

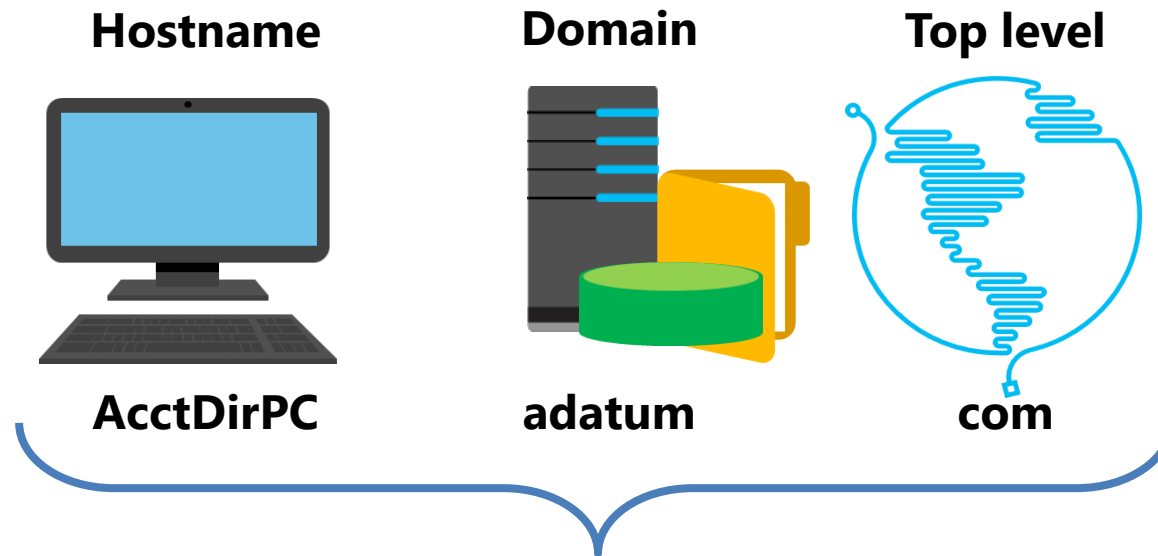
ADMINISTRATION OF OPERATING SYSTEMS

DNS on Windows
Server



How does DNS name resolution work?

A *hostname* is a computer name that is added to a domain name and top level domain to make a fully qualified domain name (FQDN)



Fully qualified domain name = AcctDirPC.adatum.com

NetBIOS names are rarely used and are being deprecated in Windows operating systems

DNS components

- DNS namespace is a hierarchical naming structure that provides multiple identifiers for each network node that can be identified relative to the root domain

computer01.unitedstates.microsoft.com

- DNS infrastructure components include:
 - DNS server
 - DNS zone
 - DNS resolvers
 - Resource records

What are DNS zones and records?

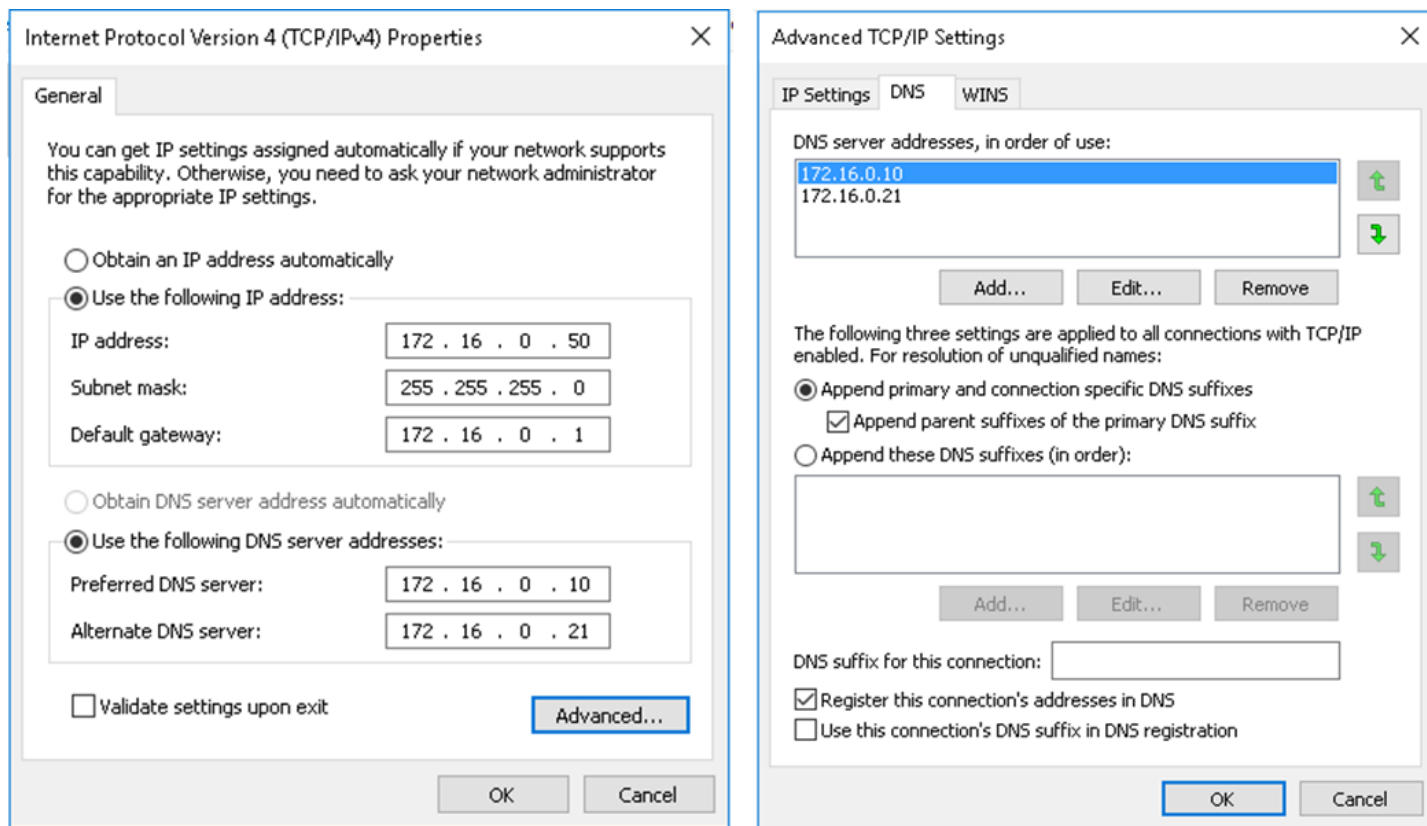
- A DNS zone is a specific portion of DNS namespace that contains DNS records
- Zone types:
 - Forward lookup zone
 - Reverse lookup zone
- Resource records in forward lookup zones include: A, MX, SRV, NS, SOA, and CNAME
- Resource records in reverse lookup zones include: PTR

Demonstration: Installing and configuring the DNS role

In this demonstration, you will learn how to:

- Install the DNS server role
- Configure the DNS Server role to forward requests to LON-DC1.adatum.com

Configuring DNS clients



```
Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses ("172.16.0.10", "172.16.0.21")
```

Tools and techniques for troubleshooting name resolution

- Windows Server 2012 R2 introduced a new Windows PowerShell DNS module with numerous cmdlets, including the **Get-DNSServerStatistics** cmdlet:
 - `$statistics = Get-DnsServerStatistics -ZoneName Adatum.com`
 - `$statistics.ZoneQueryStatistics`
 - `$statistics.ZoneTransferStatistics`
 - `$statistics.ZoneUpdateStatistics`
- Command-line tools to troubleshoot configuration issues:
 - Nslookup
 - DNSCmd
 - DNSLint
 - **Ipconfig**
- The troubleshooting process:
 - Identify client DNS server with **nslookup** or **Resolve-DnsName**
 - Communicate via ping, use **nslookup** to verify records

Managing DNS services

- You can manage DNS services by:
 - Delegating DNS administration through membership in the DNS Admins group
 - Viewing DNS logs in Event Viewer
 - Enabling DNS debug logging in the DNS server properties
 - Enabling aging and scavenging to remove stale records
- Backup methods for the DNS database depend on how the database is deployed:
 - Back up Active Directory–integrated zones through System State backups by using **dnscommand** or by using Windows PowerShell
 - Copy or back up primary zone files that are not using AD DS integration

