Understanding Active Directory

S. Vaidyanathan

Agenda

Introduction to Active Directory Domain Services

AD Logical Concepts

AD Physical Concepts

DNS

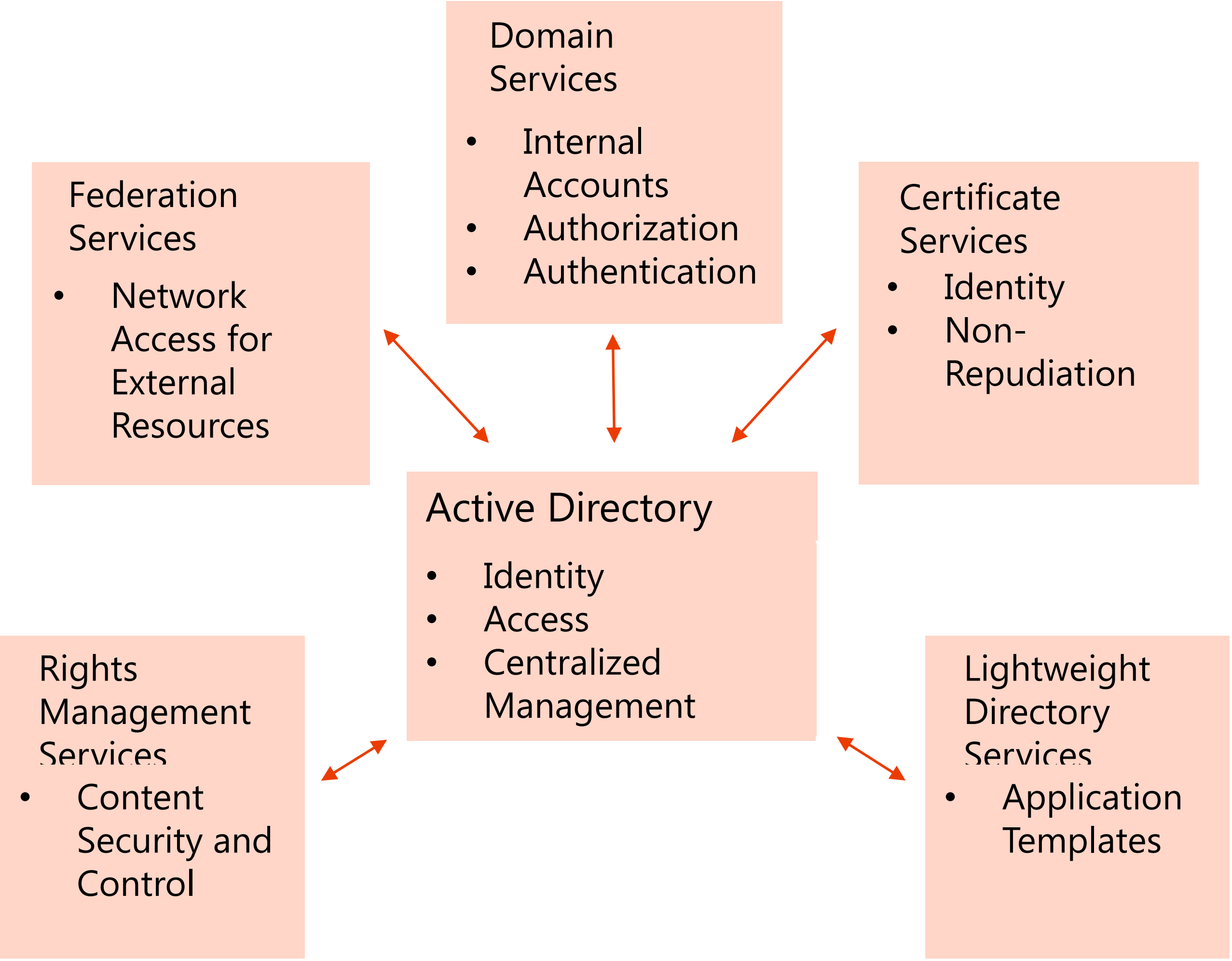
Replication

Operations Masters

Active Directory Domain Services

What is Active Directory

- What is Active Directory?
  - A collection of services (Server Roles and Features) used to manage identity and access for and to resources on a network



