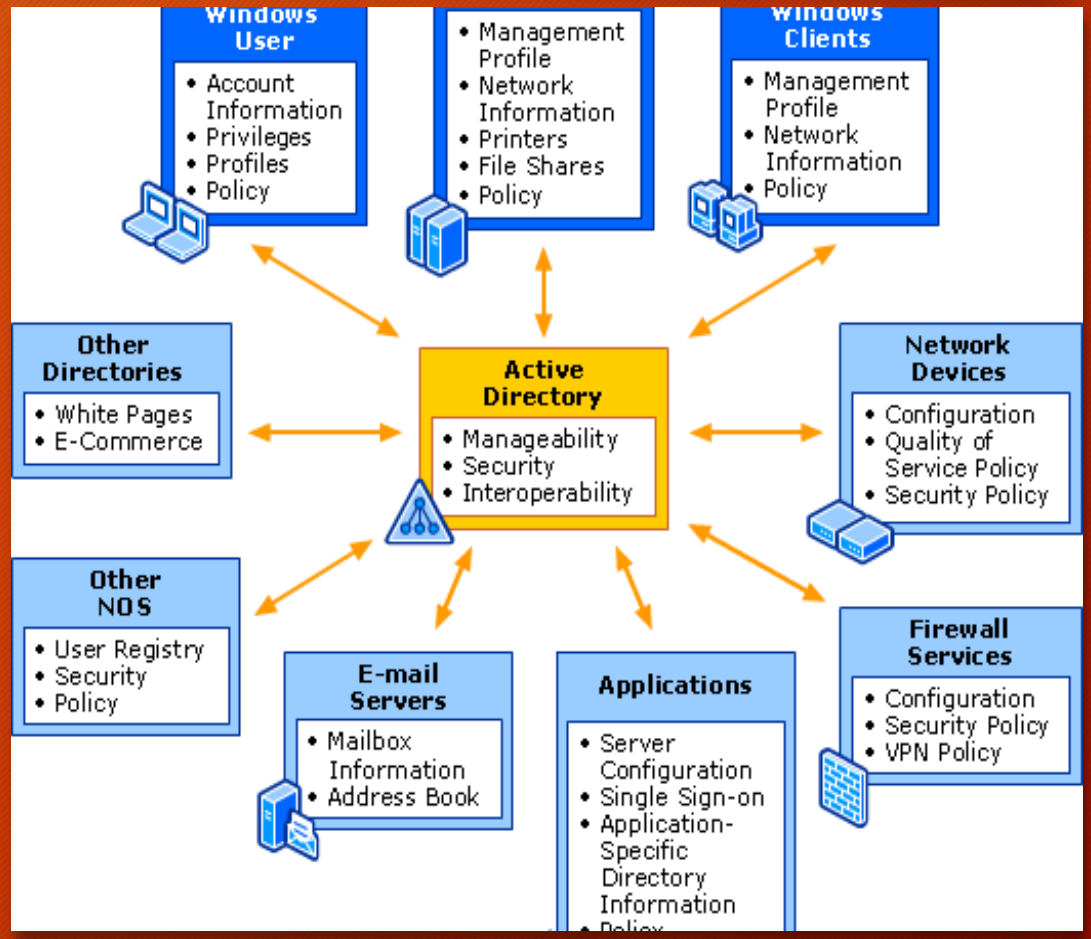
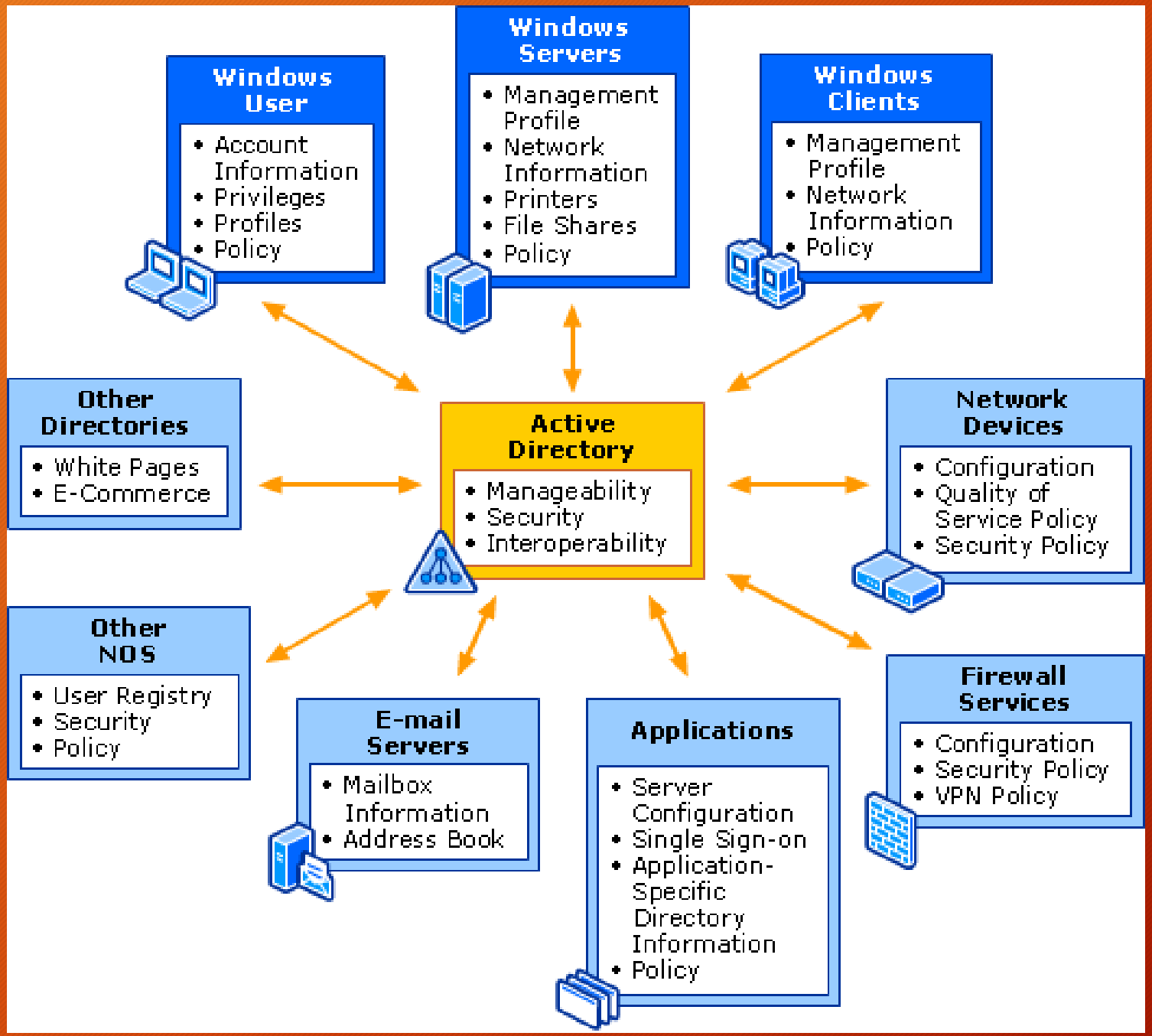
Active Directory Administration