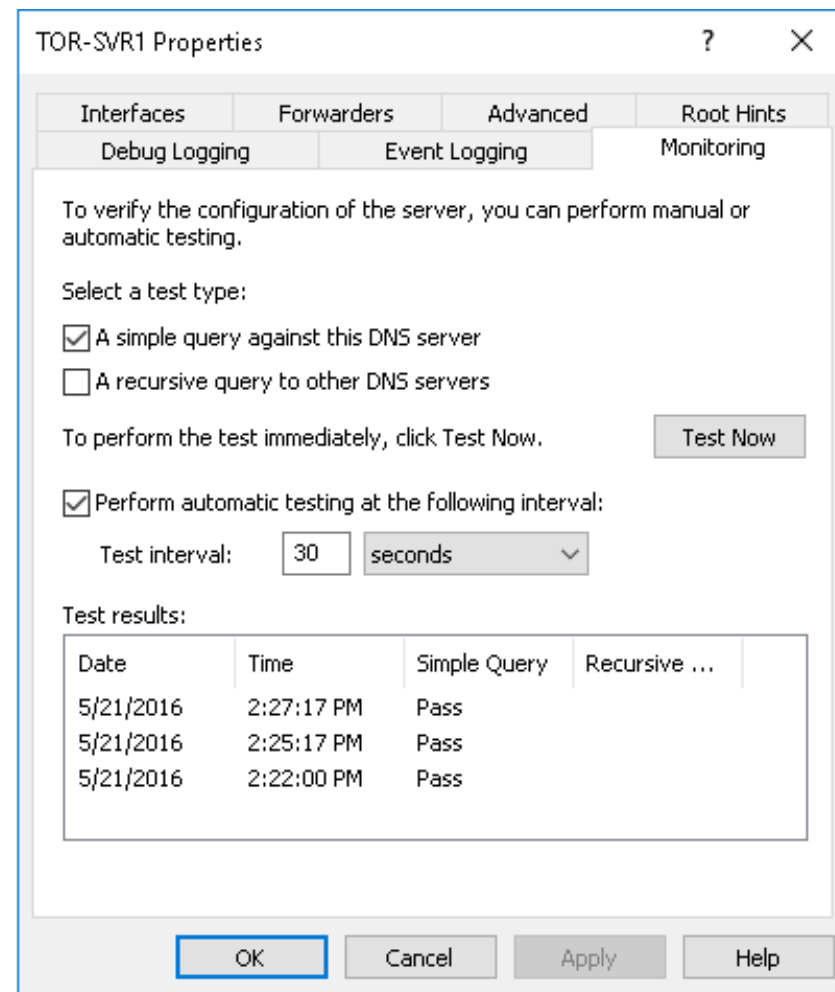
Demonstration: Troubleshooting name resolution

In this demonstration, you will learn how to:

- Use Windows PowerShell cmdlets to troubleshoot DNS
- Use command-line tools to troubleshoot DNS

Testing DNS servers

- **Monitoring** tab on DNS Console:
 - Simple query
 - Recursive query
- Windows PowerShell
 - **Get-DnsServerDiagnostics**
 - **Test-DnsServer**
- **Nslookup -d2 FQDN** Audit and Analytic event logging:
 - Use Event Viewer or tracelog.exe



Demonstration: Testing the DNS server

In this demonstration, you will learn how to:

- Test the DNS server
- Configure auditing and analytical logging of events
- Use Windows PowerShell to configure global DNS settings

DNS resource record types

DNS resource records include:

- SOA: Start-of-authority resource record
- A: IPv4 host address resource record
- CNAME: Alias resource record
- MX: Mail exchange resource record
- SRV: Service locator resource record
- NS: Name server resource record
- AAAA: IPv6 host address resource record
- PTR: Pointer resource record

Creating records in DNS

New Host

Name (uses parent domain name if blank):
ATL-SVR1

Fully qualified domain name (FQDN):
ATL-SVR1.Contoso.com.

IP address:
172.16.18.25

Create associated pointer (PTR) record

Add Host Cancel

New Resource Record

Alias (CNAME)

Alias name (uses parent domain name if left blank):
www

Fully qualified domain name (FQDN):
www.Contoso.com.

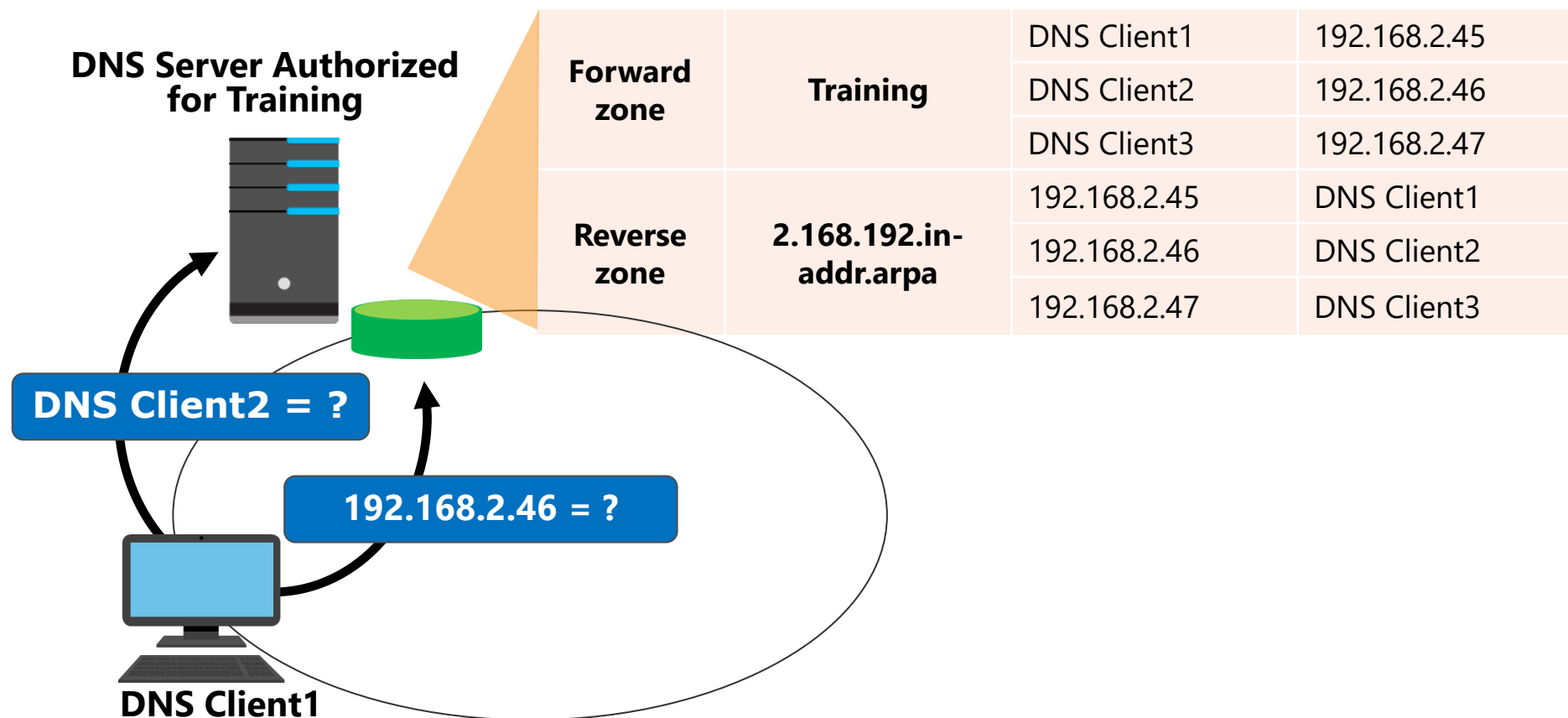
Fully qualified domain name (FQDN) for target host:
ATL-SVR1.Contoso.com Browse...

OK Cancel

**Add-DnsServerResourceRecordA -ZoneName Contoso.com -Name ATL-SVR1
-IpAddress 172.16.18.25**

Configuring DNS zones

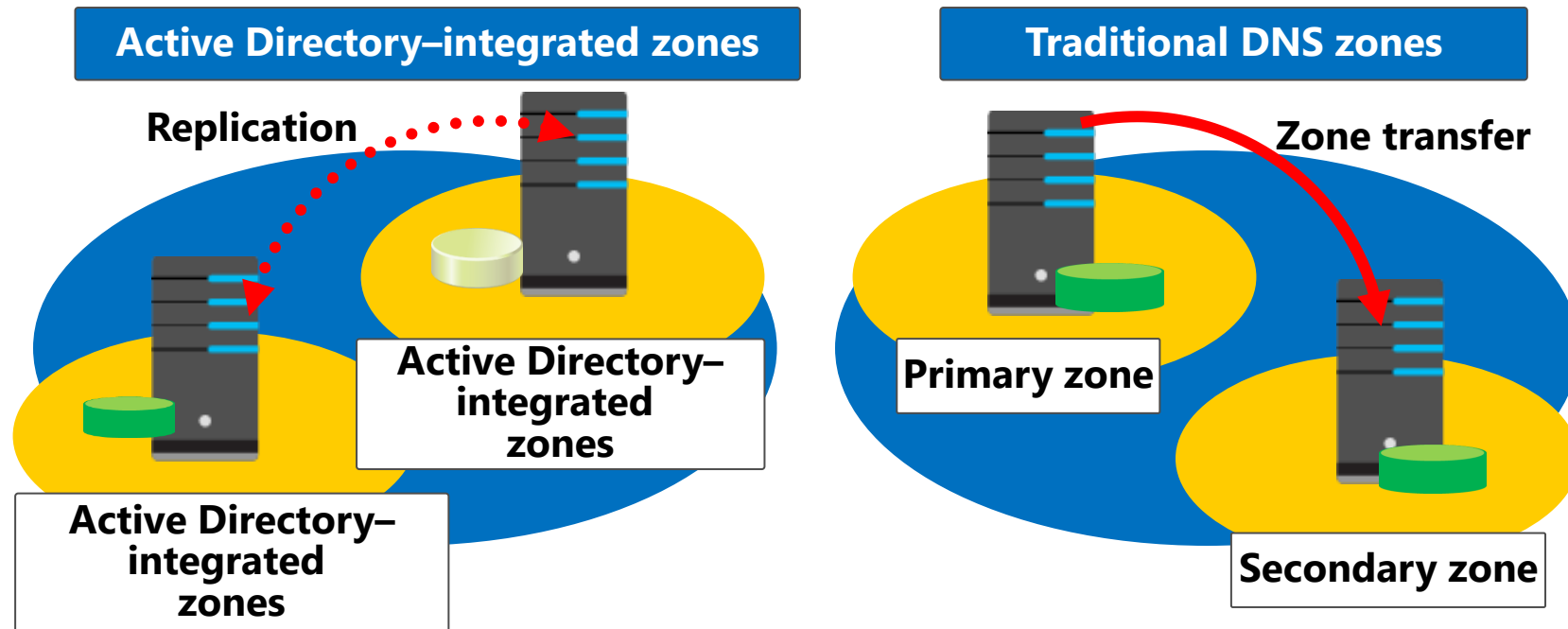
Namespace: training.contoso.com



What are primary and secondary zones?

