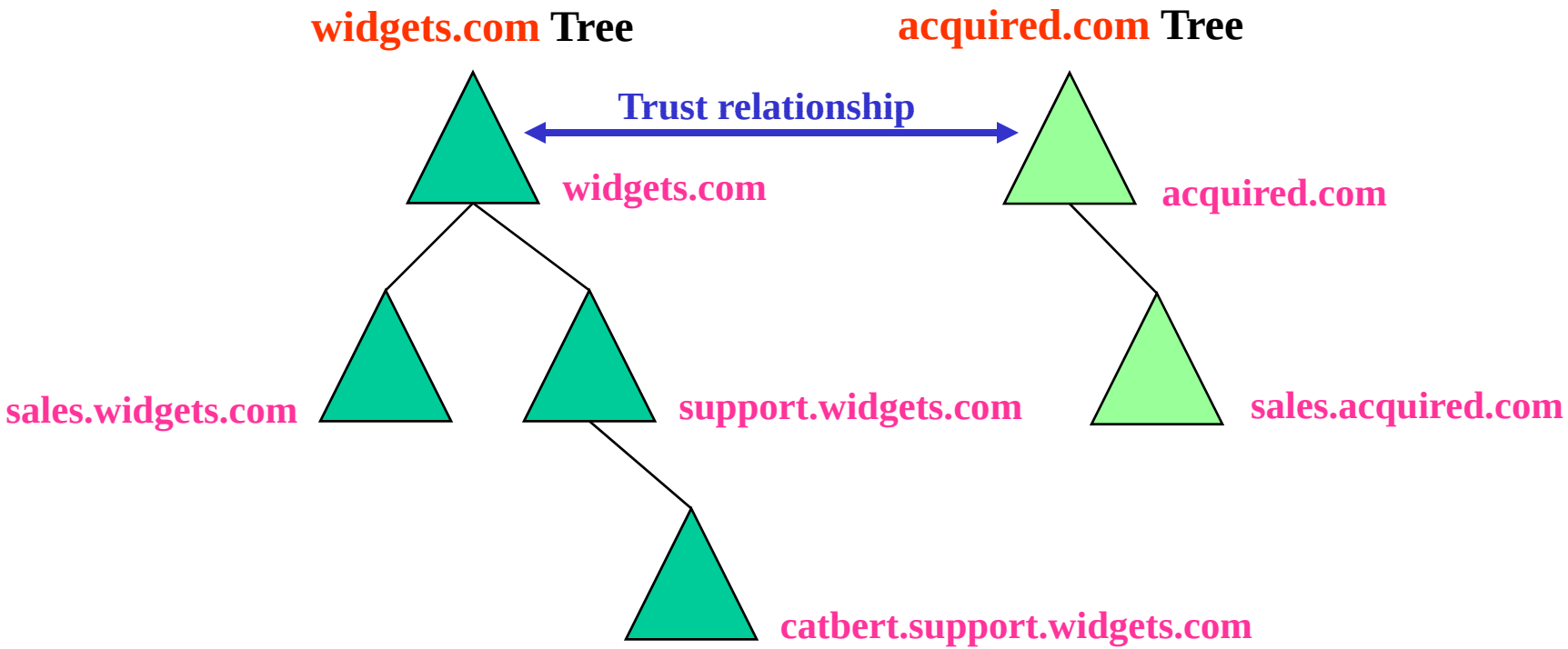
- An Active Directory Forest is a collection of one or more Active Directory Trees
- For an Active Directory Forest to exist with two or more Active Directory Trees, the Active Directory trees must form a noncontiguous namespace based on different DNS “root” domain names
- The Active Directory Trees are joined together at the “root” with a two way Trust relationship

Active Directory Forest

- All Active Directory Trees in an Active Directory Forest share a common
  - Schema
  - Configuration
  - Global Catalog (GC)

Active Directory Forest Example

- Here is an example of a Domain Forest



Active Directory Organizational Unit

- An Organizational Unit (OU) is a type of Active Directory "container" that is placed in a Domain
  - This allows administrators to logically organize and store objects in a Domain
  - Each Domain can implement its own Organizational Unit hierarchy independent of other Domains

[1] This topic is covered in a separate lecture. Refer to "Profiles and Policies" for details