Domain Services

- Internal Accounts
- Authorization
- Authentication

Federation Services

- Network Access for External Resources

Certificate Services

- Identity
- Non-Repudiation

Active Directory

- Identity
- Access
- Centralized Management

Rights Management Services

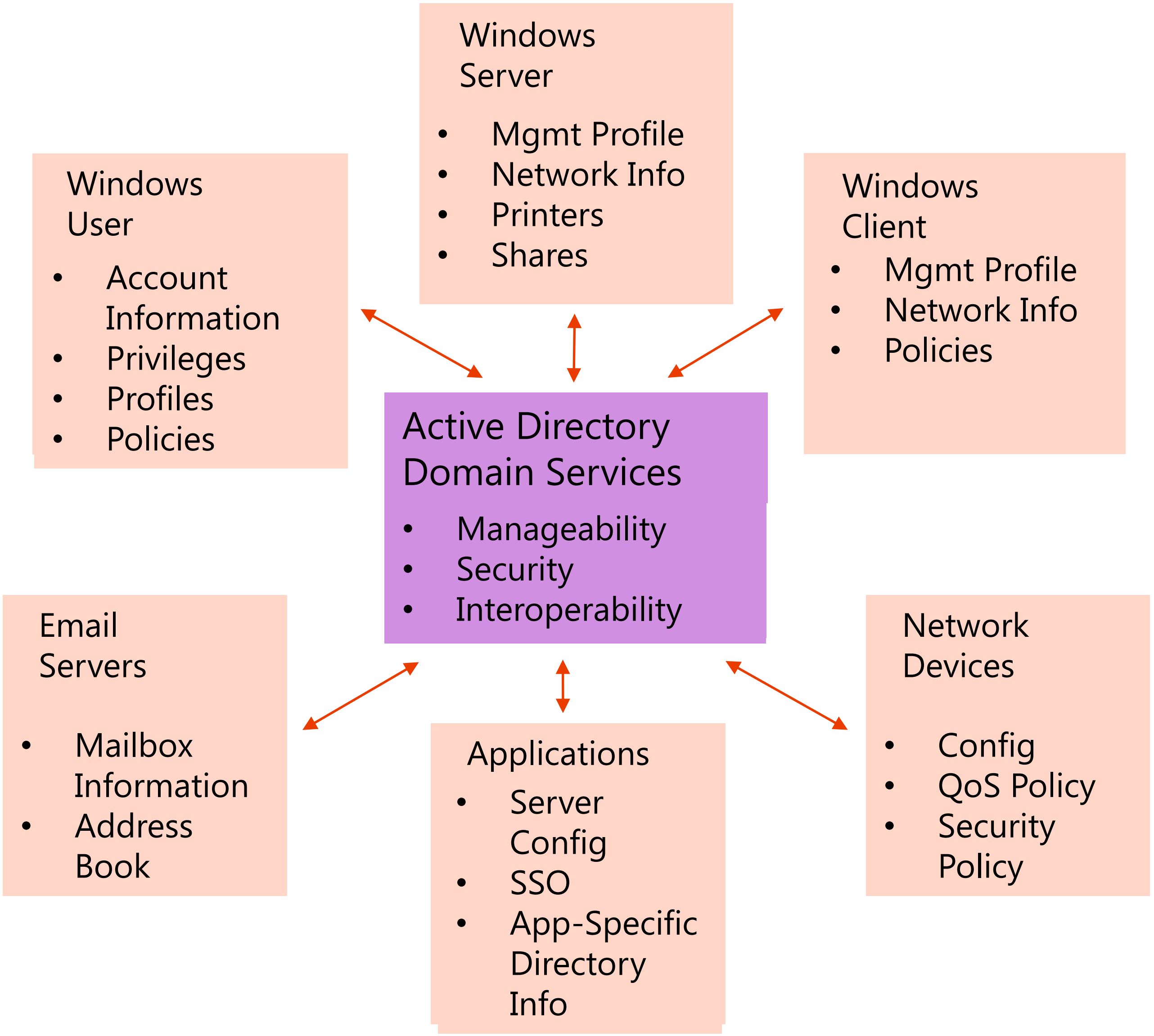
- Content Security and Control

Lightweight Directory Services

- Application Templates

What is AD DS?