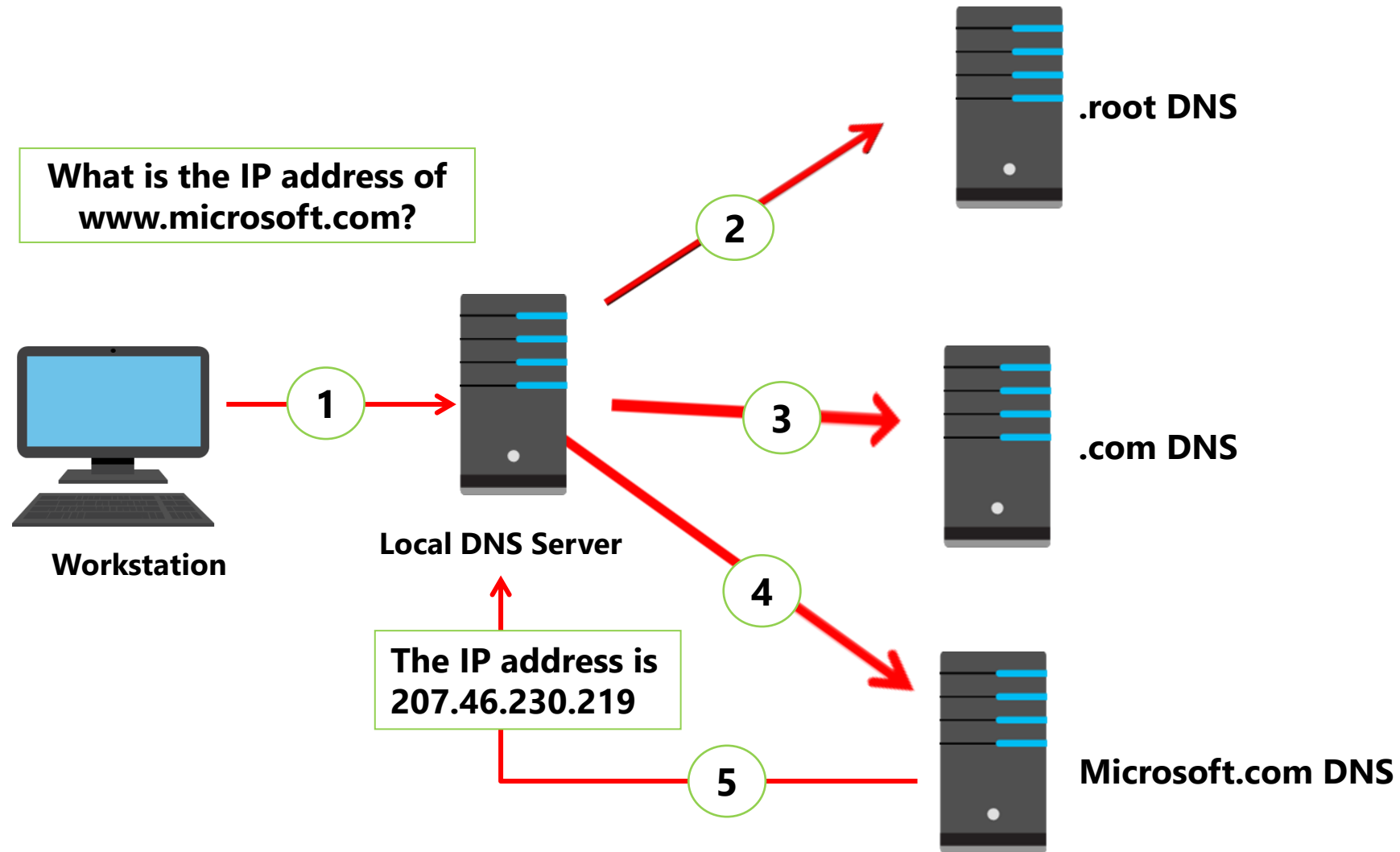
Zones	Description
Primary	Read/write copy of a DNS database
Secondary	Read-only copy of a DNS database
Stub	Copy of a zone that contains only records used to locate name servers
Active Directory–integrated	Zone data is stored in AD DS rather than in zone files

Configuring zone replication



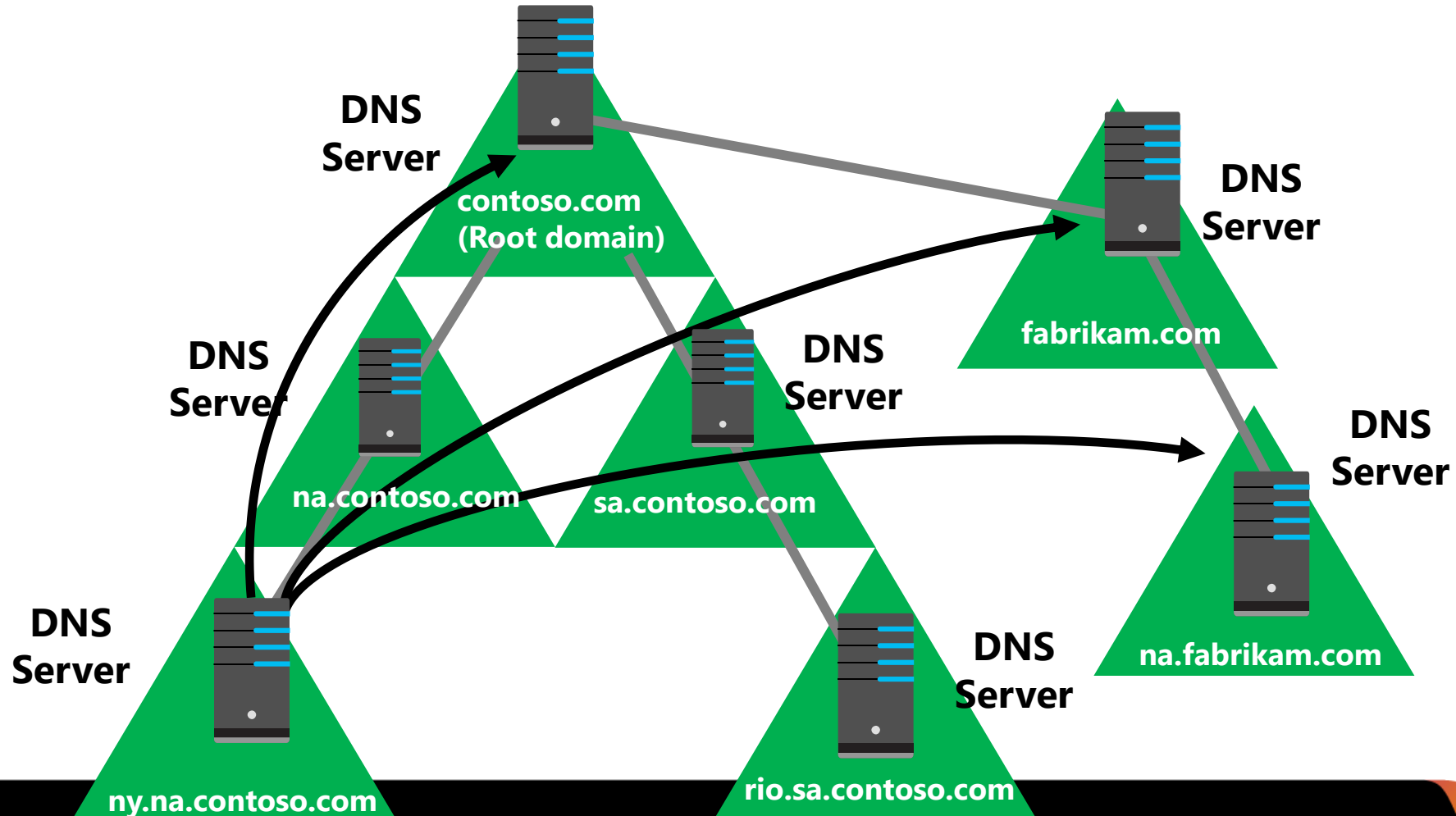
Zones	Description
Active Directory-integrated zones	<ul style="list-style-type: none"> • Perform incremental replication between DNS servers • Adjust the Active Directory replication schedule
Traditional DNS zones	<ul style="list-style-type: none"> • Replicate between primary and secondary zones • Perform an incremental rather than a complete zone transfer

