DNS
DNS a AD

http://www.cs.vsb.cz/navrat

Jan Žák

Agenda

- Obecné DNS
- DNS a domény
- Forwardery
- Zóny
- Záznamy
- Integrace do AD
- NSLOOKUP
- DNSLINT

Types of Names

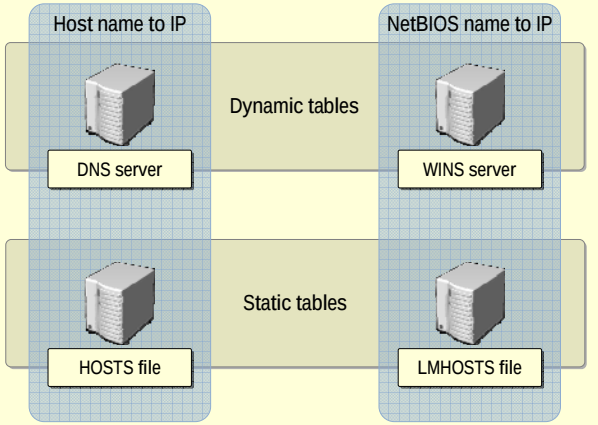
Host name:

- Assigned to a computer's IP address
- Up to 255 characters long
- Can contain alphabetic and numeric characters, hyphens, and periods
- Together with domain name, this creates a fully qualified domain name

NetBIOS name:

- A 16-byte address
- 15 of the bytes may be used for the name which may include alphabetic and numeric characters, hyphens, and periods
- The 16th byte is used by the services that a computer offers to the network

Mapping Names: Dynamic or Static Tables



Dynamic IP Mapping

DNS Server:

- A system for naming computers and network services
- Is a naming system organized in a hierarchical fashion
- Maps domain names to IP address
- Stores mapping records
- Is assigned to a computer's IP address

WINS Server:

- Provides a distributed database for registering dynamic mappings of NetBIOS names
- Maps NetBIOS names to IP addresses

Static IP Mapping

DNS server

- Provides name resolution for host name to IP address
- Allows multiple host names to be assigned to the same IP address

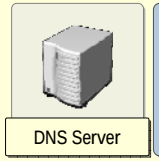
HOSTS file

WINS Server

- Provides a distributed database for registering dynamic mappings of NetBIOS names
- Maps NetBIOS names to IP addresses

LMHOSTS file

Selecting a Name Resolution Method



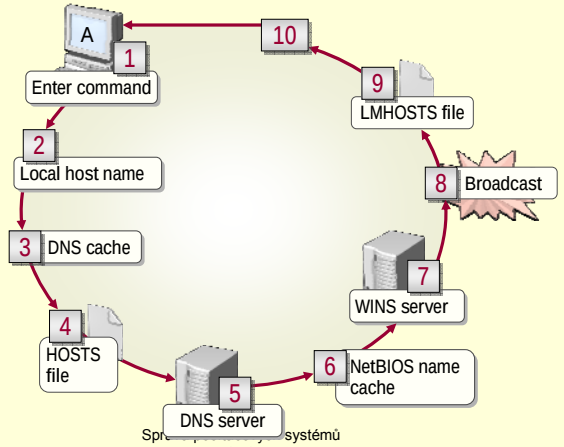
DNS is required when:

- Client is a member of the Active Directory domain
- Client needs to communicate over the Internet

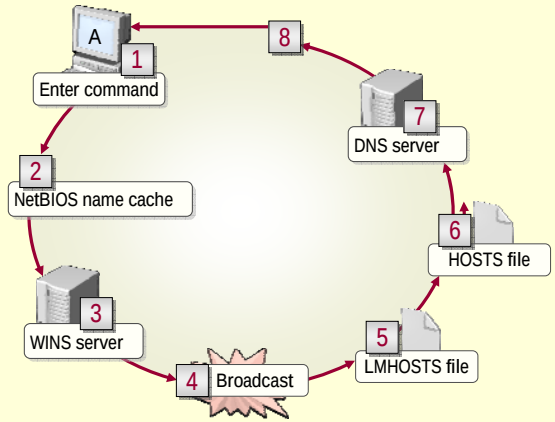
WINS is required when:

- Client is a member of a Windows NT 4.0 or earlier domain
- Client applications or services require NetBIOS name resolution