- What is Active Directory Domain Services?
  - A directory service is both the directory information source and the service that makes the information available and usable
  - A phone book…



Windows Server

- Mgmt Profile
- Network Info
- Printers
- Shares

Windows User

- Account Information
- Privileges
- Profiles
- Policies

Windows Client

- Mgmt Profile
- Network Info
- Policies

Active Directory Domain Services

- Manageability
- Security
- Interoperability

Email Servers

- Mailbox Information
- Address Book

Applications

- Server Config
- SSO
- App-Specific Directory Info

Network Devices

- Config
- QoS Policy
- Security Policy

What does AD DS do?

- Scalable, secure, and manageable infrastructure for user and resource management
  - stores and manages information about network resources
  - provides support for directory-enabled applications such as Microsoft® Exchange Server
  - allows for centralized management

What does AD DS do?

AD DS provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network, such as users, computers, and other devices, into a hierarchical containment structure. The hierarchical containment structure includes the AD DS forest, domains in the forest, and organizational units (OUs) in each domain. A server that is running AD DS is called a domain controller.

What does AD DS do?

Organizing network elements into a hierarchical containment structure provides the following benefits:

- The forest acts as a security boundary for an organization and defines the scope of authority for administrators. By default, a forest contains a single domain, which is known as the forest root domain.
- Additional domains can be created in the forest to provide partitioning of AD DS data, which enables organizations to replicate data only where it is needed. This makes it possible for AD DS to scale globally over a network that has limited available bandwidth. An AD DS domain also supports a number of other core functions that are related to administration, including network-wide user identity, authentication, and trust relationships.

OUs simplify the delegation of authority to facilitate the management of large numbers of objects. Through delegation, owners can transfer full or limited authority over objects to other users or groups. Delegation is important because it helps to distribute the management of large numbers of objects to a number of people who are trusted to perform management tasks.

Active Directory – Logical Concepts

Domains

Forest

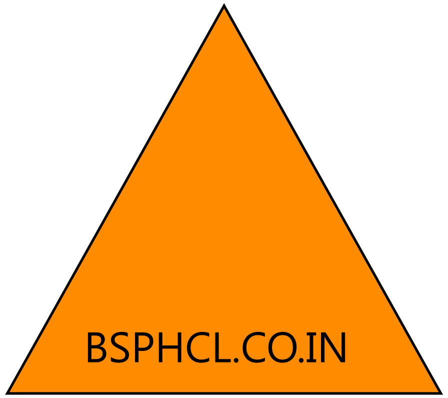
Trees

Organisational Unit

Active Directory Logical Concepts

Domains

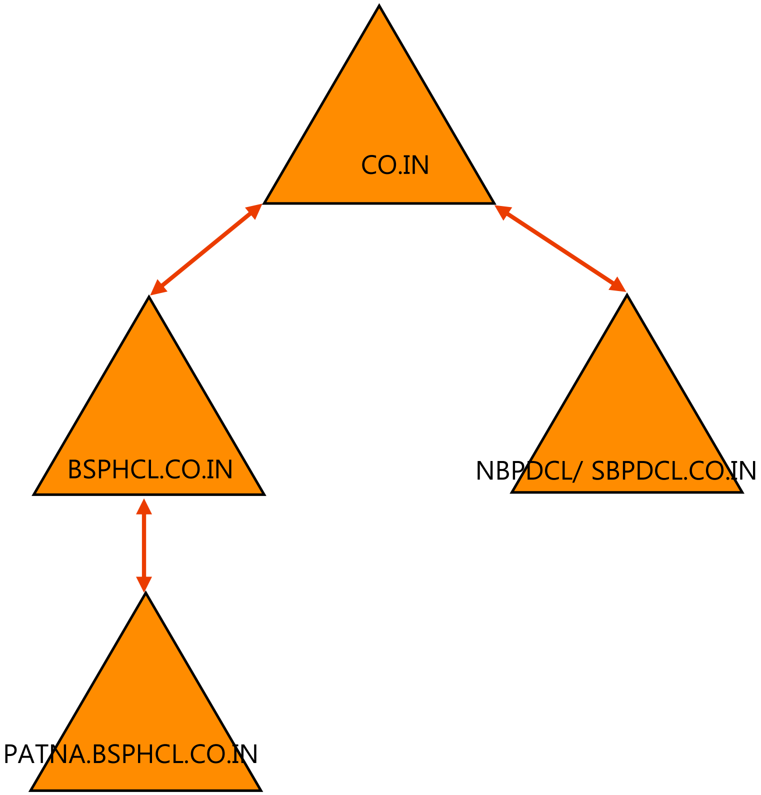
- Boundary of Security
  - Authentication
  - Security Policies
- Boundary of Replication
  - Domain NC Replication
- Boundary of DNS Namespace
- Boundary of Administration