Resolving DNS names between zones



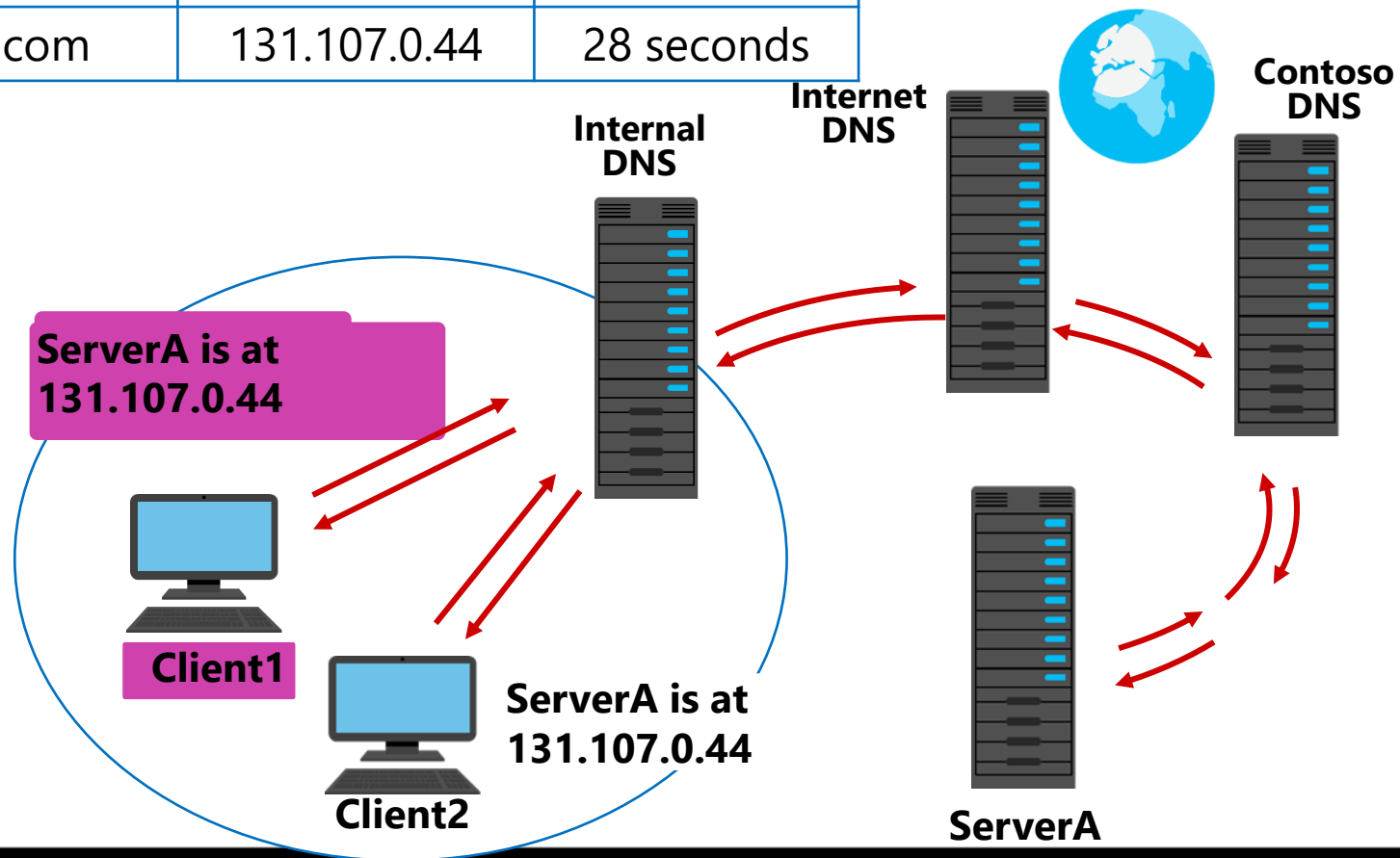
What is a stub zone?

Without stub zones, the ny.na.contoso.com server must query several servers to find the server that hosts the na.fabrikam.com zone



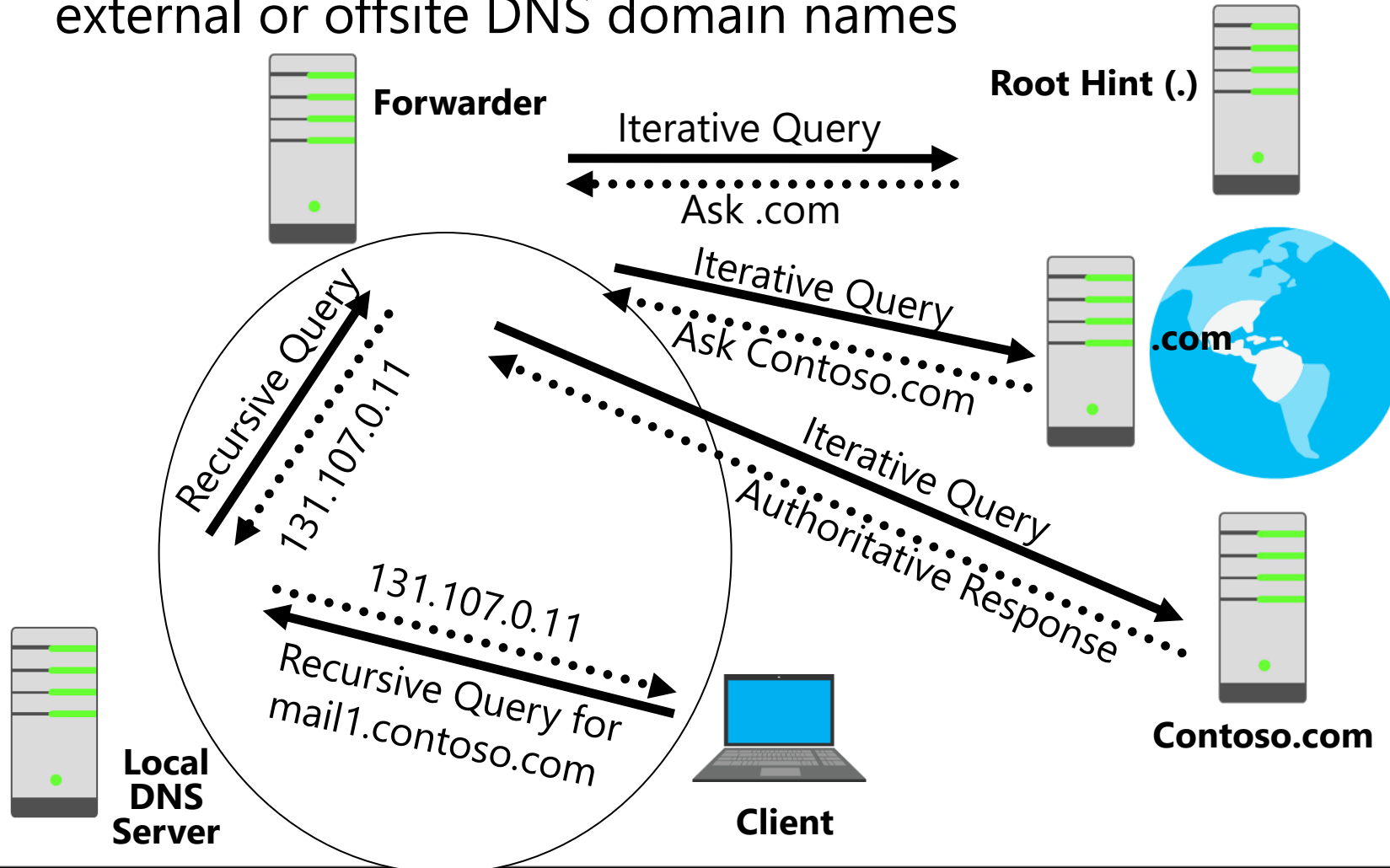
What is DNS caching?

DNS server cache		
Host name	IP address	TTL
ServerA.contoso.com	131.107.0.44	28 seconds



What is DNS forwarding?