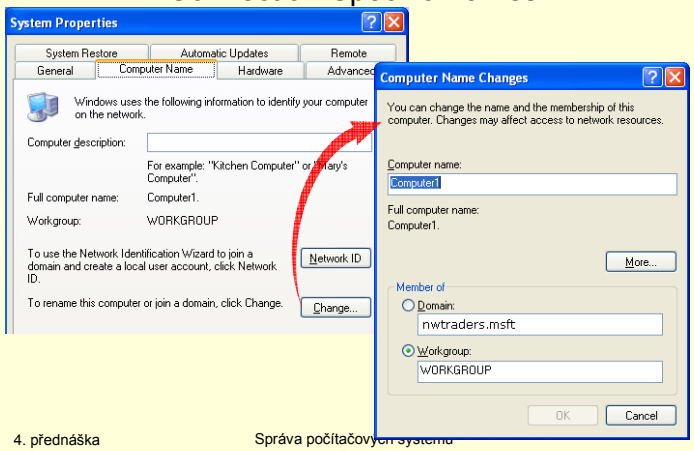
Host Name Resolution Process



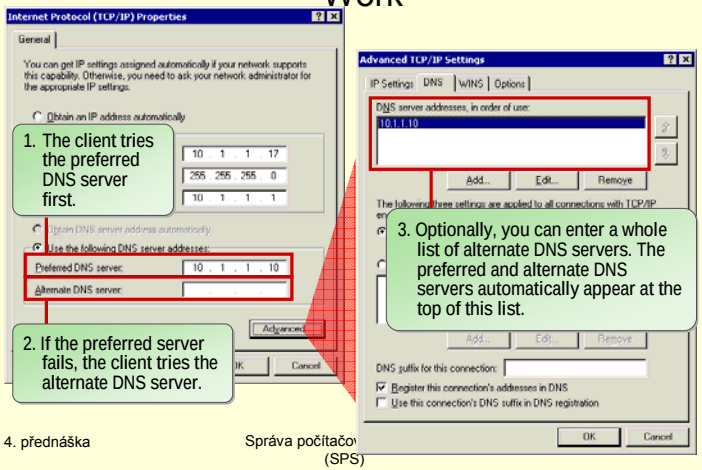
The NetBIOS Name Resolution Process



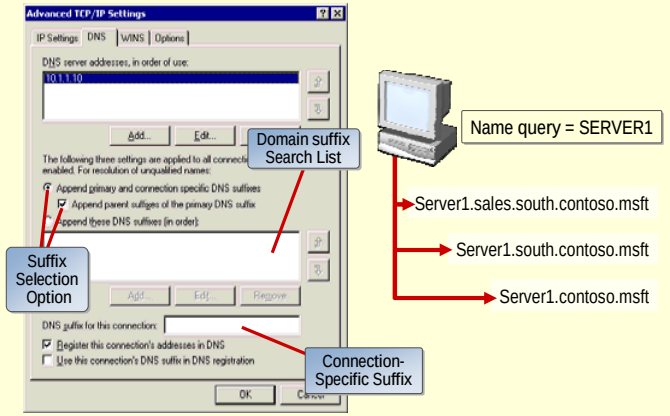
Specifying Host Names, Domain Names, and Connection-Specific Names



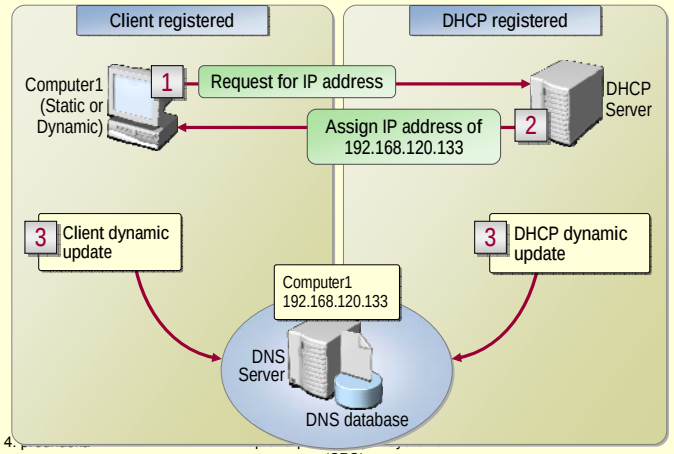
How Preferred and Alternate DNS Servers Work



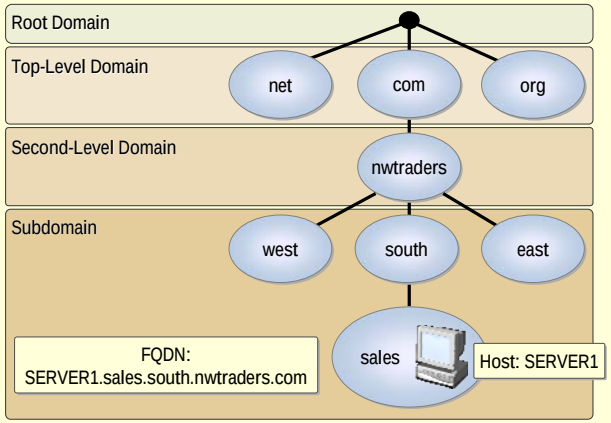
How Suffixes Are Applied



Configuring DHCP to Dynamically Update DNS



What Is a Domain Namespace?



