Module 4

Implementing DNS

Module Overview

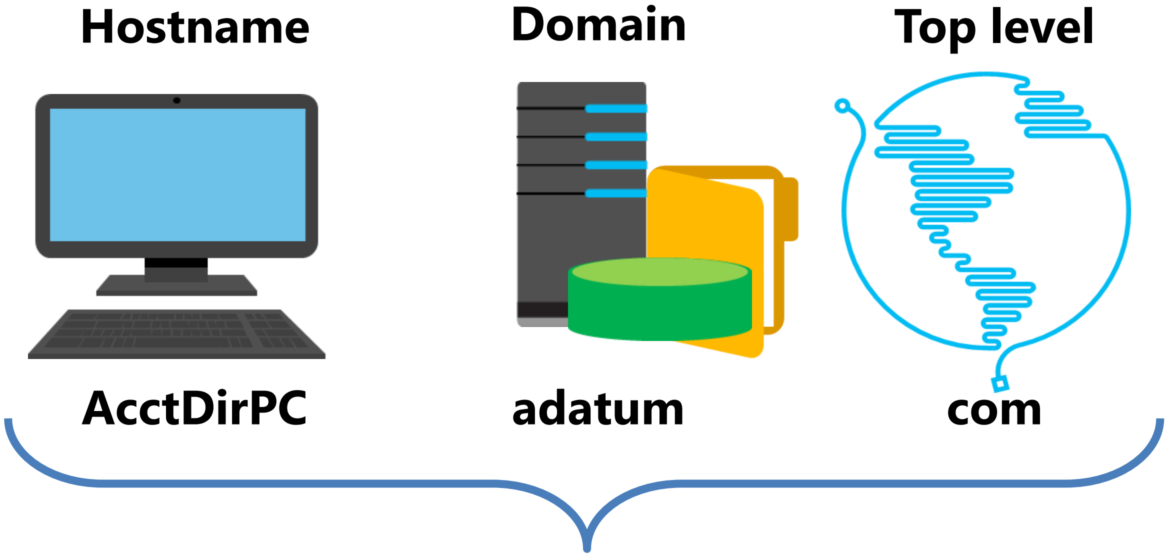
- Implementing DNS servers
- Configuring zones in DNS
- Configuring name resolution between DNS zones
- Configuring DNS integration with AD DS
- Configuring advanced DNS settings

Lesson 1: Implementing DNS servers

- How does DNS name resolution work?
- DNS components
- What are DNS zones and records?
- Demonstration: Installing and configuring the DNS role
- Configuring DNS clients
- Tools and techniques for troubleshooting name resolution
- Managing DNS services
- Demonstration: Troubleshooting name resolution
- Testing DNS servers
- Demonstration: Testing the DNS 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)



Hostname

Domain

Top level

AcctDirPC

adatum

com

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?

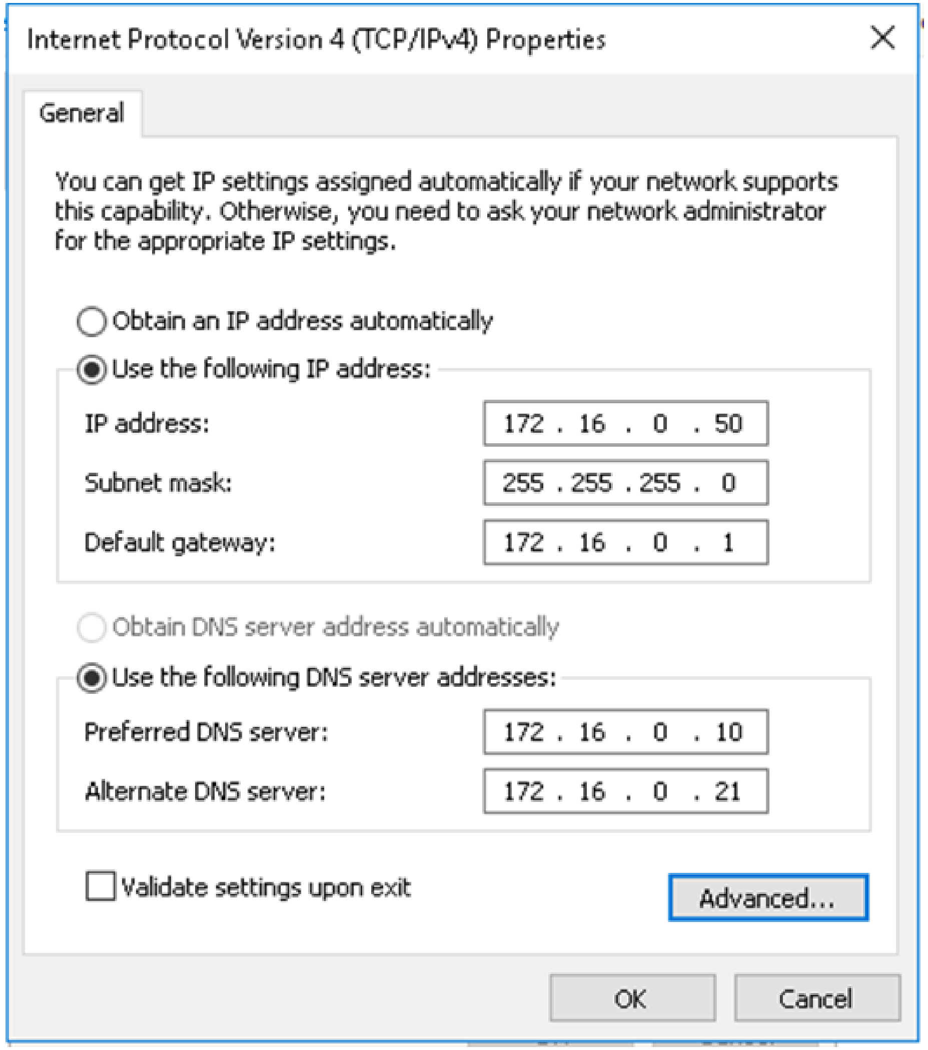
- A DNS zone is a specific portion of DNS namespace that contains DNS records
- Zone types:
  - Forward lookup zone
  - Reverse lookup zone
- Resource records in forward lookup zones include: A, MX, SRV, NS, SOA, and CNAME
- Resource records in reverse lookup zones include: PTR