Active Directory Logical Concepts

Trees

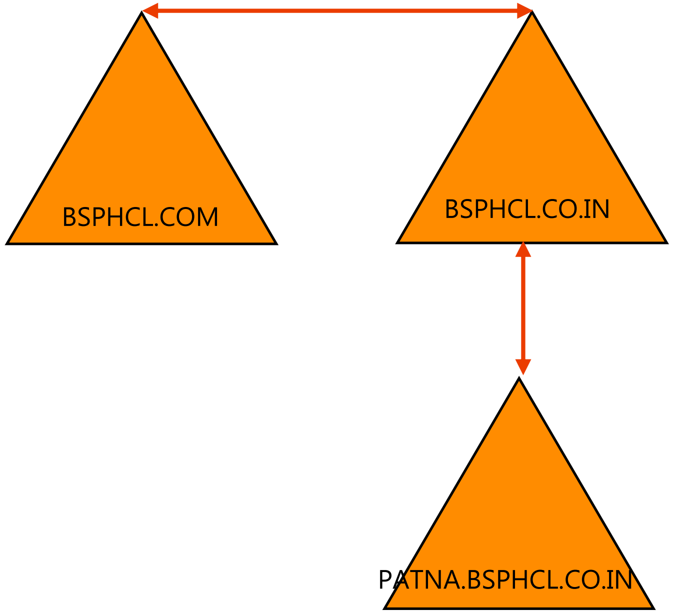
- Hierarchy of Domains forming a contiguous namespace
- Transitive Trust Relationships
- All Domains in a Tree share:
  - Schema
  - Configuration
  - Global Catalog



Active Directory Logical Concepts

Forests

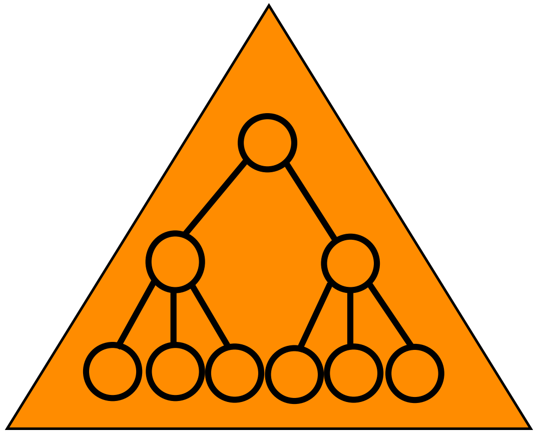
- Hierarchy of Domains forming a contiguous or disjoint namespace
- Transitive Trust Relationships
- All Domains in a Forest share:
  - Schema
  - Configuration
  - Global Catalog



Active Directory Logical Concepts

Organizational Units

- Containers within Domains
- Distinct Units of Administration
- Unique to Domains