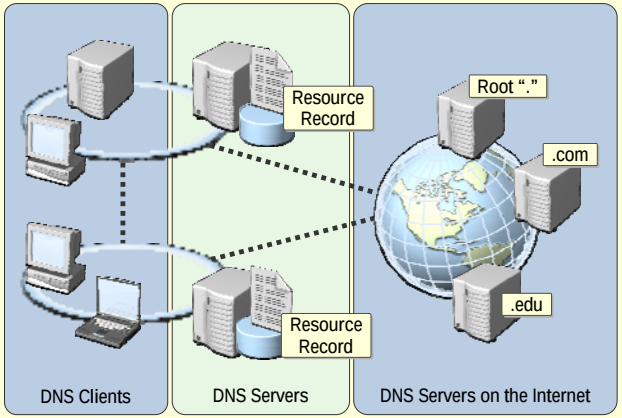
Standards for DNS Naming

The following characters are valid for DNS names:

- A through Z
- a through z
- 0 through 9
- Hyphen (-)

The underscore (_) is a reserved character

What Are the Components of a DNS Solution?



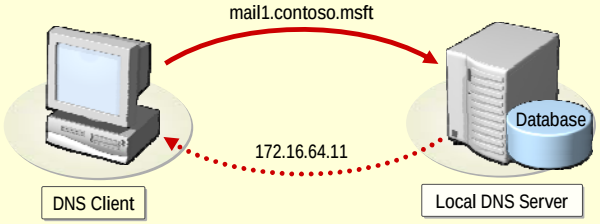
What Is a DNS Query?

A *query* is a request for name resolution and is directed to a DNS server

- Queries are recursive or iterative
- DNS clients and DNS servers both initiate queries
- DNS servers are authoritative or nonauthoritative for a namespace
- An authoritative DNS server for the namespace will either:
  - Return the requested IP address
  - Return an authoritative "No"
- A nonauthoritative DNS server for the namespace will either:
  - Check its cache
  - Use forwarders
  - Use root hints

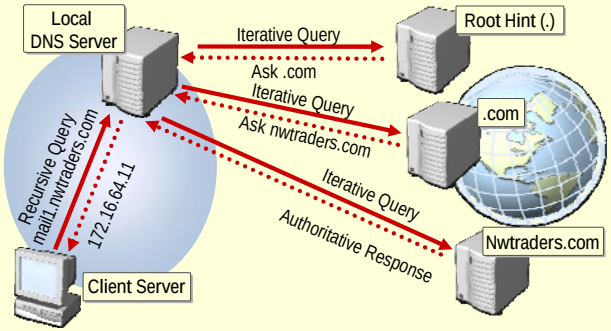
How Recursive Queries Work

A *recursive query* is sent to a DNS server and requires a complete answer



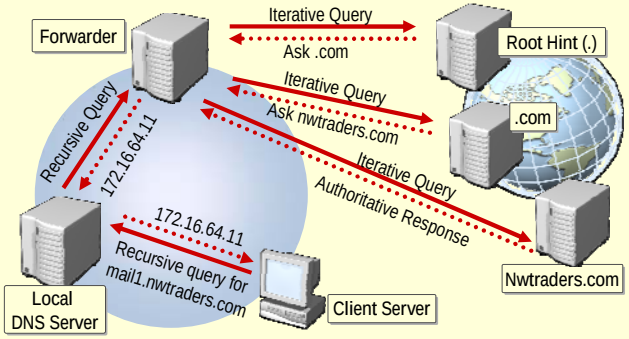
How Iterative Queries Work

An iterative query directed to a DNS server may be answered with a referral to another DNS server



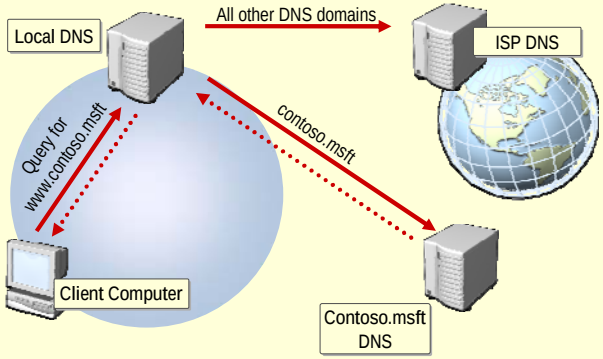
How Forwarders Work

A *forwarder* is a DNS server designated to resolve external or offsite DNS domain names