By
Joseph Cheung

April 27, 2016




Windows User
• Account Information
• Privileges
• Profiles
• Policy
Windows Servers
• Management Profile
• Network Information
• Printers
• File Shares
• Policy
Windows Clients
• Management Profile
• Network Information
• Policy
Other Directories
• White Pages
• E-Commerce
Active Directory
• Manageability
• Security
• Interoperability
Network Devices
• Configuration
• Quality of Service Policy
• Security Policy
Other NOS
• User Registry
• Security
• Policy
E-mail Servers
• Mailbox Information
• Address Book
Applications
• Server Configuration
• Single Sign-on
• Application-Specific Directory Information
• Policy
Firewall Services
• Configuration
• Security Policy
• VPN Policy

Active Directory administration
By Joseph Cheung

Active Directory

- Overview
- Active Directory Structure
- Network Topology

CONCEPTS OF ACTIVE DIRECTORY

An active directory stores information about all the resources on a network; such as users, groups, computers, files, printers, and applications.

Plus

It provides all the services, making the information available and useful.

CONCEPTS OF ACTIVE DIRECTORY

Active directory stores information about resources in hierarchical structure

It contains objects that represents different types of network resources, users, printers and so on.

AD information is used to authenticate/authorize users, computers, resources which are part of a network

Object has attributes

Each object has

1. attributes,
   a. such as the user's first name, last name and email address; or
   b. A printer's asset number and location
2. GUID – 128bit global identifier
3. SID – Security identifier

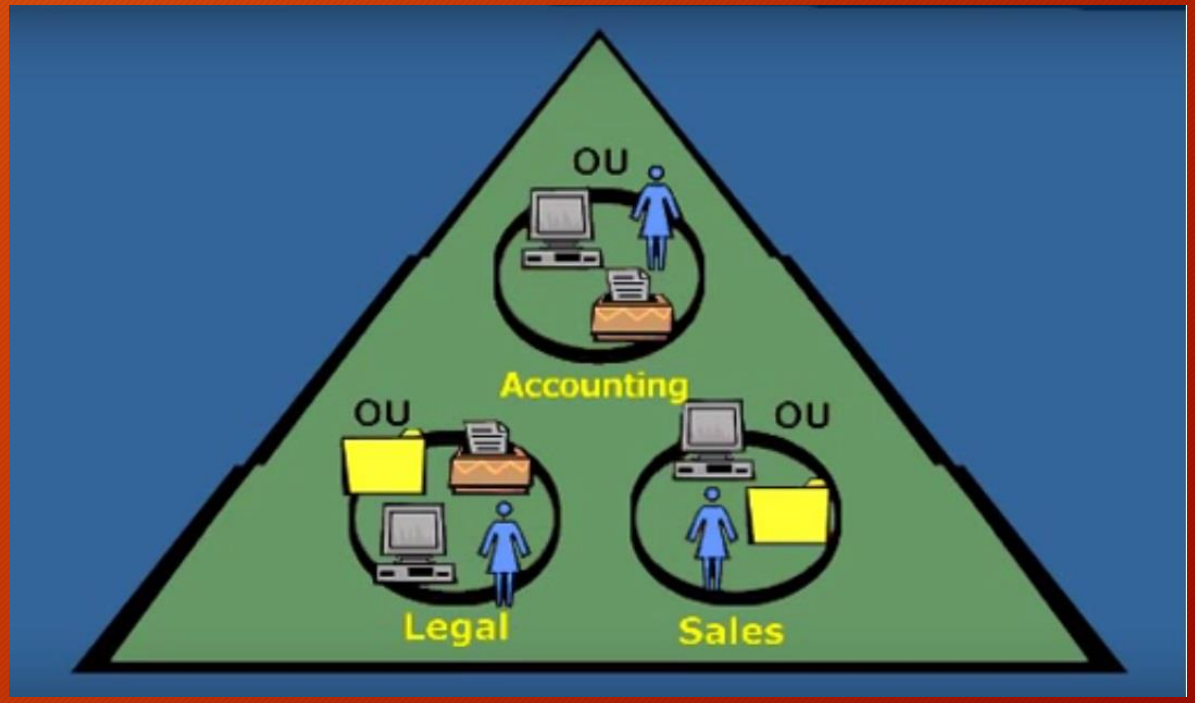
Object Examples

Forest	Computer
Domain	Shared Folder
Organizational Unit	Printer
User	Site
Group	Subnet
Contact	