Active Directory – Physical Concepts

Domain Controllers

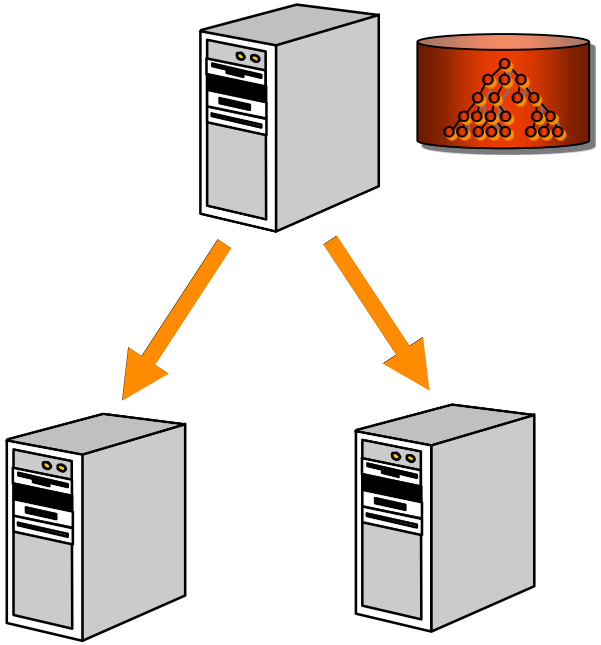
Sites

Global Catalog

Active Directory Physical Concepts

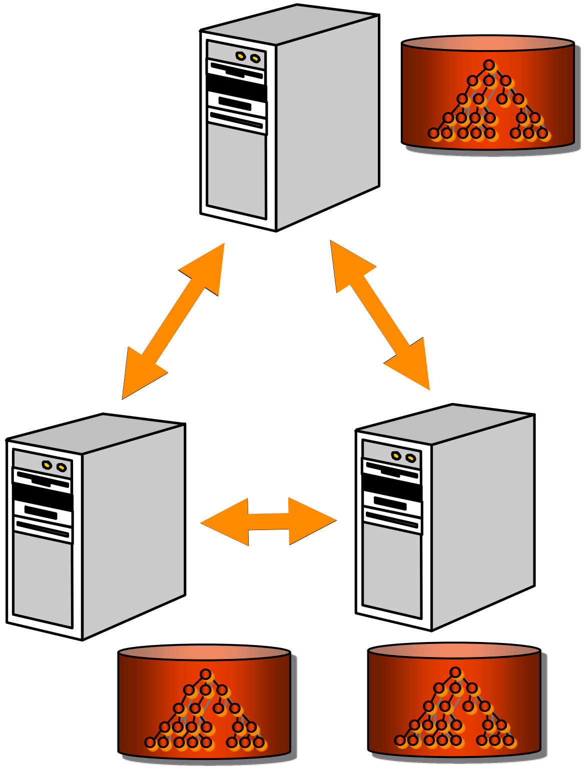
Domain Controllers

Primary Domain Controller (PDC)



Backup Domain Controllers (BDCs)

Domain Controllers (DCs)