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



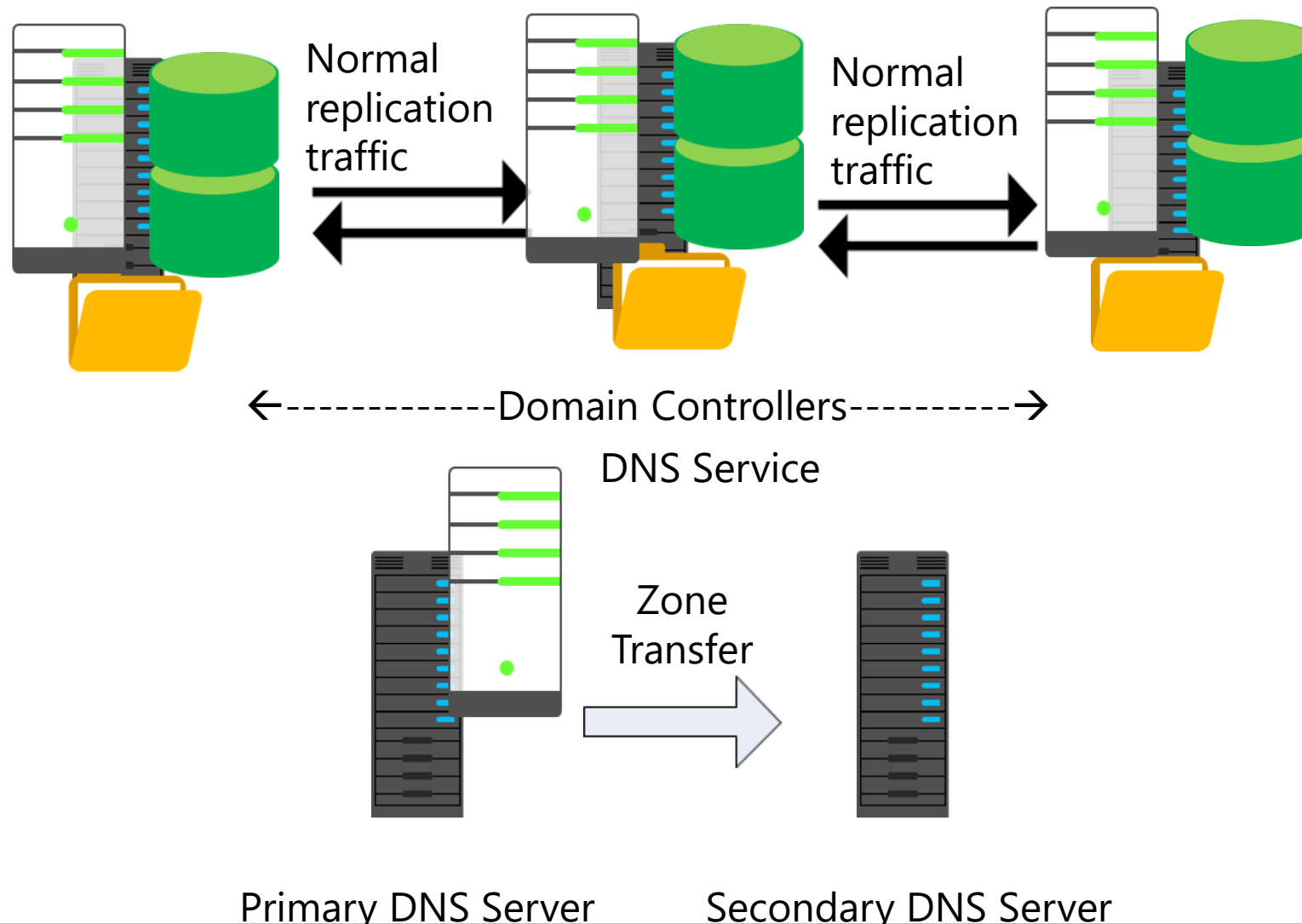
DNS forwarding and stub zone guidance

- When to use conditional forwarding
 - Points to a different domain name
 - Name can even be in a different top level
 - When you want all name resolution for that name to take a particular path
- When to use stub zones
 - Usually when the domain name is below a higher level
 - Delegation below a delegation

Configuring DNS integration with AD DS

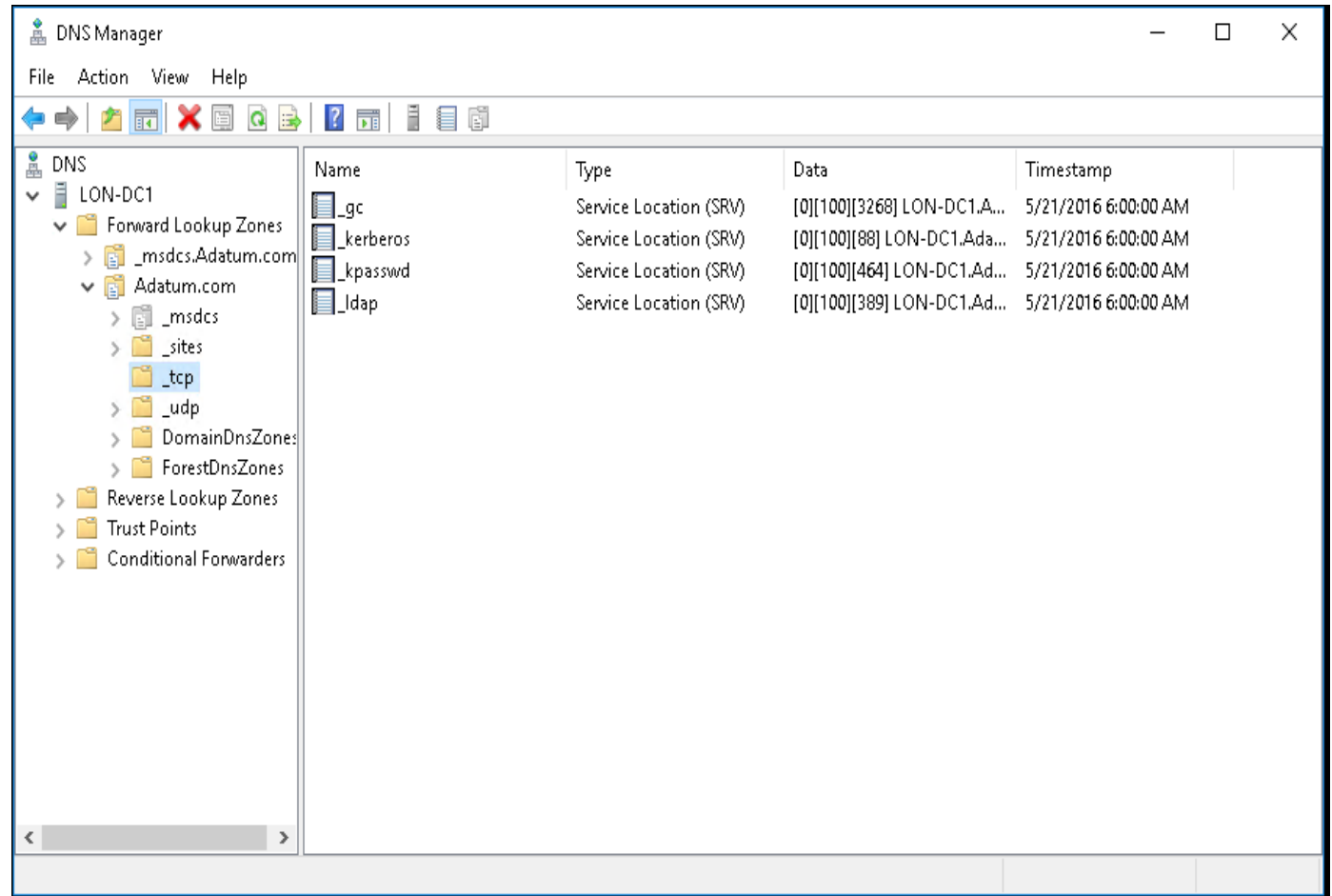
- Overview of AD DS and DNS integration
- What are Service Resource Locator records?
- Benefits of Service Resource Locator records
- What are Active Directory–integrated zones?
- Application partitions in AD DS
- Dynamic updates
- Demonstration: Configuring AD DS–integrated zones

Overview of AD DS and DNS integration



What are Service Resource Locator records?

- Domain controllers register SRV records as follows:
 - `_tcp.adatum.com` — All domain controllers in the domain
 - `_tcp.sitename._sites.adatum.com` — All services in a specific site
- Clients query DNS to locate services in specific sites



The screenshot shows the DNS Manager console with the following table of SRV records:

Name	Type	Data	Timestamp
_gc	Service Location (SRV)	[0][100][3268] LON-DC1.A...	5/21/2016 6:00:00 AM
_kerberos	Service Location (SRV)	[0][100][88] LON-DC1.Ada...	5/21/2016 6:00:00 AM
_kpasswd	Service Location (SRV)	[0][100][464] LON-DC1.Ad...	5/21/2016 6:00:00 AM
_ldap	Service Location (SRV)	[0][100][389] LON-DC1.Ad...	5/21/2016 6:00:00 AM

Benefits of Service Resource Locator records

Benefits of SRV resource records

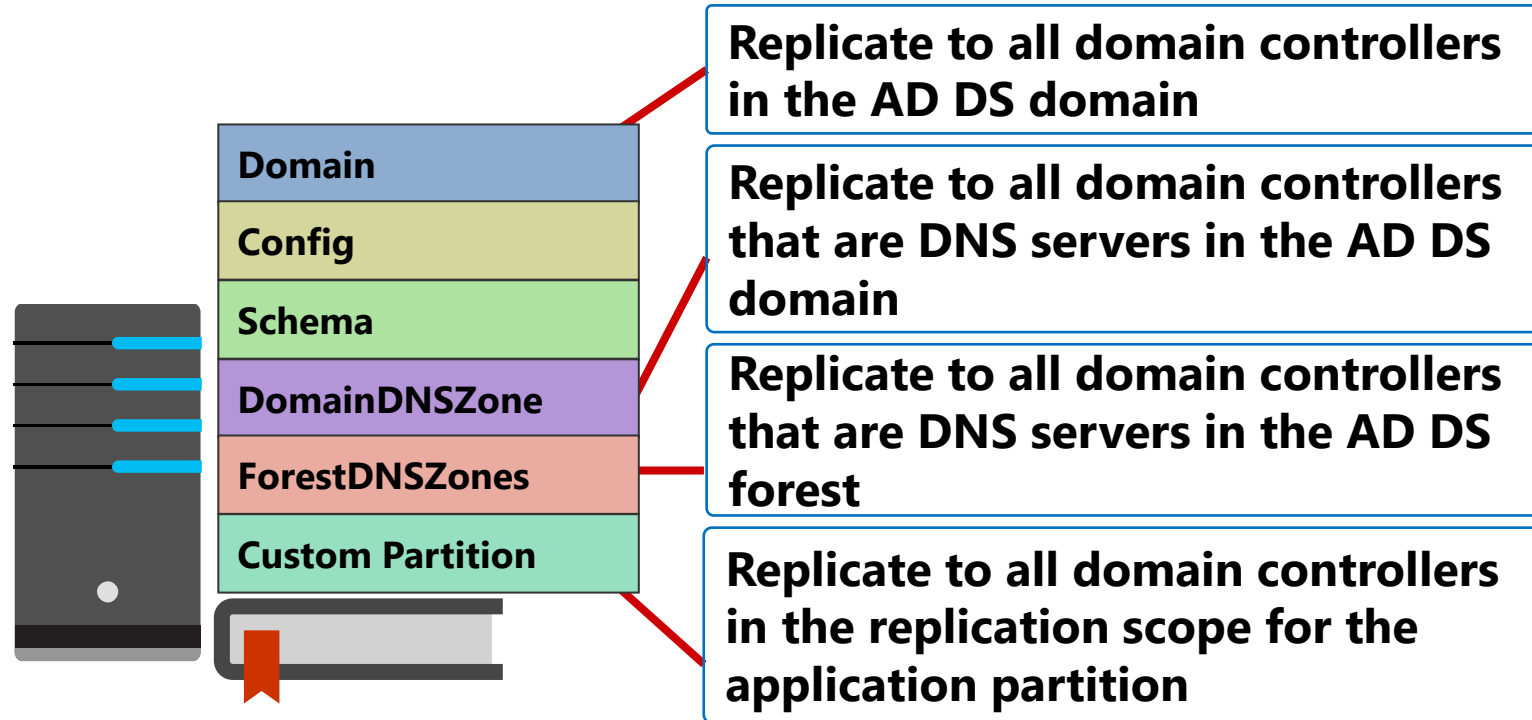
- Domain controllers register their SRV resource records dynamically, by service and site location
- Client systems in sites use SRV resource records recorded in a site to find domain controllers in their own site before attempting to connect to domain controllers across wide area network links
- Keeps network traffic across links down and manageable

What are Active Directory–integrated zones?