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 16 . 0 . 50

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 0 . 1

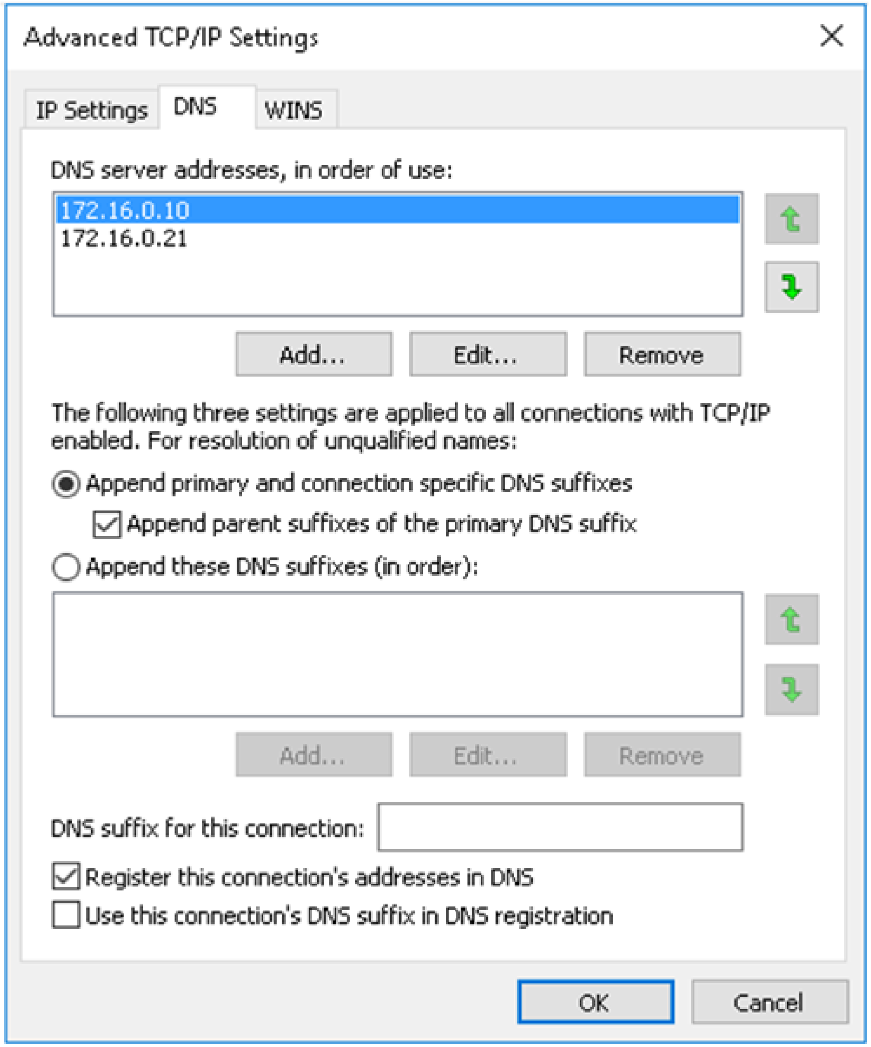
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 0 . 10