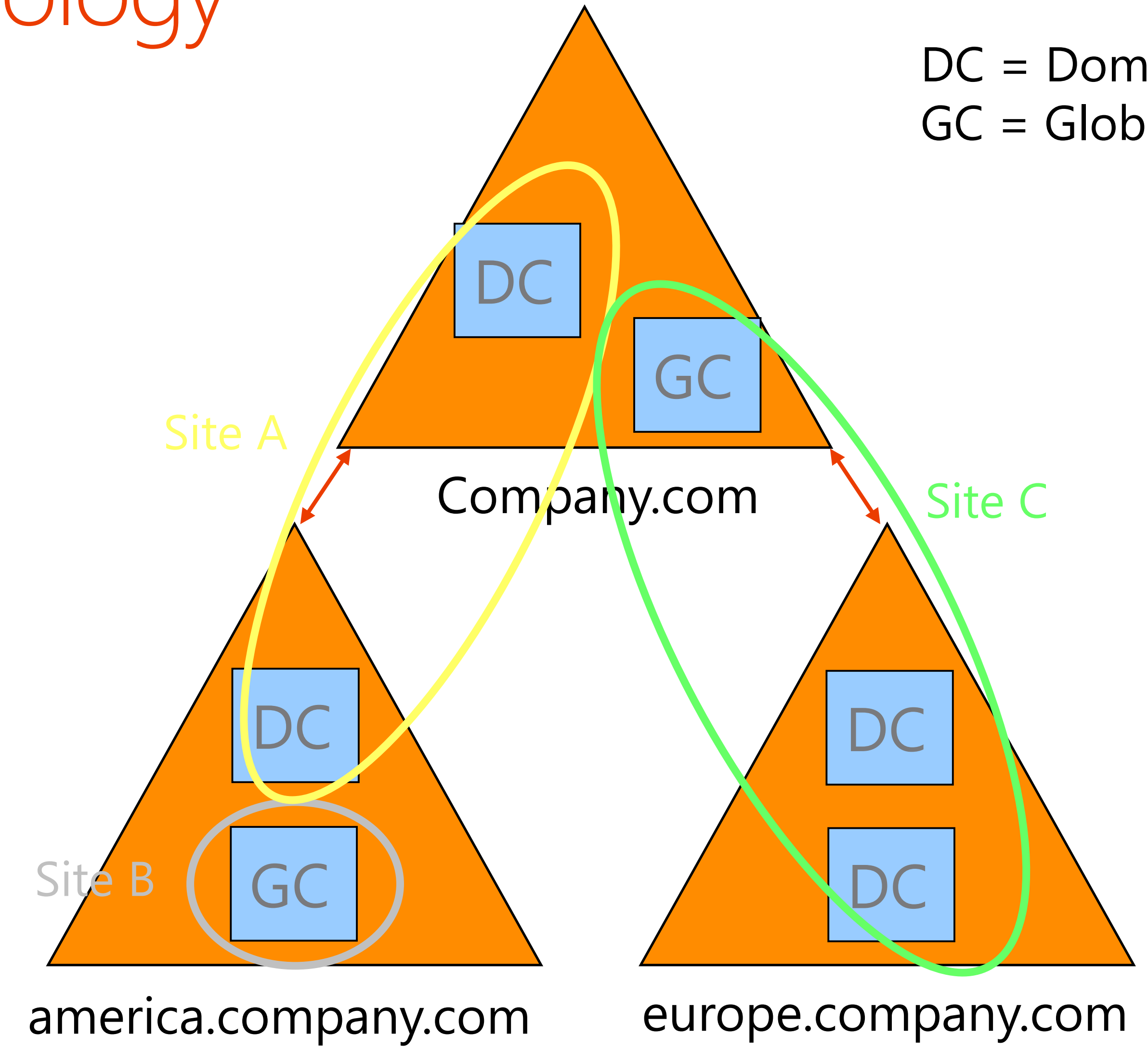
Active Directory Physical Concepts

Sites

- What is a Site?
  - A set of well-connected IP subnets
- Site Usage
  - Locating Services (e.g. Logon, DFS)
  - Replication
  - Group Policy Application
- Sites are connected with Site Links
  - Connects two or more sites

Active Directory Physical Concepts

Site Topology



DC = Domain Controller
GC = Global Catalog

Active Directory Physical Concepts

Global Catalog

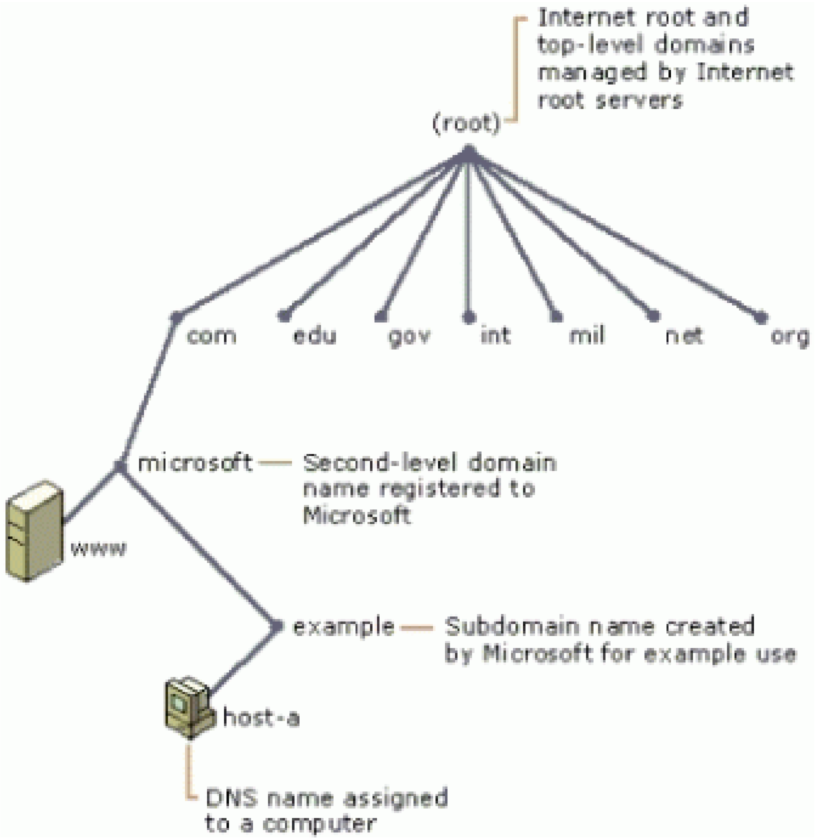
- Partial Replica of all Objects in the Forest
- Configurable subset of Attributes
- Fast Forest-wide searches
- Required at Logon for Universal Group Membership

DNS
Domain Name System

- DNS is a globally distributed database that manages IP addresses on the internet.
- DNS uses a hierarchy of domains on the internet.
  - Top level domains use the familiar names like .com, .edu, .gov.
  - The second level are registered to organizations who have a presence on the web.