STRUCTURE

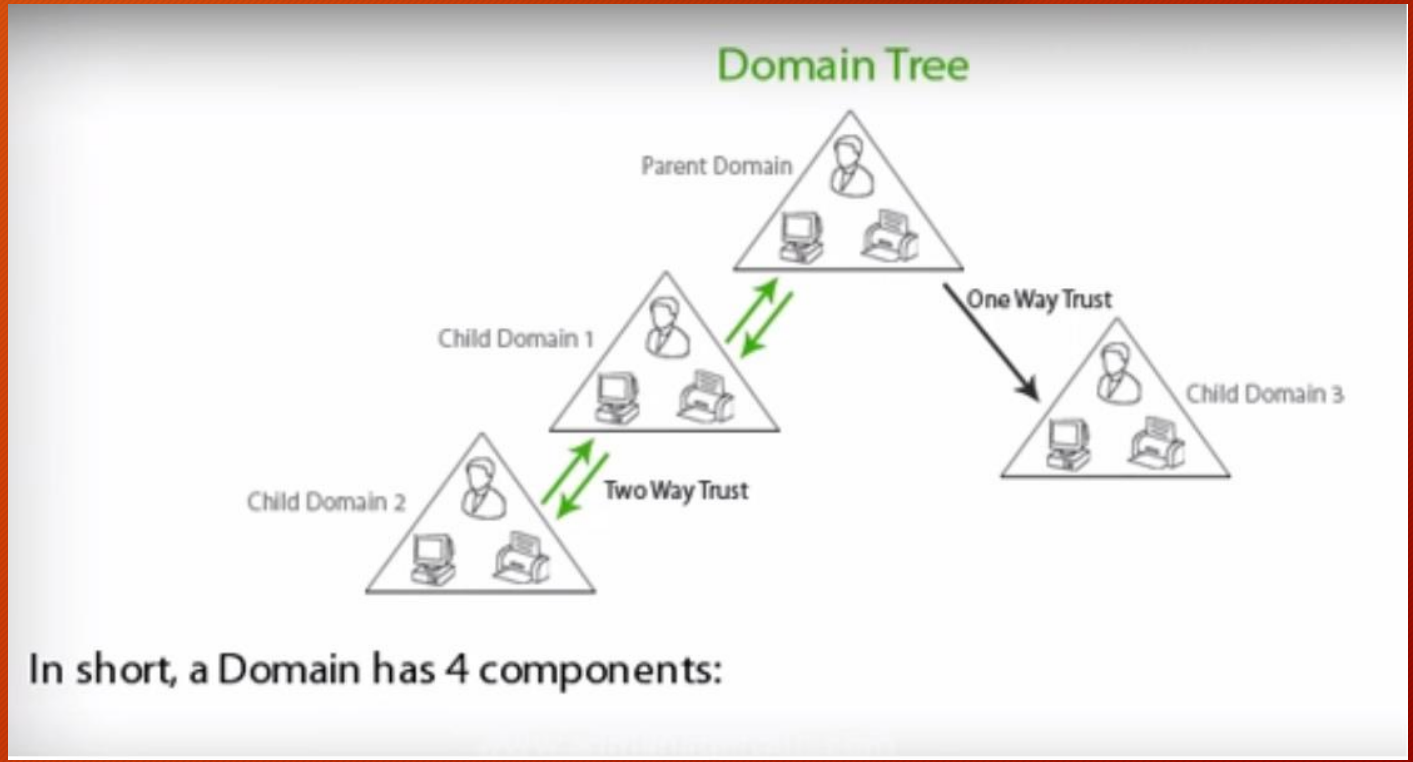
Objects are maintained in a domain

A domain is a basic unit of organization and security in active directory



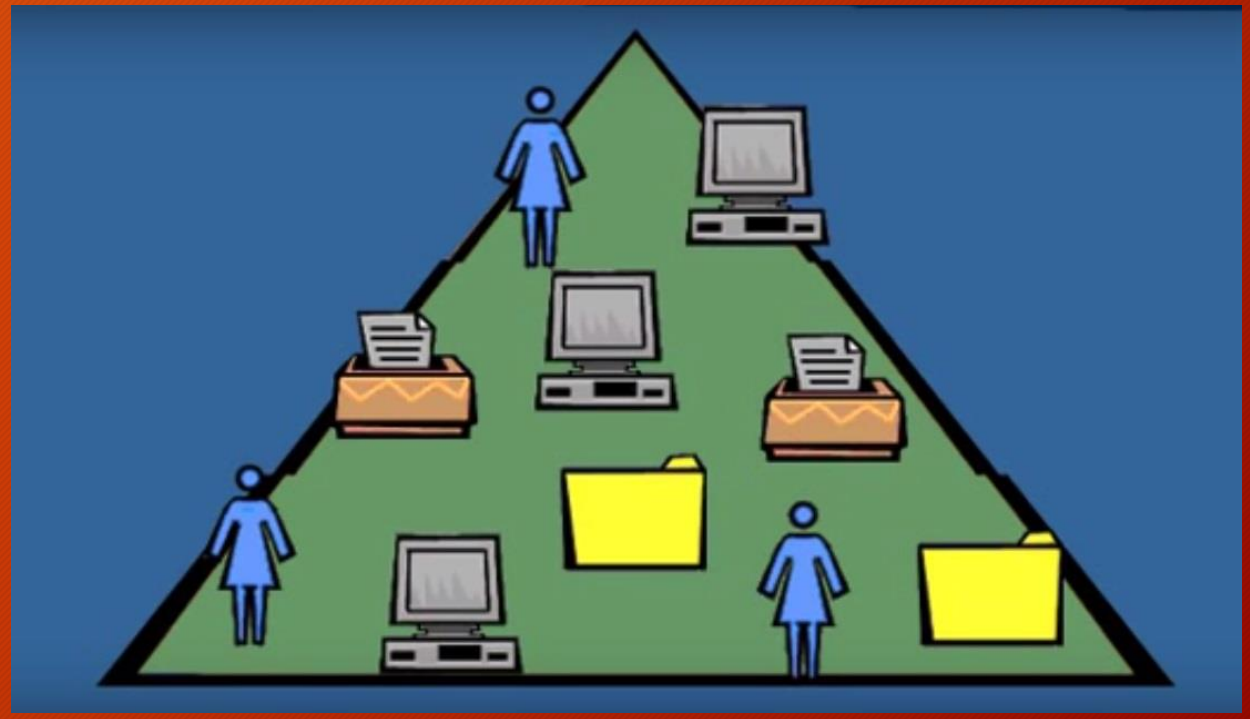
STRUCTURE
A Domain Has 4 Components

1. A hierarchical structure of containers, objects
2. An unique Domain Name
3. A security mechanism to authenticate and authorize access to Domain Resources
4. Policies that show how functionality is allowed or restricted for users, computers in a domain



STRUCTURE

Within a domain, objects can be organized into logical containers called organizational units or OUs



Organizational Unit [OU]

Using organizational unit you can create a hierarchical structure that duplicates the structure of your organization.