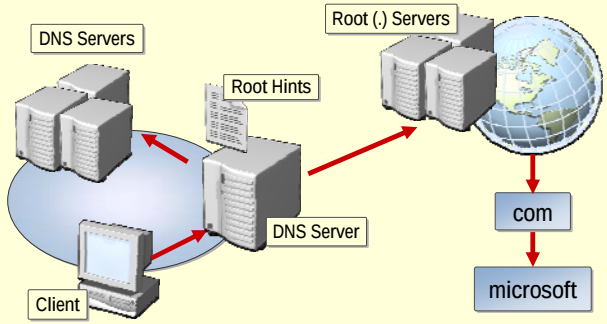
How Conditional Forwarding Works

Conditional forwarding forwards requests using a domain name condition



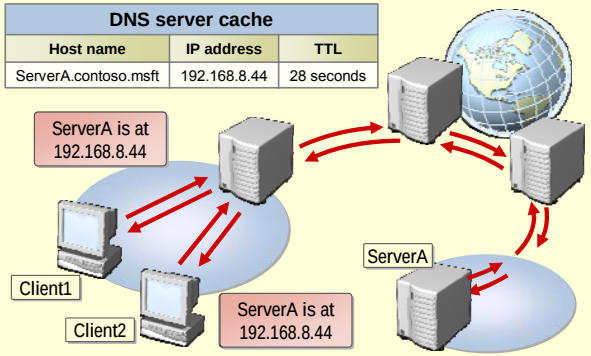
How Root Hints Work

Root hints contain the IP addresses for DNS root servers



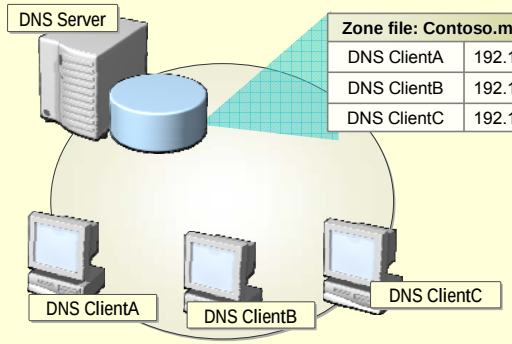
How DNS Server Caching Works

DNS server cache		
Host name	**IP address**	**TTL**
ServerA.contoso.msft	192.168.8.44	28 seconds

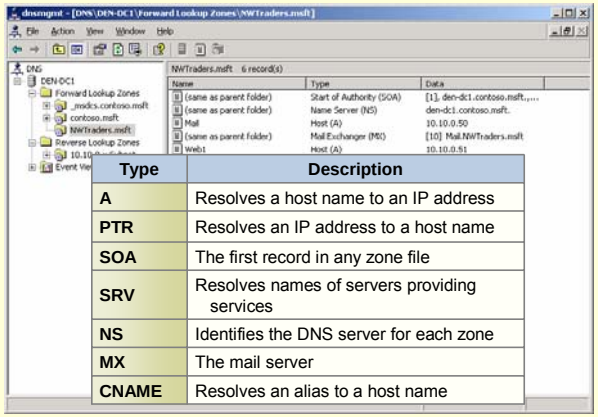


How DNS Data Is Stored and Maintained

A zone contains resource records for a contiguous portion of the DNS namespace

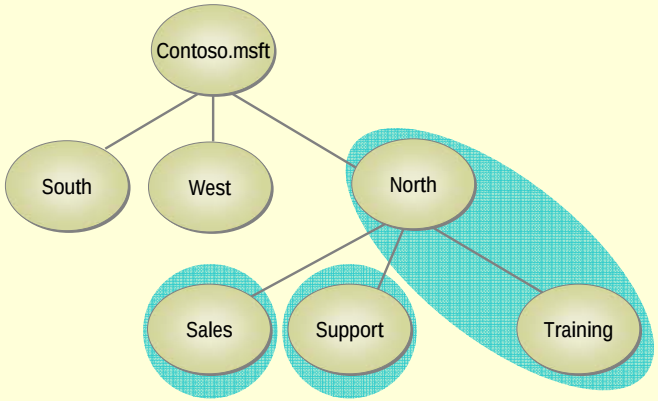


What Are Resource Records and Record Types?



Type	Description
A	Resolves a host name to an IP address
PTR	Resolves an IP address to a host name
SOA	The first record in any zone file
SRV	Resolves names of servers providing services
NS	Identifies the DNS server for each zone
MX	The mail server
CNAME	Resolves an alias to a host name

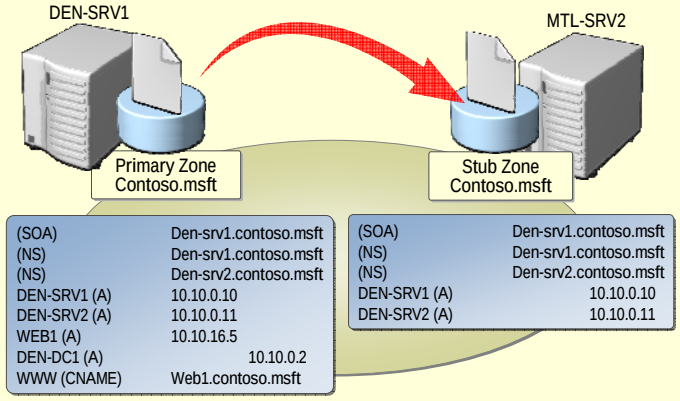
What Is a DNS Zone?