Active Directory is designed to exist within the scope of the Global DNS Namespace.

DNS Structure


Internet root and top-level domains managed by Internet root servers
(root)
com
edu
gov
int
mil
net
org
microsoft
Second-level domain name registered to Microsoft
www
example
Subdomain name created by Microsoft for example use
host-a
DNS name assigned to a computer

What is DNS?

- Internet Protocol
- Distributed database
- Maps hierarchically organized keys to values
  - E.g. host name to IP address
  - Mailer records
- Name space
- Developed to replace hosts file

DNS Namespace

- Hierarchical tree of domains
  - Root
  - Top level domains (gov, edu, com, fr, se, uk etc.)
  - Some countries have subdomains denoting organisation type (e.g. ac.uk, co.uk)
  - Subdomains generally for specific organisations (e.g. mit.edu, microsoft.com etc.)
  - Subdomains within organisation (e.g. oucs.ox.ac.uk)
- Technically, a domain is the part of the name space at or below the domain name identifying the domain.

Delegation of Responsibility

- Vital to understand this concept
- DNS Database is distributed
  - No one server is responsible for the whole namespace
- Given name server is responsible for part of the namespace
  - Called a zone
  - Server is "authoritative" for the zone

Delegation of Authority

- Authority is delegated from the top down
- Cannot simply set up a name server for a domain and expect clients to resolve names correctly
  - Will not work
- Name servers for parent domain must know that authority has been delegated to new domain
- E.g. if new ac.uk domain xxx.ac.uk is created, name servers for ac.uk must be configured with information about name servers responsible for new domain

DNS Queries

- Client queries DNS Server
- DNS Server
  - Checks its cache
  - Checks whether it contains the information in its own zone files
  - Queries other name servers iteratively
  - Returns an answer

Iterative Queries

- Example — client queries name server for IP address of fred.test.com

1. Sends query to root name servers
2. Root name servers refer to name servers authoritative for com domain
3. Queries com domain name servers
4. com name servers refer to name servers authoritative for test.com domain
5. Queries test.com domain name servers
6. test.com name returns answer
7. Name server returns answer to client

Root hints and Forwarders

- Root hints table provides IP addresses of name servers for root domain
    - Starting point for iterative queries
- DNS server can be configured as forwarder
    - Queries for information about which it is not authoritative forwarded to other name servers (forwarders)

Zones

- Zone may contain a domain or part of a domain
- A name server may be authoritative for more than one zone
- Should be a minimum of two name servers for a zone (resilience)
  - One server is primary
    - “Start of authority” for zone
  - Others are secondaries
  - Updates to primary are replicated to secondaries (zone transfer)
- Subsidiary zones can be delegated to other name servers

DNS Records

- A — host name to IP address mapping
- NS — name server
- MX — mailer exchange
- SOA — start of authority
- CNAME — canonical name (alias)
- PTR — pointer (IP address to host)
- SRV — service resource record (2000)
- …and others

Active Directory and the DNS

- Active Directory requires DNS
  - Used to locate services
    - E.g. client locating domain controller
    - Domain controller locating replication partners
- Active Directory requires SRV record support
- Active Directory prefers dynamic registration (DDNS)

How does AD use the DNS

- A 2000 system will attempt to register its A record in the DNS
- Domain controllers will attempt to register around 20 SRV records in the DNS
- Things will break if the correct records for DCs are not in the DNS

Active Directory – Replication

Naming contexts

Replication Topologies

Site Links, Bridges

Replication

Replication Details

- Naming Contexts (NCs)that are replicated
    - Schema Naming Context
    - Configuration Naming Context
    - Domain Naming Context
- Multi-master Replication
- Intra-site Bi-directional Ring Topology
- Inter-site Spanning Tree Topology
    - Synchronous RPC over TCP/IP
    - Asynchronous SMTP

Replication

Naming Contexts

- Schema
  - Definitions of object classes and attributes
  - Replicated to all DCs in the forest
- Configuration
  - AD Structure (domains, sites, and where the DCs are)
  - Replicated to all DCs in the forest
- Domain
  - Domain specific objects (users, groups, computers, and OUs)
  - Replicated to all DCs in a domain