An Active Directory–integrated zone:

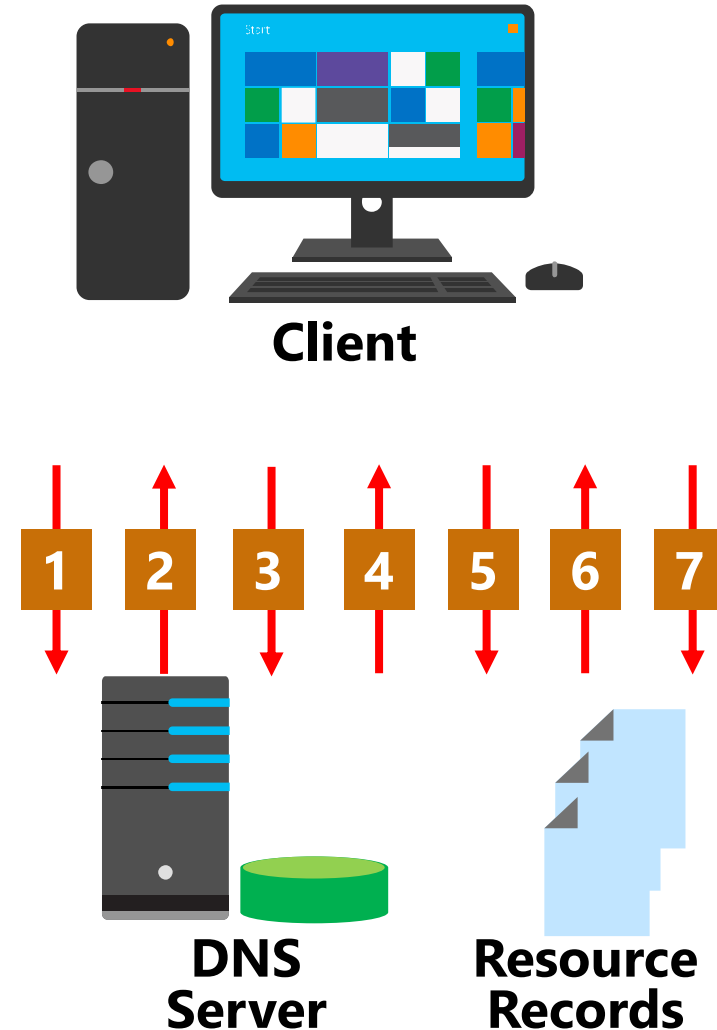
- Allows multi-master writes to zone
- Replicates DNS zone information by using AD DS replication:
 - Leverages efficient replication topology
 - Uses efficient incremental updates for Active Directory replication processes
- Enables secure dynamic updates
- Delegates zones, domains, and resource records for increased security

Application partitions in AD DS



Dynamic updates

1. The client sends an SOA query
2. The DNS server returns an SOA resource record
3. The client sends dynamic update request(s) to identify the primary DNS server
4. The DNS server responds that it can perform an update
5. The client sends unsecured update to the DNS server
6. If the zone permits only secure updates, the update is refused
7. The client sends a secured update to the DNS server



Demonstration: Configuring AD DS–integrated zones

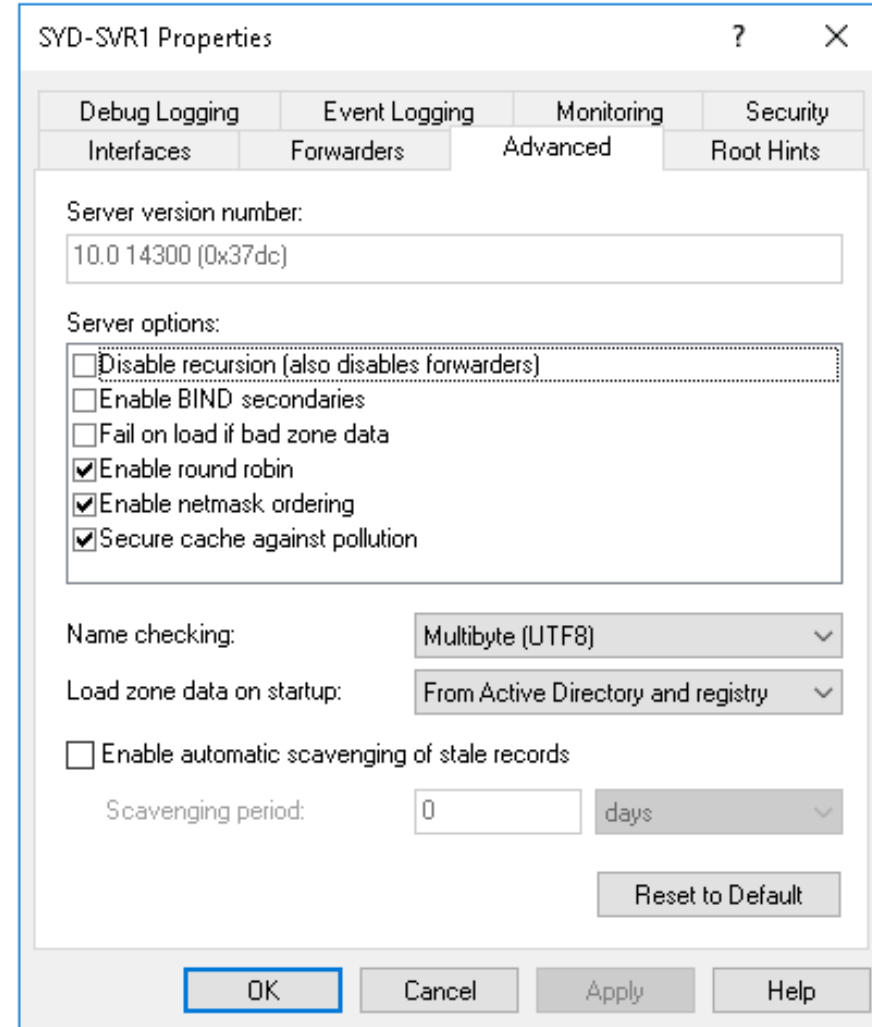
In this demonstration, you will learn how to:

- Promote a server as a domain controller
- Create an Active Directory–integrated zone
- Create a record
- Verify replication to a second DNS server

Configuring advanced DNS name resolution

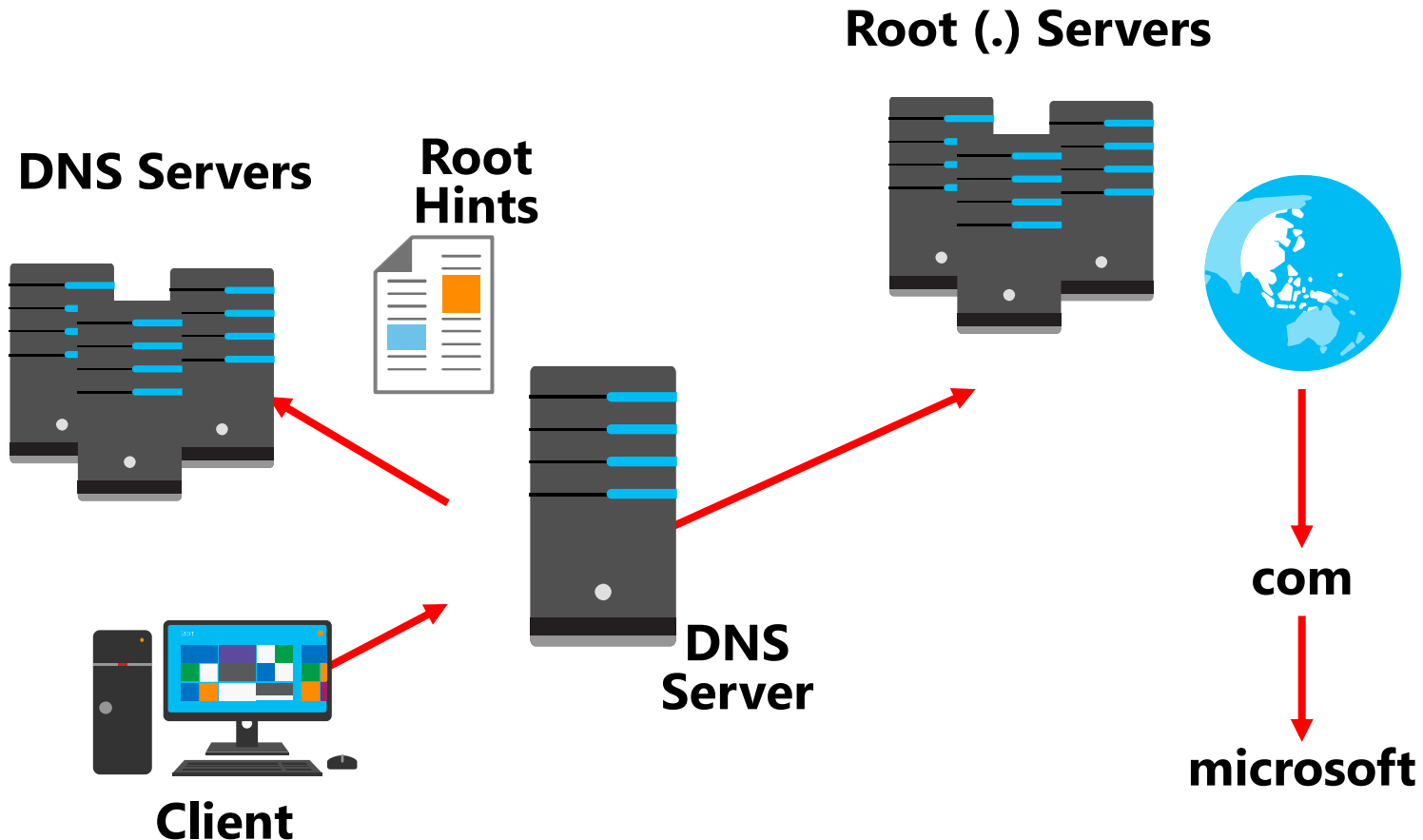
Advanced DNS name resolution:

- DNS round robin
- Netmask reordering
- Recursion



Configuring root hints

Root hints contain the IP addresses for
DNS root servers

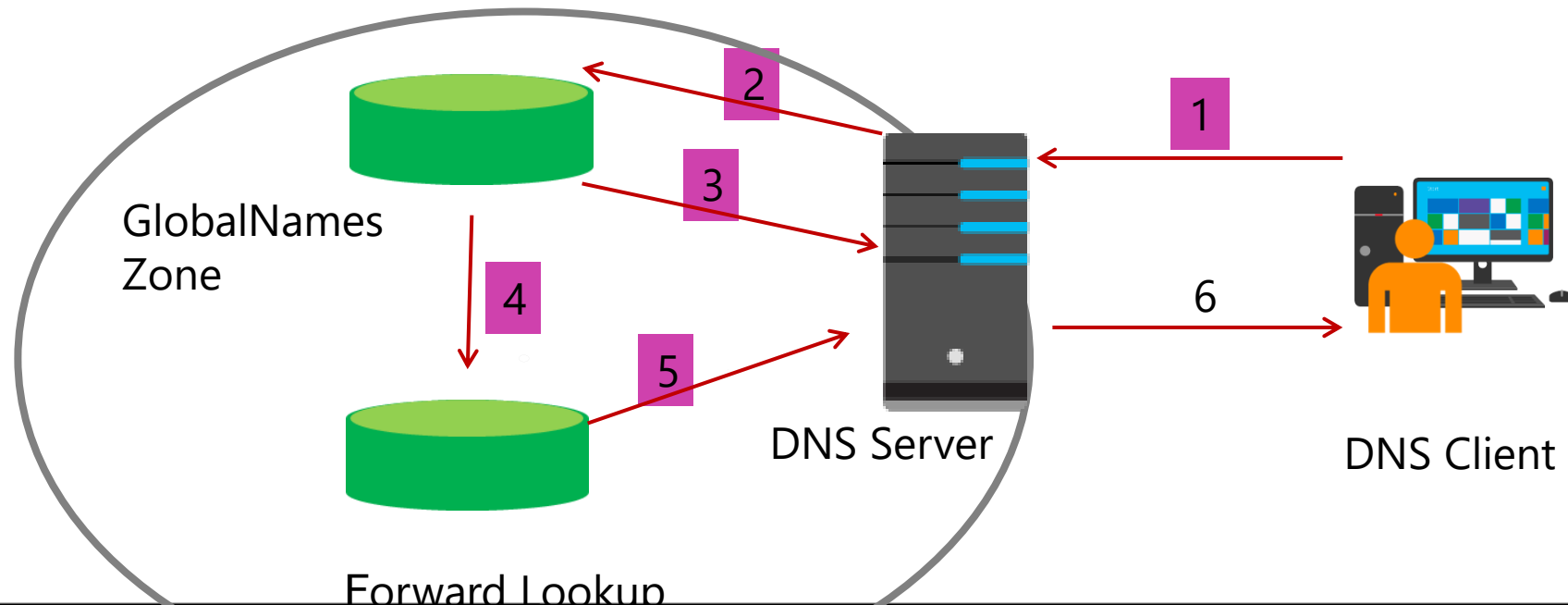


What is the GlobalNames zone?

The GlobalNames zone allows single-label names to be resolved in multiple DNS domain environments

You can configure the GlobalNames zone by using **dnscmd** or by using Windows PowerShell:

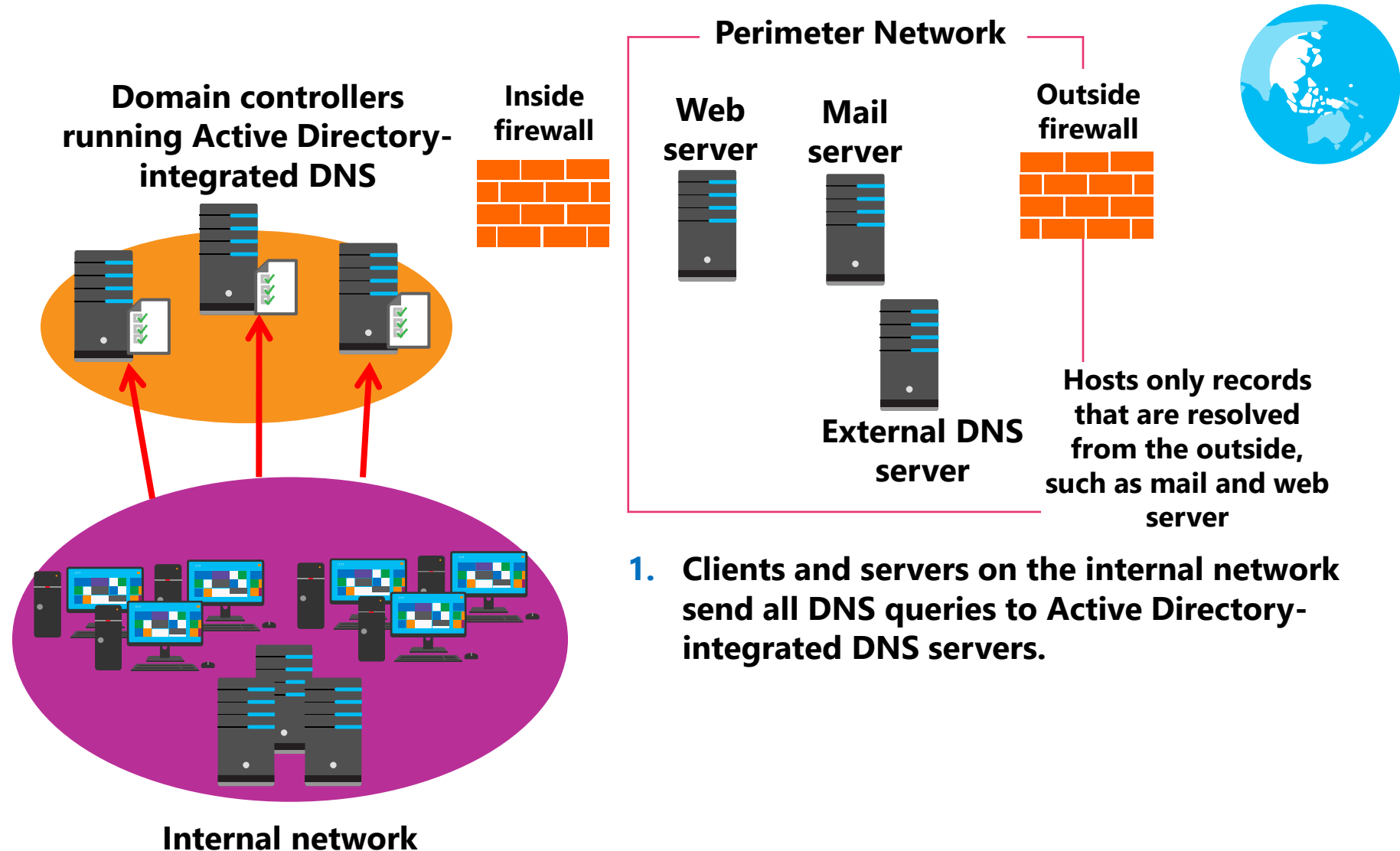
- **Get-DnsServerGlobalNameZone**
- **Set-DnsServerGlobalNameZone**