What Are DNS Zone Types?

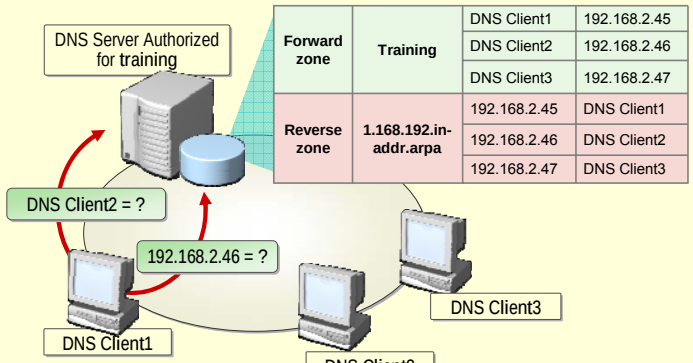
Zones	Description
Primary	Read/write copy of a DNS database
Secondary	Read-only copy of a DNS database
Stub	Copy of a zone that contains only records used to locate name servers
Active Directory integrated	Zone data is stored in Active Directory rather than in zone files

What Are Stub Zones?

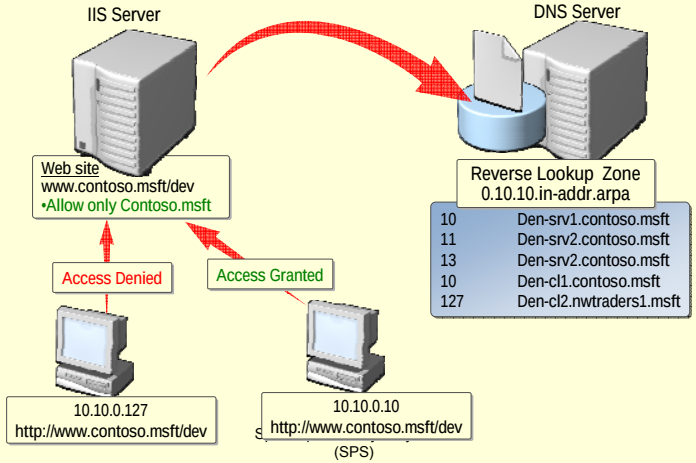


What Are Forward and Reverse Lookup Zones?

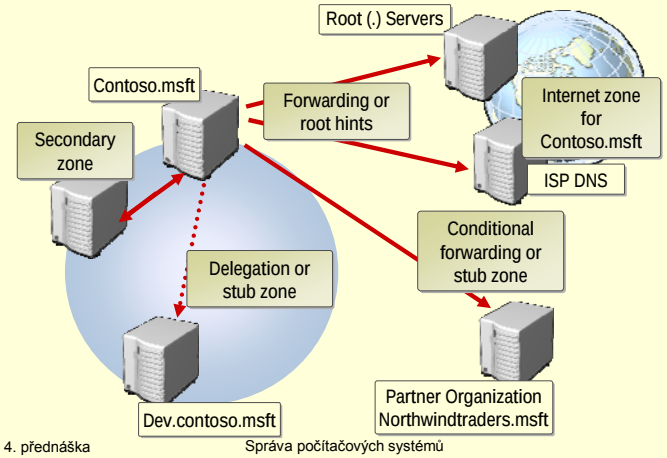
Namespace: training.nwtraders.msft



Why Use Reverse Lookup Zones?

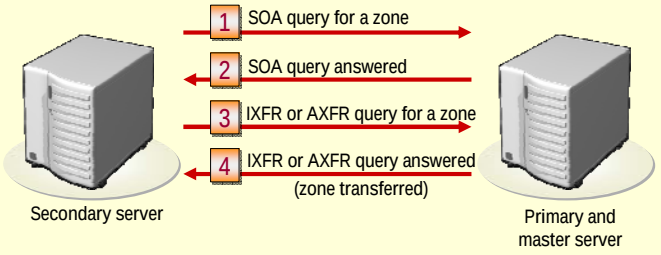


Guidelines for Configuring DNS Zones

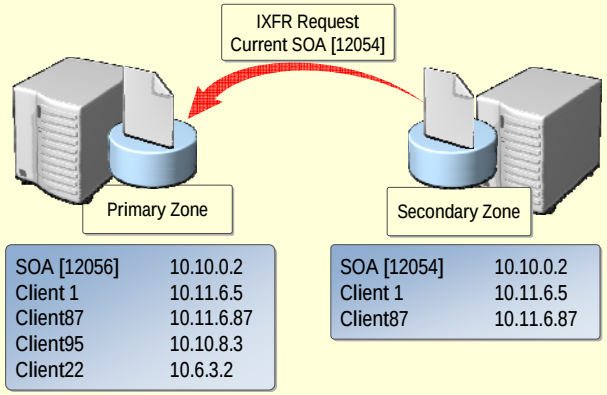


How DNS Zone Transfers Work

A *DNS zone transfer* is the synchronization of authoritative DNS zone data between DNS servers