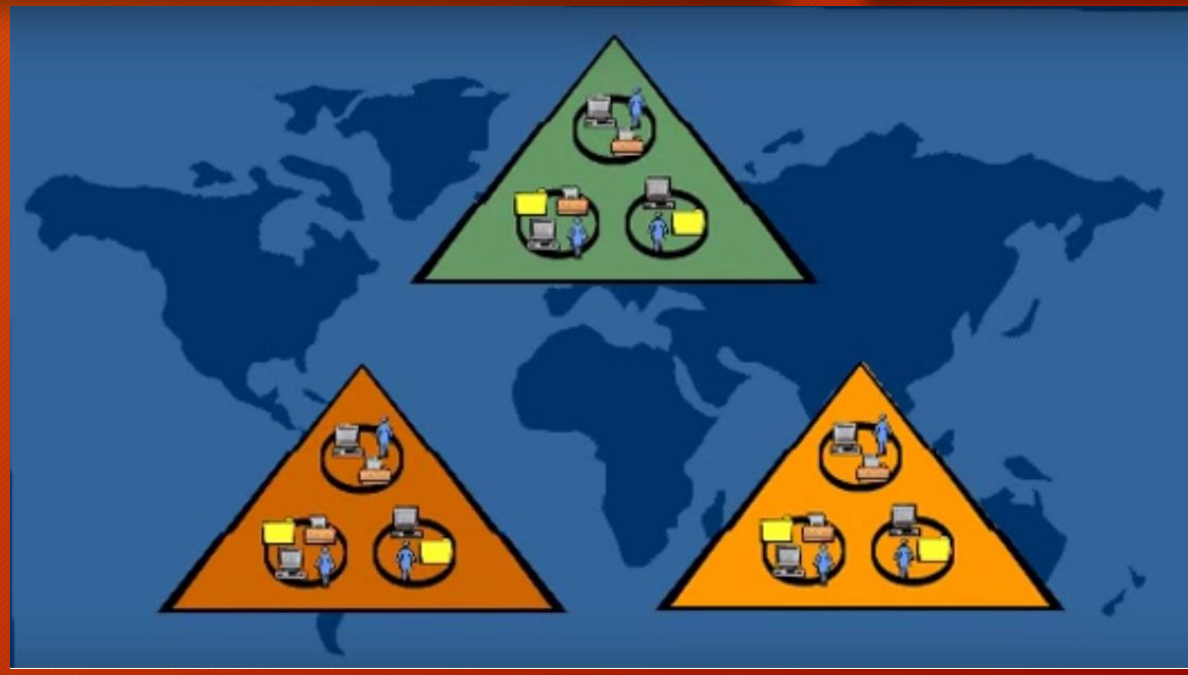
Even more importantly you can delegate some administrative responsibilities for these small units.

While administrators have full administrative rights for the entire domain. A user, such as a department or team manager can be granted rights for a particular sub-trees of organizational units or even a single organizational unit

Multiple Domain

Although organizational units are useful for delegating administrative responsibilities within a domain.

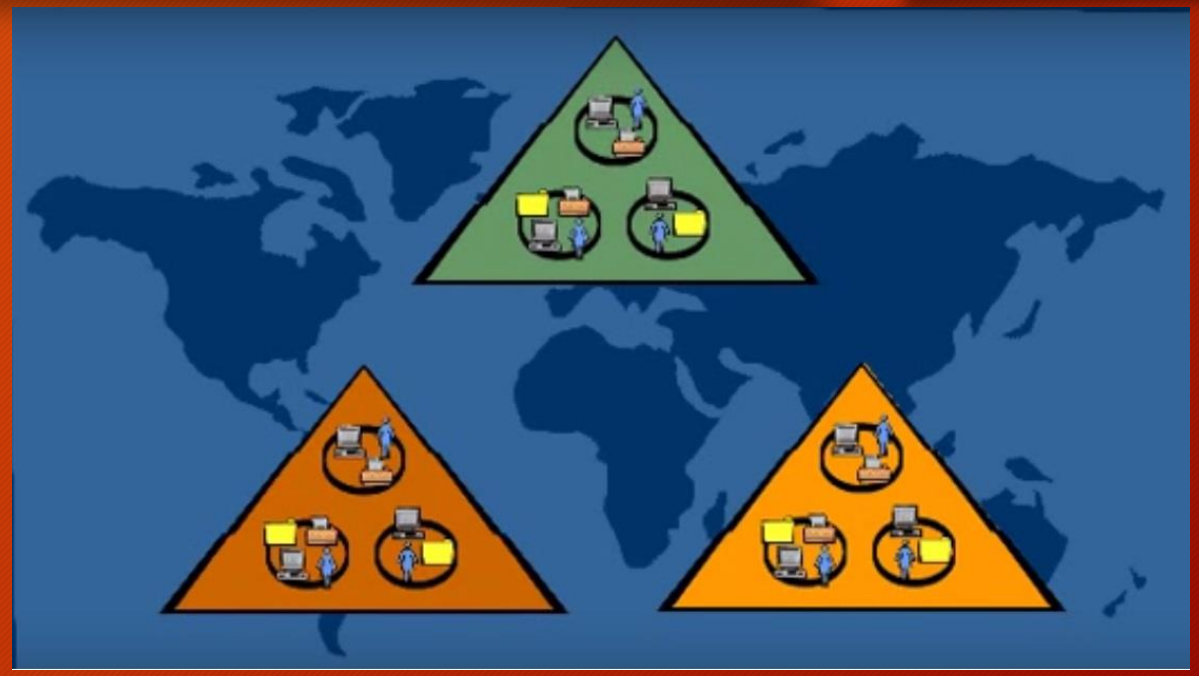
Multiple domains are useful for network administrations done by separate authorities, such as in an international organization where resources maybe maintained in different languages



Multiple Domain

Multiple domains can form a domain tree; the root domain is always created first

It becomes the parent domain to child-domains that are added directly below it



DNS

Each domain in a tree is assigned a name using the hierarchical domain naming system or DNS