Replication

Replication Topologies

- Intra-site Replication: AD replication between DCs within a Site
- Inter-site Replication: AD replication between Sites

Replication

Intra-site Replication

- RPC replication within a Site
- No compression
  - Assumes good network connections
- Uses notification process
  - 5 minutes -2k
  - Less – 2k3
- KCC generates a bi-directional Ring with extra edges

Tip: Always let KCC generate the intra-site replication topology when possible

Replication

Inter-Site Replication

- Replication between Sites
- DS-RPC (RPC over IP) or SMTP Transports
- SMTP can be used only between
  - **GCs across Sites**
  - **DCs of different domains and in different sites**
- Compression
  - 10%-20% of original size
- Scheduled

Replication

Site-links, Bridges and Bridgehead Servers

- Site-links link two or more sites
  - Costs and schedules can be specified
  - Transitive (can be disabled)
- Site-link Bridges
  - Bridge two or more site-links
- Bridgehead servers
- KCC generates a minimum cost spanning tree

Tip: Always let KCC generate the replication topology

Active Directory – Operations Masters

Overview

- Active Directory updates generally multimaster
    - Changes can be made on any DC
- Some exceptions — single master
    - Sometimes better to prevent conflict than to resolve later
        - E.g. schema updates
    - Exceptions managed by Operations Masters

Operations Master Roles

- Five roles in total
- Two roles where there is one per forest
    - Schema master
    - Domain naming master
- Three roles where there is one per domain
    - Relative Identifier (RID) master
    - Primary Domain Controller (PDC) Emulator
    - Infrastructure master

Schema Master

- Responsible for schema updates
- Only DC that can process schema updates
  - After update, replicates changes to other DCs
- If this Operations master is unavailable, no schema changes can be made

Domain Naming Master

- Responsible for changes to configuration naming context
  - Adding and removing domains
  - Adding and removing cross references to domains in external directories
  - After update, replicates to other DCs
- If unavailable, cannot add or remove domains
- Domain Naming Master must also be a global catalog server
  - May be unnecessary in single-domain forest?

RID Master

- Objects e.g. users and groups, each have a unique security identifier (SID)
  - Consists of domain SID and unique relative identifier (RID)
- RID master allocates each DC a pool of RIDs
- When a DC's RID pool falls too low, it requests additional RIDs from RID master
- RID master also controls moving objects between domains
- With no RID master, when a DC runs out of RIDs, new security principals (i.e. users, groups etc.) cannot be created on that DC

Infrastructure Master

- Object in domain referencing object in another domain uses GUID, SID and DN
  - E.g. group in one domain referencing user or group in another domain
- Infrastructure master updates SID and DN in cross-domain references
  - E.g. if referenced object moves
- Multiple-domain, infrastructure master role must not be held by GC server
  - Not a problem in single-domain forests (because no external references)

PDC Emulator

- Mixed Mode
  - Acts as NT PDC to NT BDCs
    - Supports Netlogon replication
- Native and Mixed Modes
  - Password changes replicated preferentially to PDC emulator
    - Authentication failures due to bad password at another DC forwarded to PDC emulator before failing completely
  - Manages password changes from Client machines.

PDC Emulator *cont.*

- Native and Mixed Modes
  - By default, Group Policy snap-in runs on PDC emulator
    - Reduces potential for Group Policy replication conflicts
    - Can be changed

PDC Emulator *cont.*

- Miscellaneous
  - All DCs synchronize their clock to that of the PDC emulator
    - PDC emulator of forest root domain should be synchronized to external time source
    - In multi-domain forest, PDC emulator for domain synchronizes with PDC emulator of forest root domain
  - Acts as Domain Master Browser

Default Placement of Roles

- First DC in a forest holds all roles
- First DC in a new domain within existing forest holds all domain roles
  - RID master
  - Infrastructure master
  - PDC emulator

Guidelines for the Placement of Roles

- Keep schema master and domain naming master roles on same DC
  - DC should also be a global catalog server
- Put RID master and PDC emulator roles on the same DC
- In multi-domain forest, the infrastructure master must not be a global catalog server
  - Should have good connection to global catalog server

Guidelines for the Placement of Roles *cont.*

- Single-domain forest
  - Keep all five roles on same DC which should also be a global catalog server
- Multiple-domain forest
  - Move infrastructure master role to a DC that is not a global catalog server

Thank you!!!