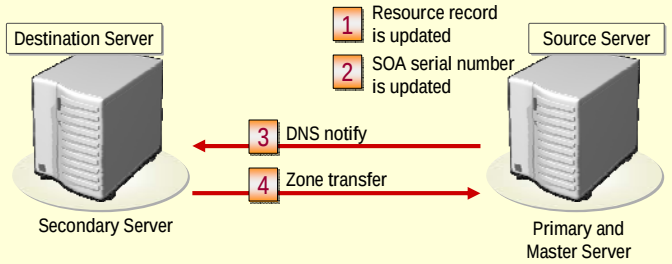


How Incremental Zone Transfers Work



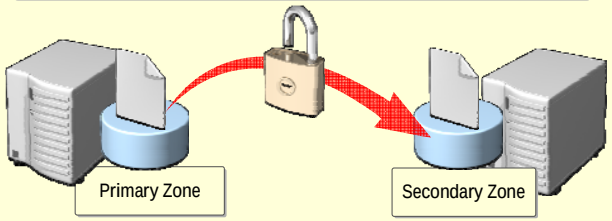
How DNS Notify Works

A *DNS notify* is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur



How to Secure Zone Transfers

- Restrict zone transfer to specified servers
- Encrypt zone transfer traffic
- Consider using Active Directory integrated zones

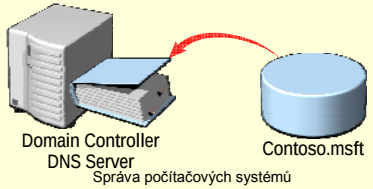


Active Directory Integrated Zones

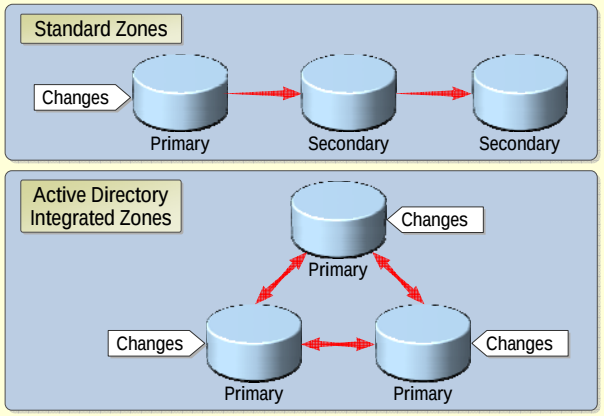
Active Directory integrated zones store DNS zone data in the Active Directory database

Requirements:

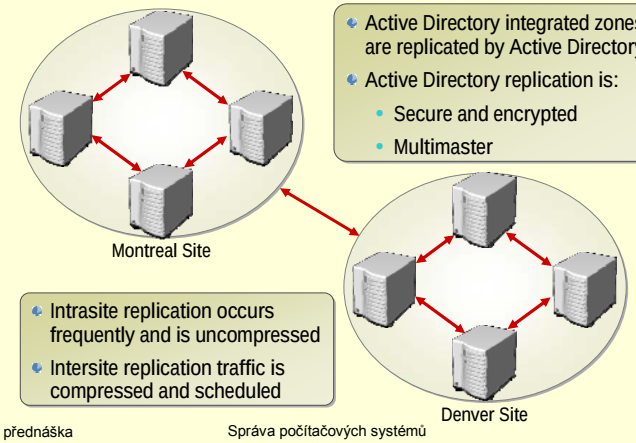
- Active Directory must be installed
- DNS service must be installed to service client requests



Why Use Active Directory Integrated Zones?



Replicating Active Directory Integrated Zones

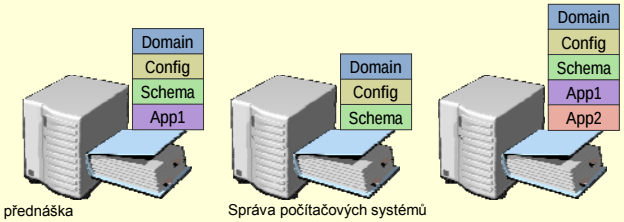


- Active Directory integrated zones are replicated by Active Directory
- Active Directory replication is:
  - Secure and encrypted
  - Multimaster

- Intrasite replication occurs frequently and is uncompressed
- Intersite replication traffic is compressed and scheduled