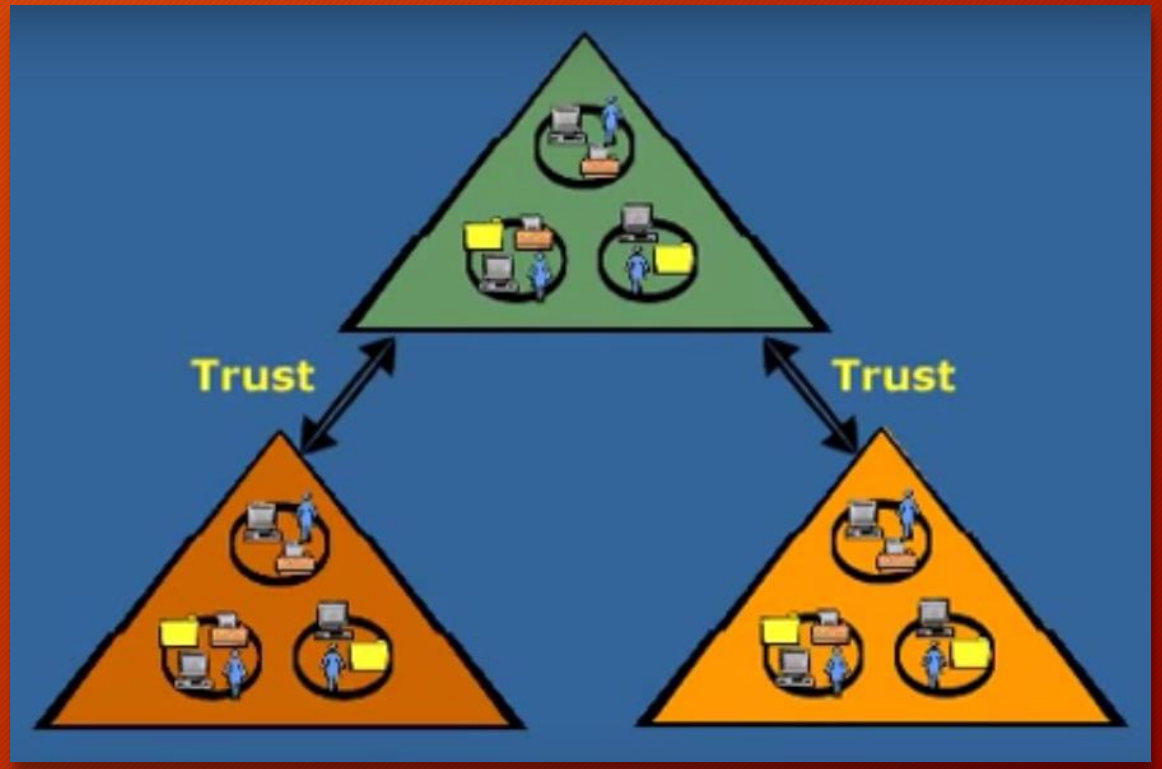
As other domains are joint to a tree, the name of a child is added to the parents name, reflecting their relationship

To make network resources globally available to users, by default, active directory transparently joint domains to a 2-way transitive relationship

TRUST RELATIONSHIPS

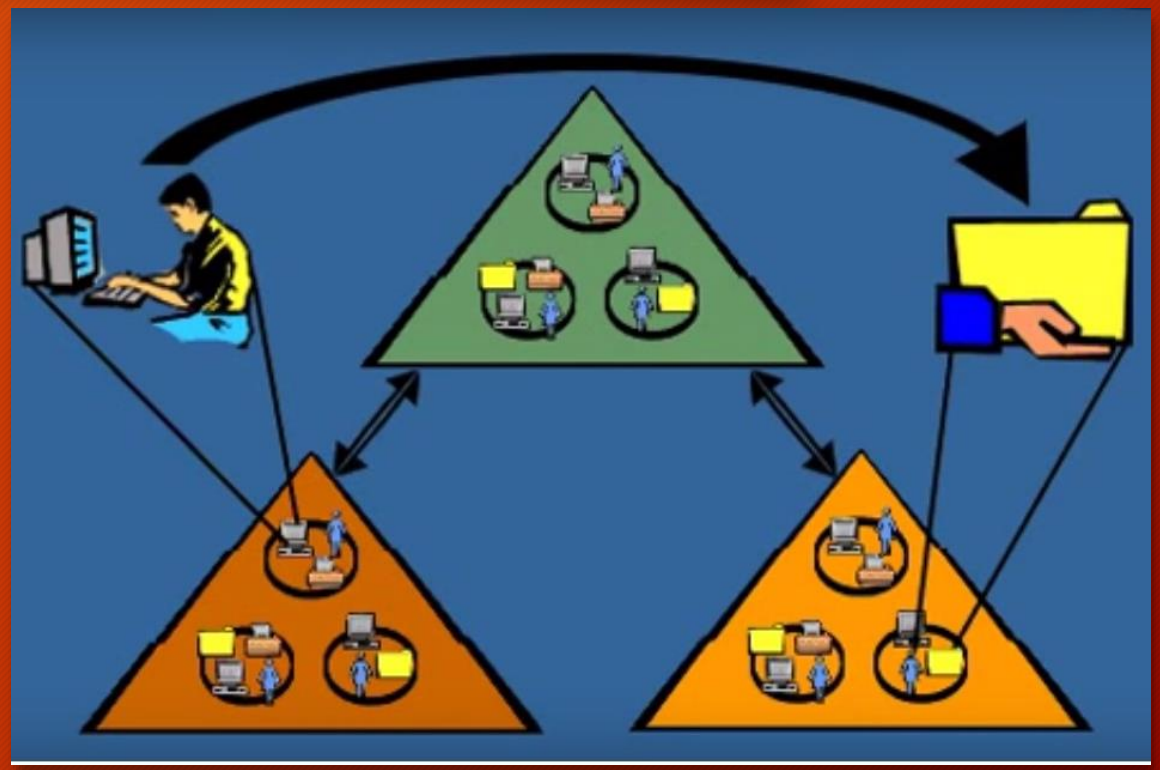
Trust relationship make the domain resources available to users in other domains.

Transitive means that the trust relationship carry thru automatically to other domains in the tree