Active Directory Organizational Unit

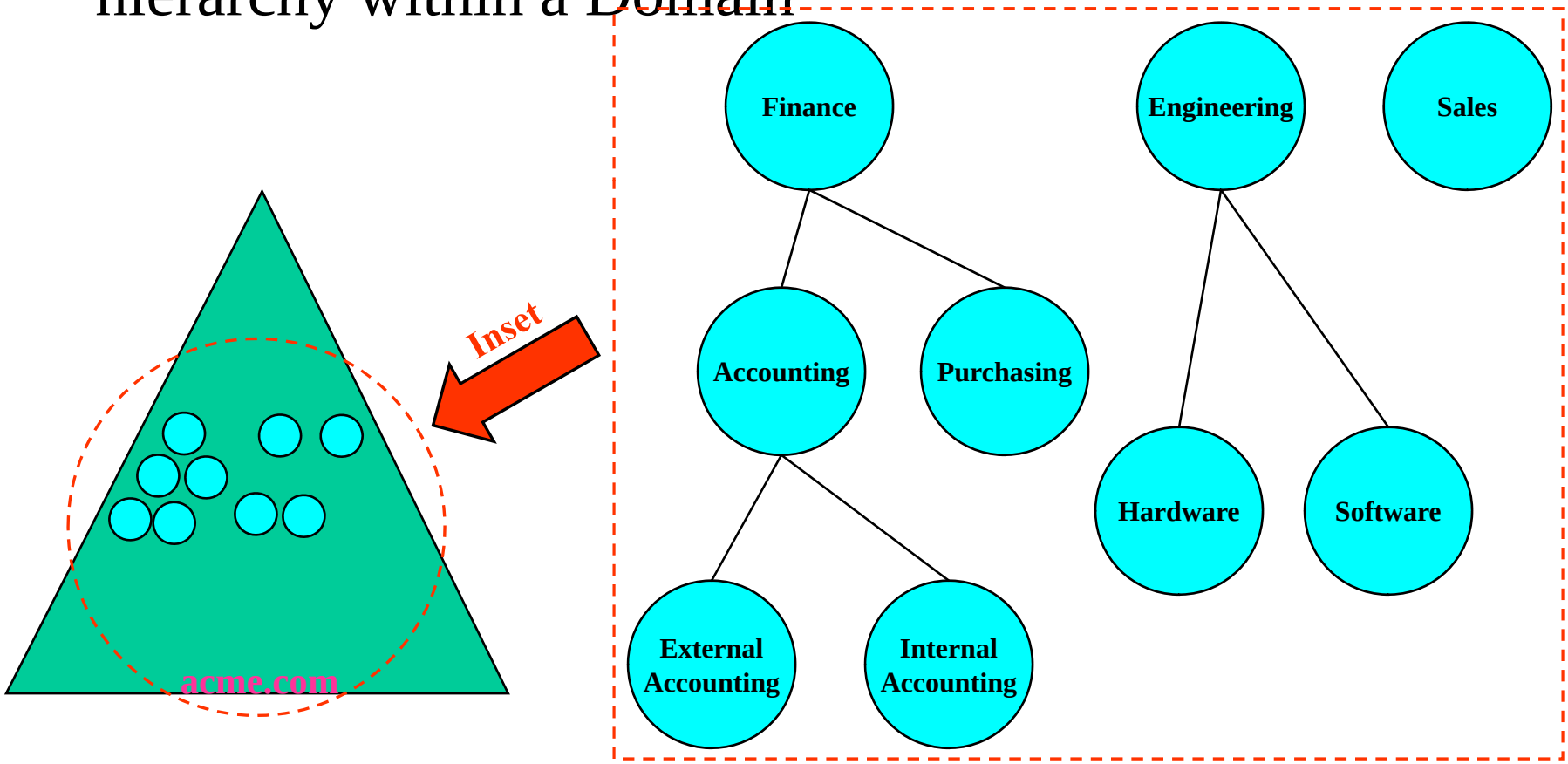
- An OU can contain zero or more of the following Active Directory Objects
  - User
  - Group
  - Computer
  - Printer
  - Shared Folder
  - Organizational Unit (OU)
    - this implies that Organizational Units can be nested

Active Directory Organizational Unit

- An OU allows an administrator
  - to delegate administration
  - to apply Group Policy to subsets of your users and computers
  - to keep objects with identical security requirements together

Active Directory
Organizational Unit Example

- Here is an example of an Organizational Unit hierarchy within a Domain

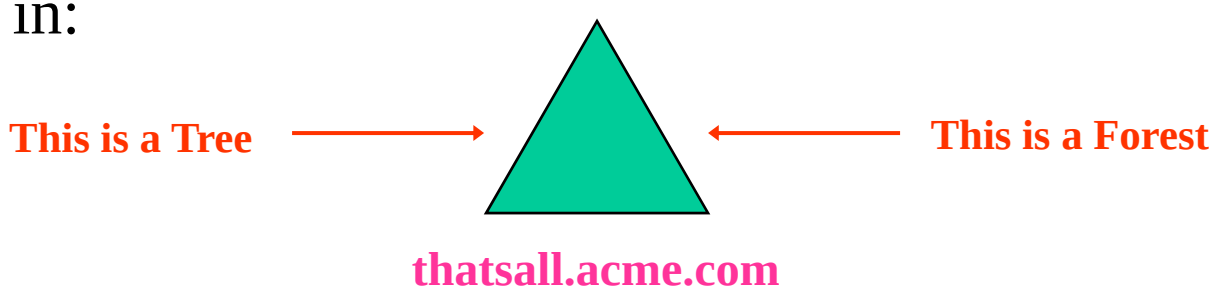


Domains at Their Simplest

- Tree(s) and Forest(s) are used to help scale Active Directory at the enterprise
  - This scaling is accomplished using the following components
    - the use of an Active Directory Tree comprised of more than one Domain
    - the use of an Active Directory Forest comprised of more than one Tree

Domains at Their Simplest

- At the most fundamental level of Active Directory deployment
  - You start out with a single Domain
  - You may end up with a single Domain
- This single Domain may contain no Organizational Units
- These terms - “Tree” and “Forest” - “compress” into a single Domain
  - As in:



Creating a Windows 2003 Domain Controller

- A Windows (>NT) Server can become a Domain Controller through the "Active Directory Installation" wizard
  - The program is called "DCPROMO" (Domain Controller promotion / demotion)
    - Start Menu -> Run .. (enter "DCPROMO" as the program name)
  - You can also perform this task "indirectly" through
    - Start Menu -> Programs -> Administrative Tools -> Configure Your Server
      - choose Active Directory and select "Start the Active Directory wizard"

Creating a Windows 2003 Domain Controller

- The Active Directory Installation wizard can create the following types of Domain Controllers
  - Create a new forest of Domain trees (Forest Root Domain)
  - Create a new Domain tree in an existing forest
  - Create a new child Domain in an existing Domain tree
  - Create an additional Domain Controller for an existing Domain
- You will need to have administrative rights in the appropriate Domain
- The Active Directory Installation wizard can also be used to “demote” a Domain Controller to a member Server