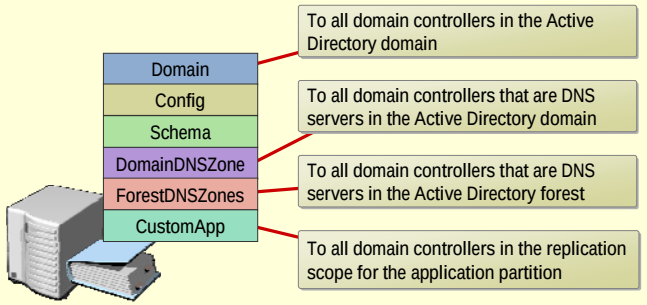
DNS and Active Directory Partitions

- A DNS zone can be stored in the domain partition or in an application partition
- Administrators can define the replication scope of application partitions
- DomainDNSzones and forestDNSzones are default application partitions that store DNS-specific data



Configuring DNS to Use Active Directory Partitions

Windows Server 2003 domain controllers can store Active Directory integrated zones in application partitions



What Are Dynamic Updates?

A *dynamic update* is the process of a DNS client automatically updating records in DNS

Dynamic updates:

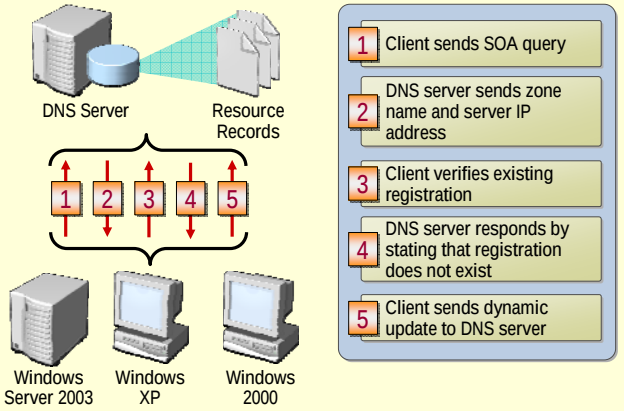
- Reduce administrative overhead
- Streamline management of resource records

A *manual update* is the process of an administrator manually updating records in DNS

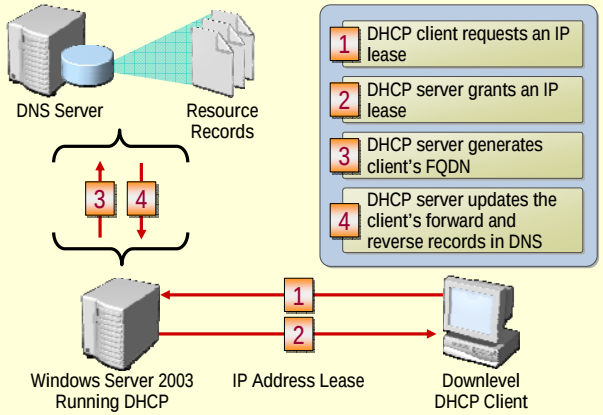
Manual updates:

- Provide greater control over resource records
- Increase administrative overhead
- Should be used for Internet DNS servers

How DNS Clients Register Resource Records

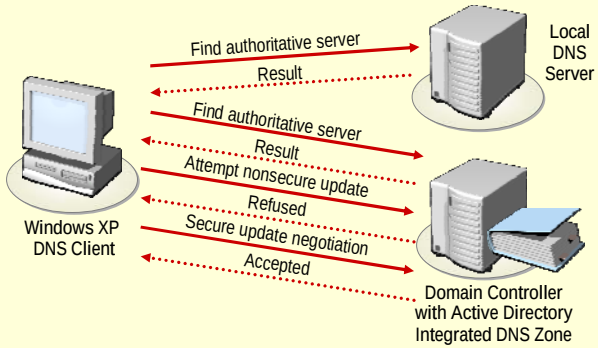


How DHCP Servers Register Resource Records



How Active Directory Integrated DNS Zones Use Secure Dynamic Updates

A *secure dynamic update* is accepted only if the client has the proper credentials to make the update



What Are Service Locator Records?

SRV records allow DNS clients to locate TCP/IP-based Services. SRV records are used when:

- A domain controller needs to replicate
- A client searches Active Directory
- A user attempts to change his or her password
- An Exchange 2003 server performs a directory lookup
- An administrator modifies Active Directory

SRV record syntax:

```
protocol.service.name  TTL  class  type  priority  weight  port  target
```

Example of a SRV record

```
_ldap._tcp.contoso.msft  600  IN  SRV  0  100  389 den-dc1.contoso.msft
```

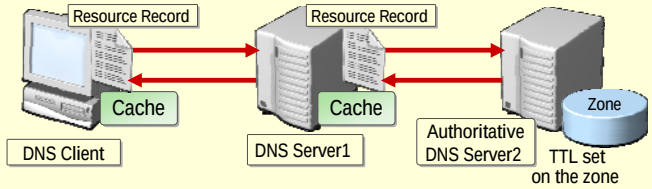

How SRV Records Are Registered

To register SRV records, consider the following:

- The Net Logon service is responsible for updating SRV records in DNS
- DNS dynamic updates should be enabled
- %systemroot%\system32\config\netlogon.dns contains the SRV records that are registered

What Is the Time to Live?