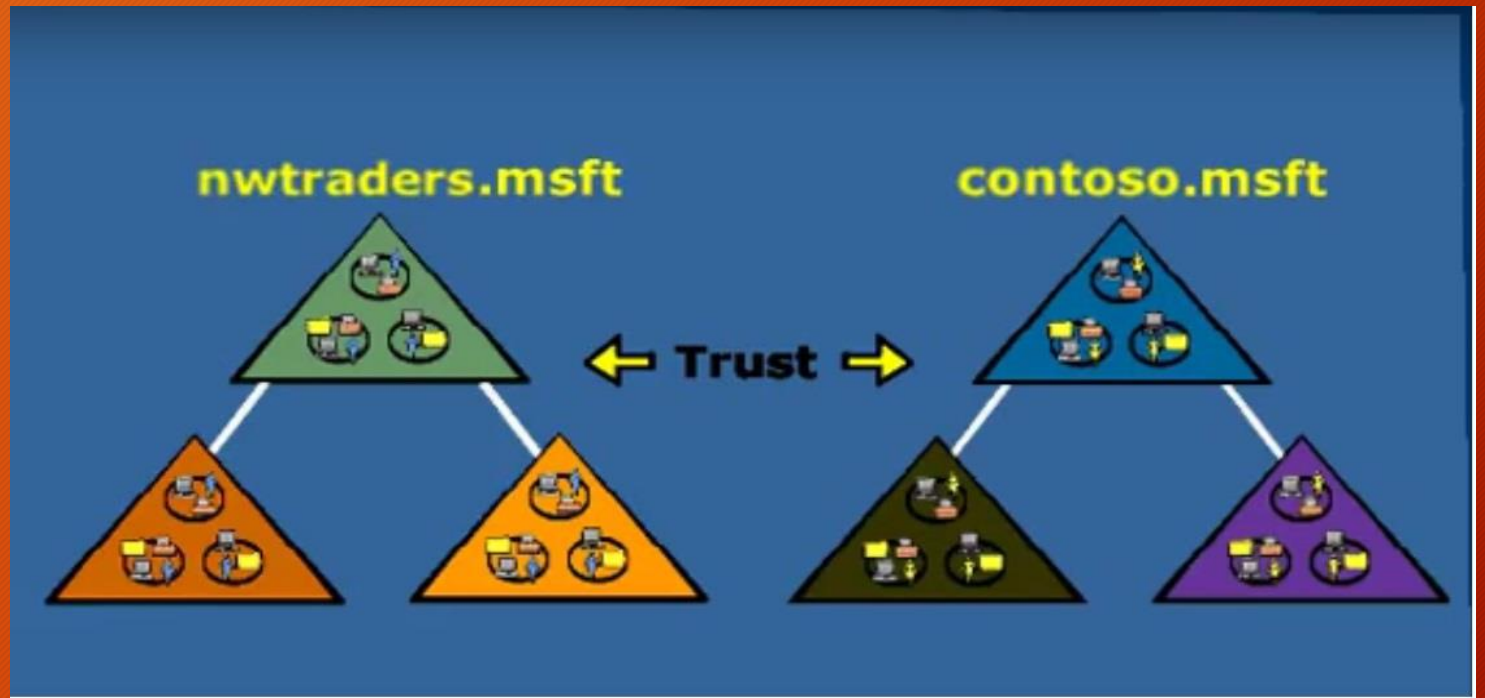
TRUST RELATIONSHIPS

So, users in one domain may have access to resources anywhere in the tree; except of course to resources that have been restricted.



TRUST RELATIONSHIPS

- The tree model of multiple domains can be extended to a forest of trees.
- Or organizations who need to maintain a separate organizational structures, such as a company that needs distinct public identities for its subsidiaries.



TREES IN A FOREST SHARE

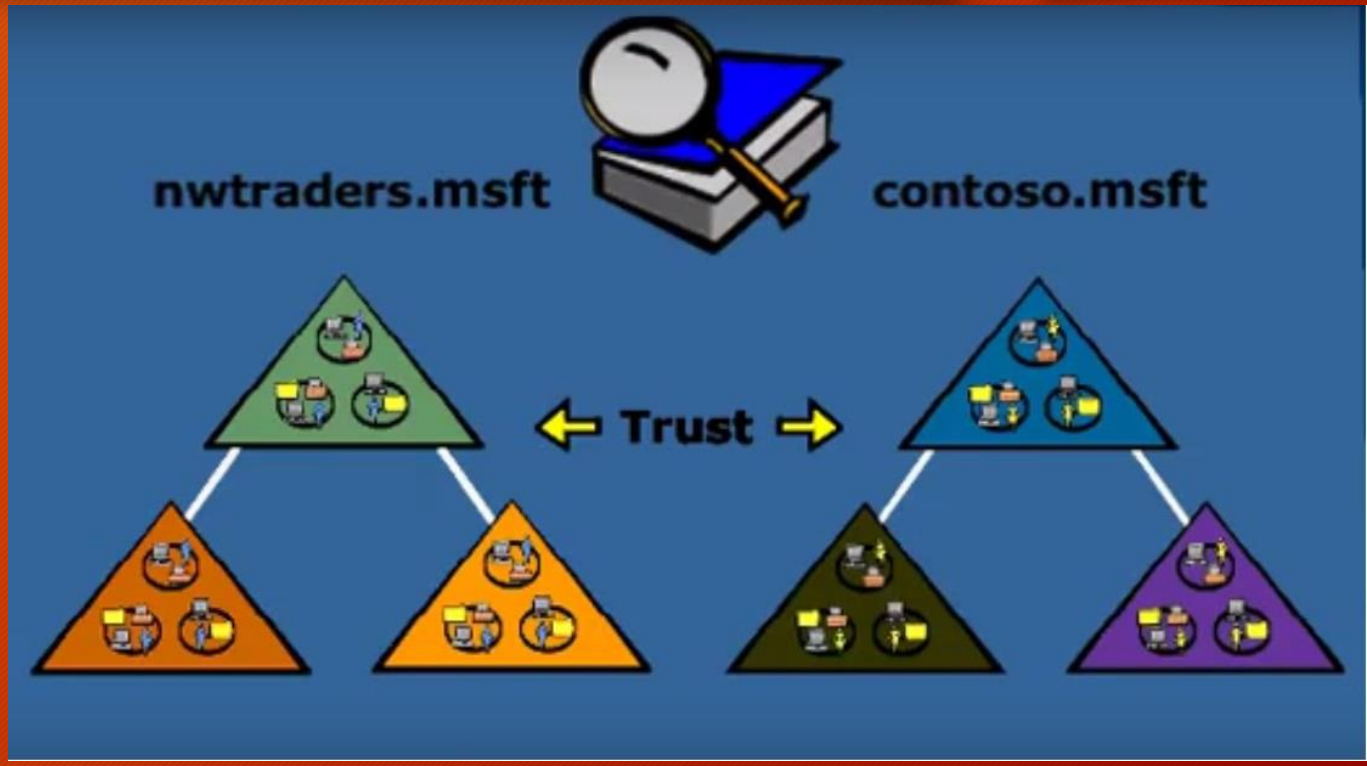
Although each tree can have different naming scheme, they share 3 things

- Transitive trust relationships between any domain within the forest
- A common schema - a complete set of object types; and
- They share a comprehensive global catalog