Demonstration: Configuring the GlobalNames zone

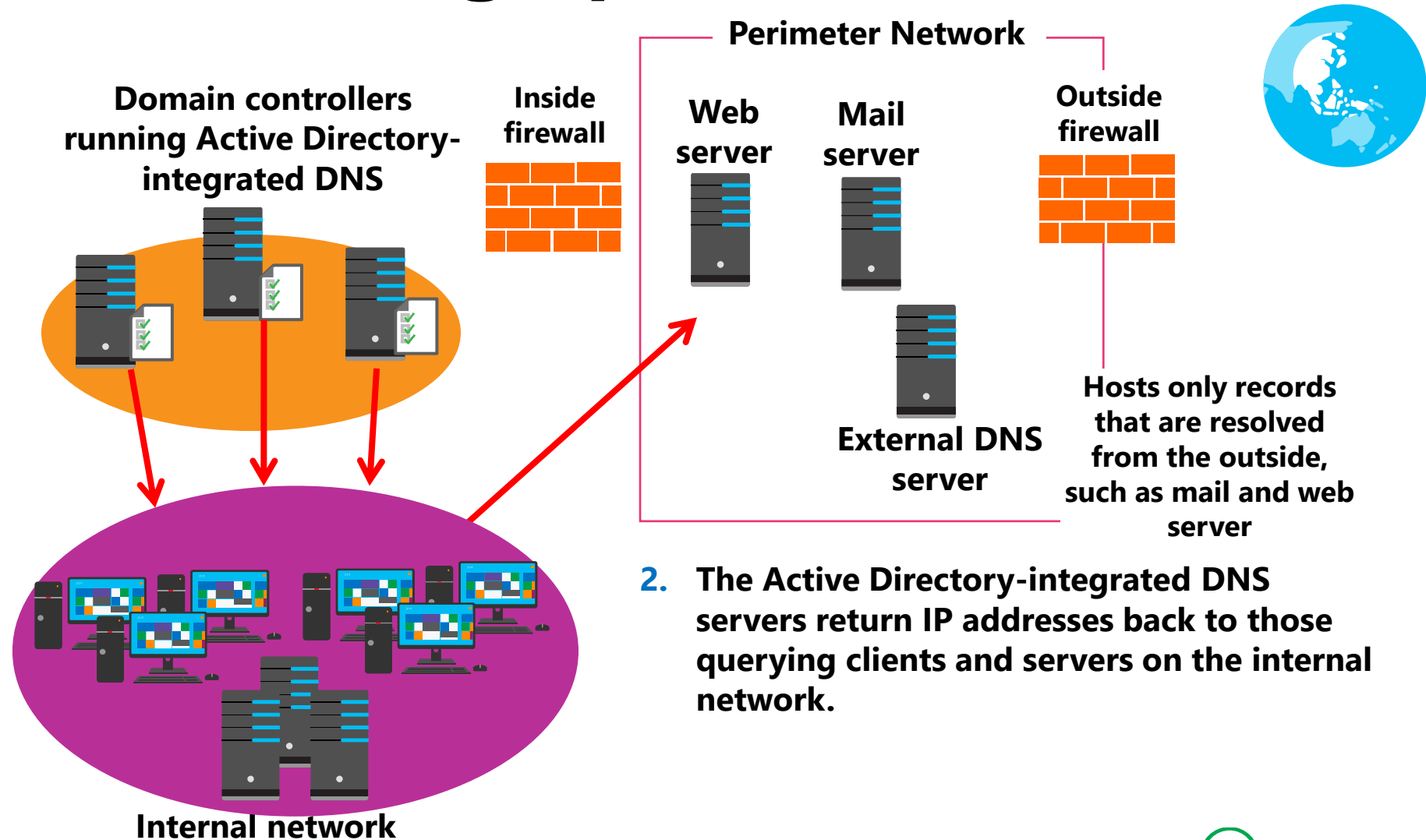
In this demonstration, you will learn how to create a GlobalNames zone

Understanding split DNS



1. Clients and servers on the internal network send all DNS queries to Active Directory-integrated DNS servers.

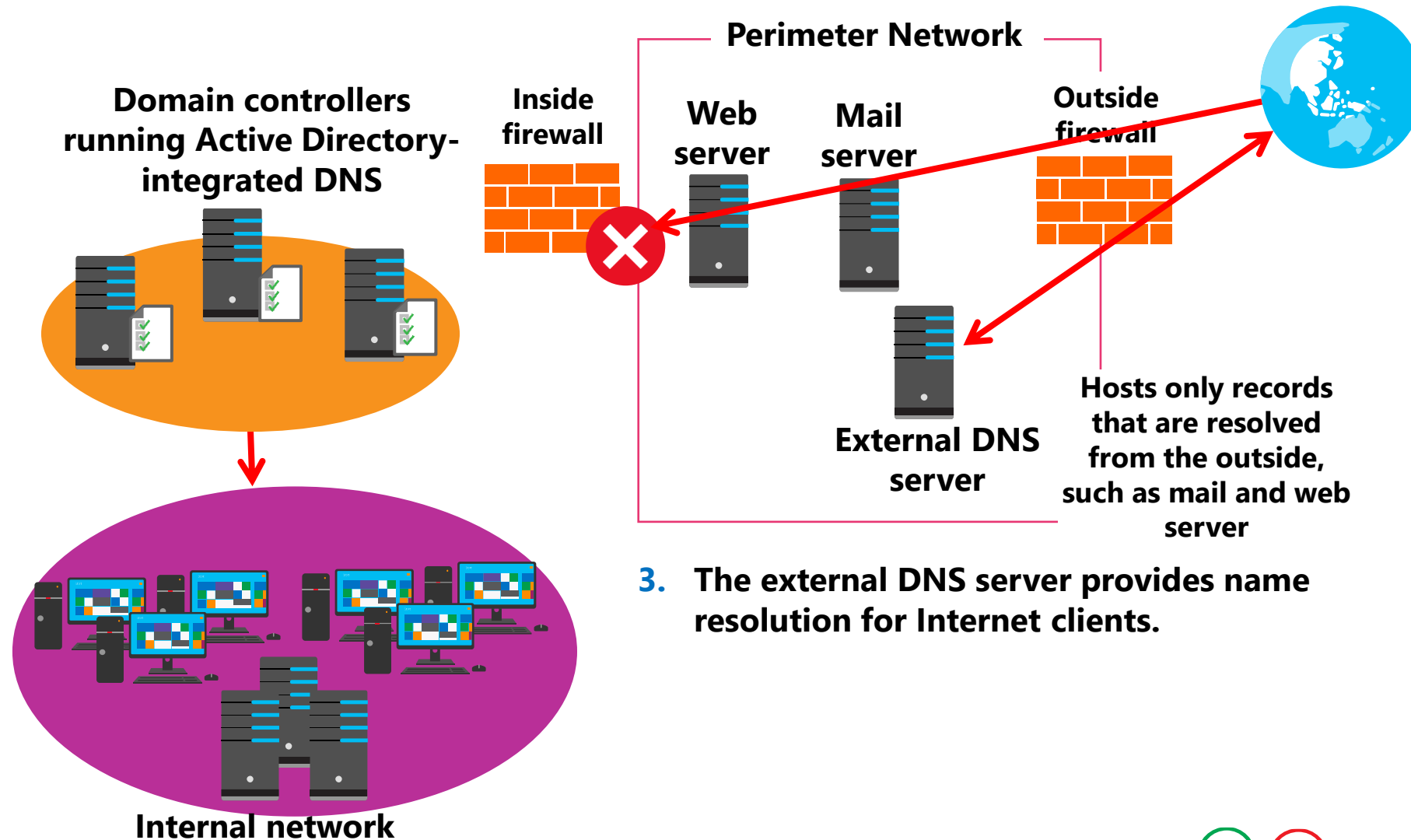
Understanding split DNS



2. The Active Directory-integrated DNS servers return IP addresses back to those querying clients and servers on the internal network.



Understanding split DNS



Implementing split DNS

- Same namespace:
 - Internal records should not be available externally
 - Records might need to be synchronized between internal and external DNS
- Unique namespace:
 - Record synchronization is not required
 - Existing DNS infrastructure is unaffected
 - Clearly delineates between internal and external DNS
- Subdomain:
 - Record synchronization is not required
 - Contiguous namespace is easy to understand

DNS policies

- DNS policy scenarios:
 - Application high availability
 - Traffic management
 - Split brain DNS
 - Filtering
 - Forensics
- DNS policy objects:
 - Client subnet
 - Recursion scope
 - Zone scope
- Use Windows PowerShell to create and manage DNS policies

Demonstration: Configuring DNS policies

In this demonstration, you will learn how to create a DNS policy that returns a different server address that depends upon the client location

Implementing DNS security

DNS Security Feature	Description
DNS cache locking	Prevents entries in cache being overwritten until a certain percentage of TTL has expired
DNS socket pool	Randomizes the source port for issuing DNS queries. Enabled by default in Windows Server 2012
DANE	Uses TLSA records that state the CA from which they should expect a certificate
DNSSEC	Enables cryptographically signing DNS records so that client computers can validate responses
RRL	Ignores DDOS queries or replies to them in truncation requiring a three-way handshake in TCP
Unknown Record Support	Will not do any record-specific processing for the unknown records, but will send them back in responses if queries are received

Implementing DNSSEC

DNSSEC functions as follows:

- If a zone has been digitally signed, a query response will contain digital signatures
- DNSSEC uses trust anchors, which are special zones that store public keys associated with digital signatures
- Resolvers use trust anchors to retrieve public keys and build trust chains
- DNSSEC requires trust anchors to be configured on all DNS servers participating in DNSSEC
- DNSSEC uses the NRPT, which contains rules that control the requesting client computer behavior for sending queries and handling responses

Demonstration: Configuring DNSSEC

In this demonstration, you will learn how to use the Zone Signing Wizard in the DNS Manager console to configure DNSSEC

Managing DNS clients

Cmdlet	Description
Get-DnsClient	Gets details about a network interface on a computer
Set-DnsClient	Set DNS client configuration settings for a network interface
Get-Dns ClientServerAddress	Gets the DNS server address settings for a network interface
Set-Dns ClientServerAddress	Sets the DNS server address for a network interface
Get-DnsClient	Gets details about a network interface on a computer

- `Set-DnsClient -InterfaceAlias Ethernet -ConnectionSpecificSuffix "adatum.com"`

References

- For more information, refer to the following links:
 - [Manage Servers with Windows Admin Center](#)
 - [DhcpServer](#)
 - [DNS Policy Scenario Guide](#)
 - [Publishing Applications with SharePoint, Exchange and RDG](#)

Hvala na pažnji!