The *Time to Live* value indicates how long a record should be cached



1. The records in the zone are sent to other DNS servers and clients in response to queries
2. Records are cached based on the TTL period supplied in the record
3. When the TTL expires, the record is removed from the cache

What Are Aging and Scavenging Parameters?

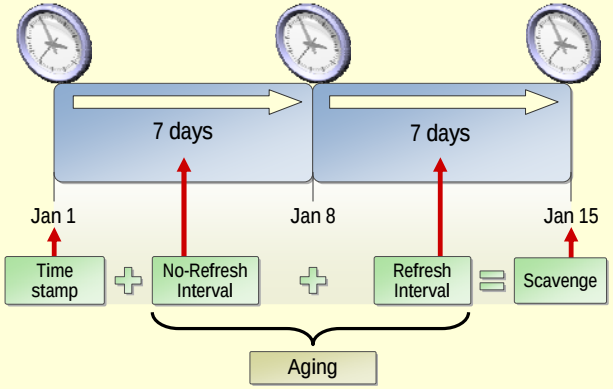
Aging determines when a stale record should be removed from the DNS database

Scavenging removes outdated or extinct names from the database

A *refresh attempt* is the process of a computer renewing its DNS record

Parameter	Description	Example
No-Refresh Interval	**DNS server *does not* accept refresh attempts**	**7 days (default)**
Refresh Interval	**DNS server *does* accept refresh attempts**	**7 days (default)**

How Aging and Scavenging Work



Why Verify That a Resource Record Exists?

To identify problems with your DNS solution, you can verify:

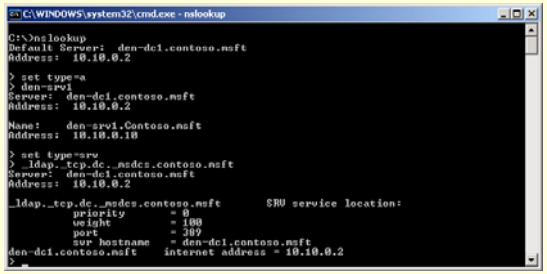
- Missing records
- Incomplete records
- Incorrectly configured records

You can use the following three tools to monitor DNS:

- Nslookup
- Dnscmd
- Dnslint

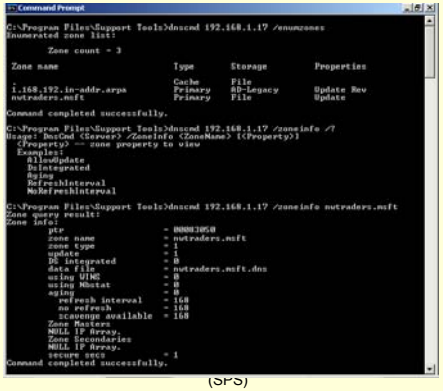
What Is Nslookup?

Nslookup is a command-line tool used to diagnose DNS infrastructure



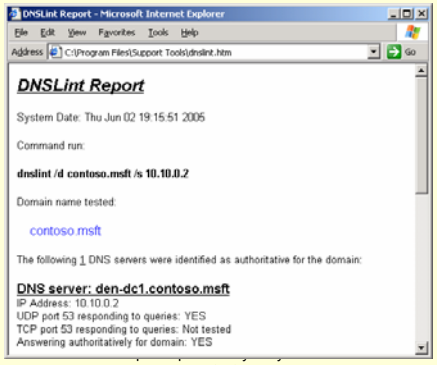
What Is Dnscmd?

Dnscmd allows you to complete many DNS administrative tasks from the command prompt



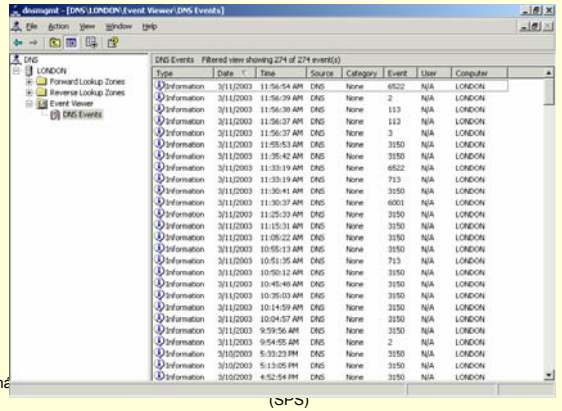
What Is Dnslint?

The *Dnslint* tool can run a series of queries to help diagnose common DNS name resolution problems



What Is a DNS Event Log?

A *DNS event log* is configured to log only DNS events



What Is DNS Debug Logging?

DNS debug logging allows for detailed DNS statistics and information to be gathered