Global Catalog

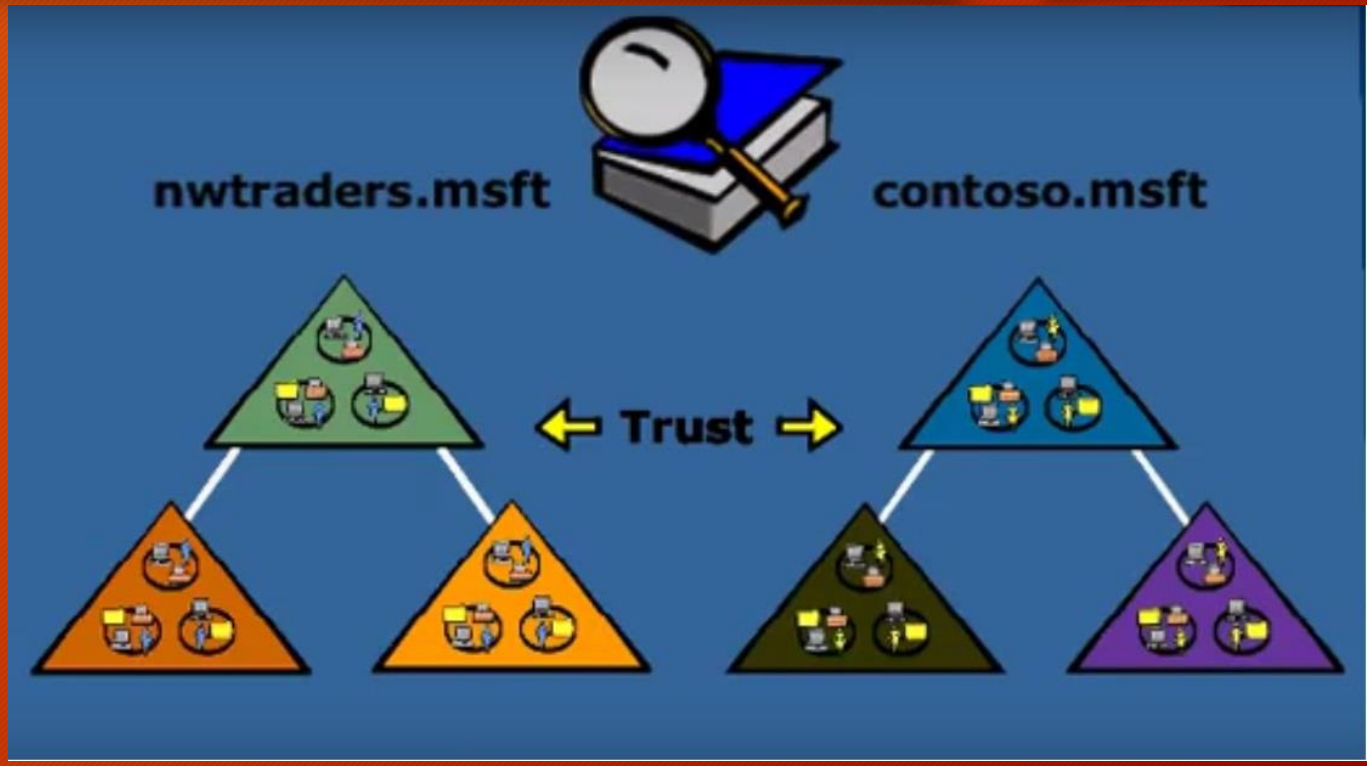
The global catalog holds all the objects for all domains, so it's easy for users to locate a specific object anywhere in the Enterprise.

To keep query response time fast, the global catalog maintains only a sub-set of attributes for each object.



Global Catalog

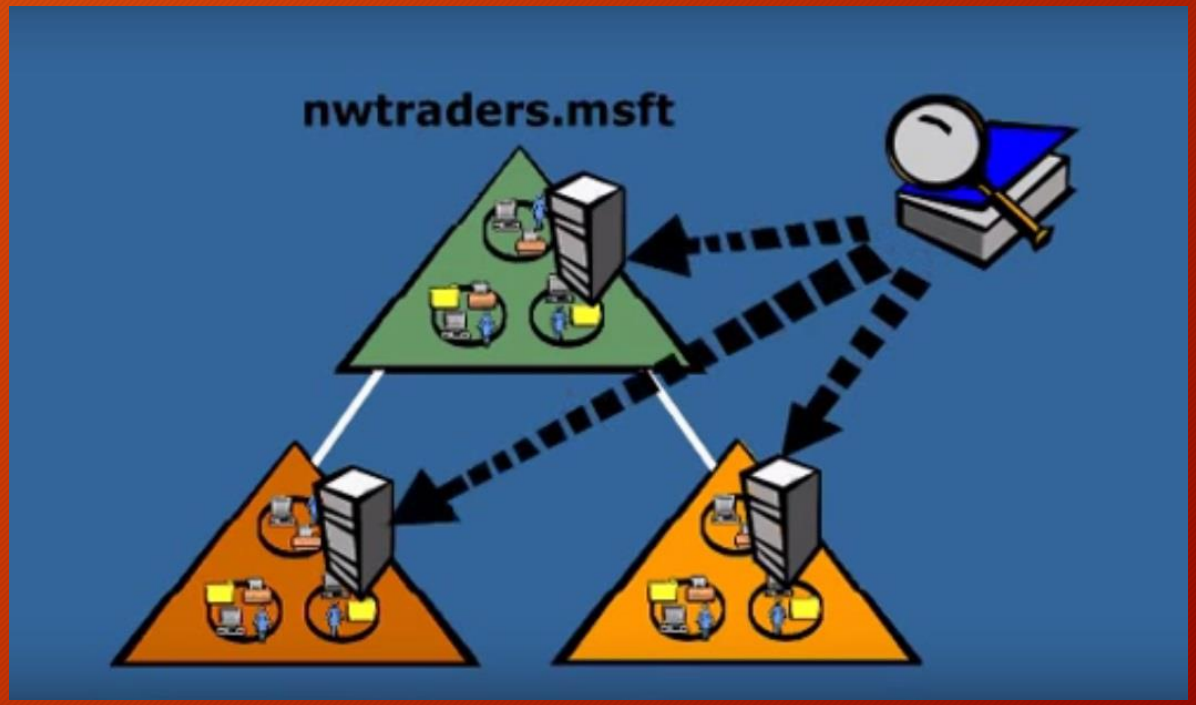
The global catalog is automatically replicated to those domain controllers throughout the forest that are designated as global catalog service



Global Catalog

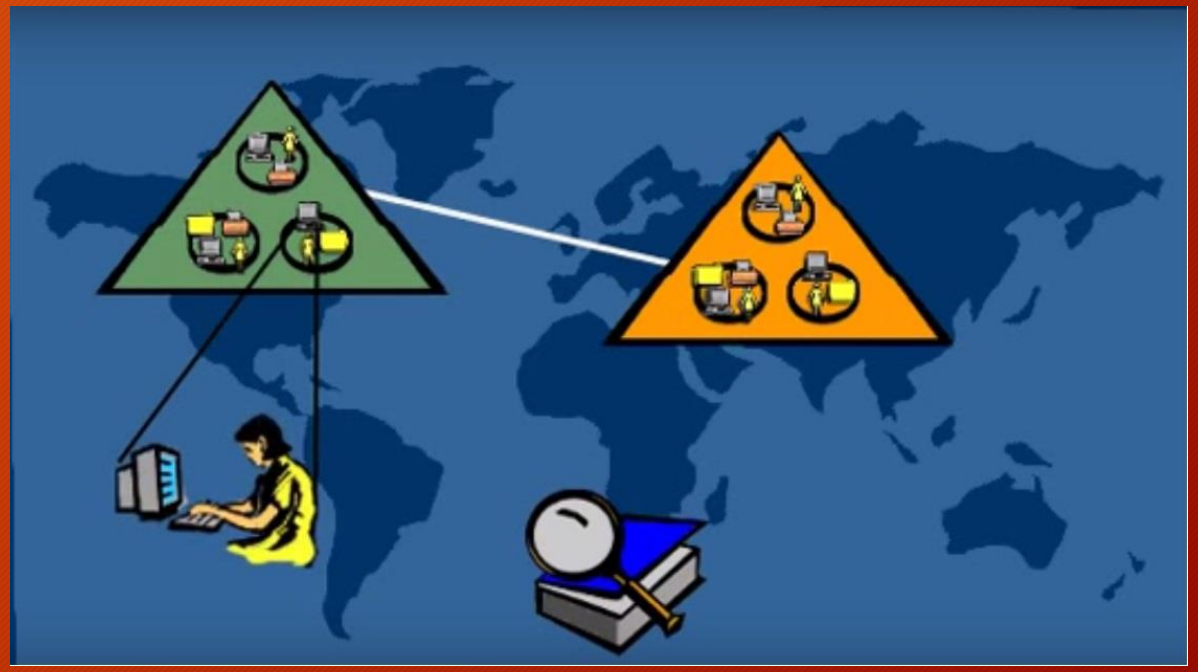
DOMAIN CONTROLLER

1. manages ACTIVE DIRECTORY information and users interactions, including directory searches across the enterprise;
2. Is responsible for all the authentications, authorizations, additions, deletions, audits, modifications, inside a Domain.



Global Catalog

For example if the marketing manager in the Minneapolis's office wants to send a hard copy of the file out to the subsidiary in Paris, she can query the ACTIVE DIRECTORY global catalog for a printer on the 2nd floor office of Rue Lafayette, the global catalog resolves the query and returns the location



ACTIVE DIRECTORY - Network Topology

- Finally, let's look how AD relates to network topology
- To optimize active directory performance it may be beneficial to divide the network into sites, especially it has geographic separate locations connected by slow links

SITES

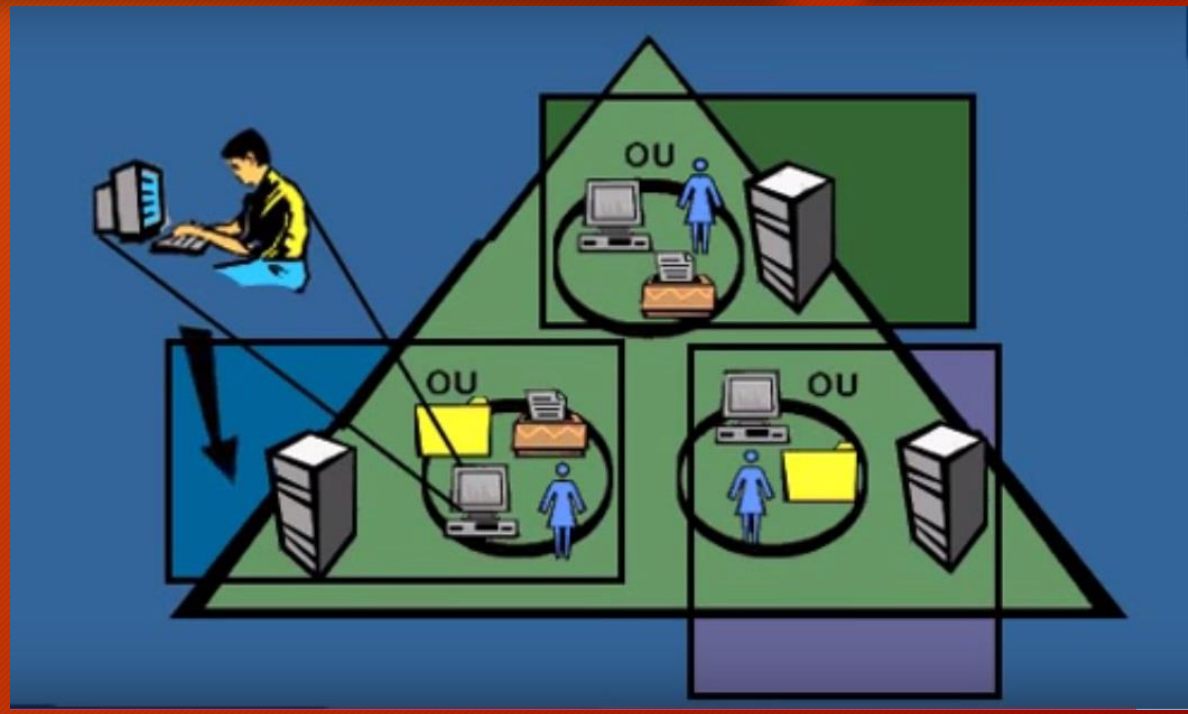
A site is one or more IP subnets connected by a hi-speed link.

Sites help reduce active directory traffic, such as work stations logged-on in replication

For example when a user who logs on win2012 will try to find the active directory controller in the same site of the user's computer to validate the logon request.

SITES

Staying within the same site serve to reduce unnecessary traffic between the domain controllers; and the network operates more efficiently



SITES

In addition, replication of active directory between sites can be scheduled in off-peak hours when demand for resources between sites is usually lower

ACTIVE DIRECTORY - conclusion

Active directory enable users to access resources and

The administrators to secure the resources across the enterprise network.

Active Directory Administration

28

Thank You

By
Joseph Cheung

April 27, 2016