Alternate DNS server: 172 . 16 . 0 . 21

□ Validate settings upon exit



Advanced TCP/IP Settings

IP Settings | DNS | WINS

DNS server addresses, in order of use:

172.16.0.10
172.16.0.21

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

```
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 **dnscmd** or by using Windows PowerShell
  - Copy or back up primary zone files that are not using AD DS integration

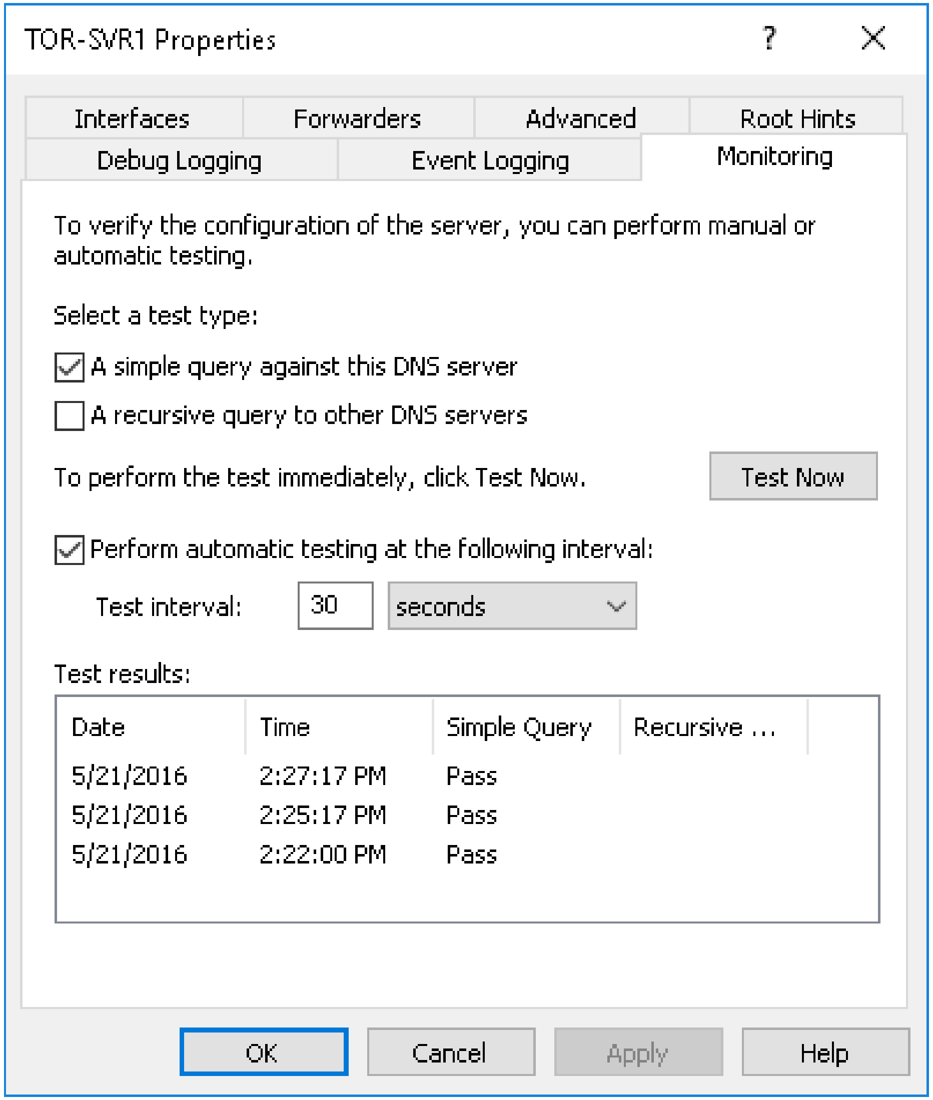
Demonstration: Troubleshooting name resolution

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



To verify the configuration of the server, you can perform manual or automatic testing.

Select a test type:

☑ A simple query against this DNS server

☐ A recursive query to other DNS servers

To perform the test immediately, click Test Now.

☑ Perform automatic testing at the following interval:

Test interval: 30 seconds

Test results:

Date	Time	Simple Query	Recursive ...
5/21/2016	2:27:17 PM	Pass	
5/21/2016	2:25:17 PM	Pass	
5/21/2016	2:22:00 PM	Pass	

Demonstration: Testing the DNS server

In this demonstration, you will learn how to:

- Test the DNS server
- Configure auditing and analytical logging of events

Lesson 2: Configuring zones in DNS

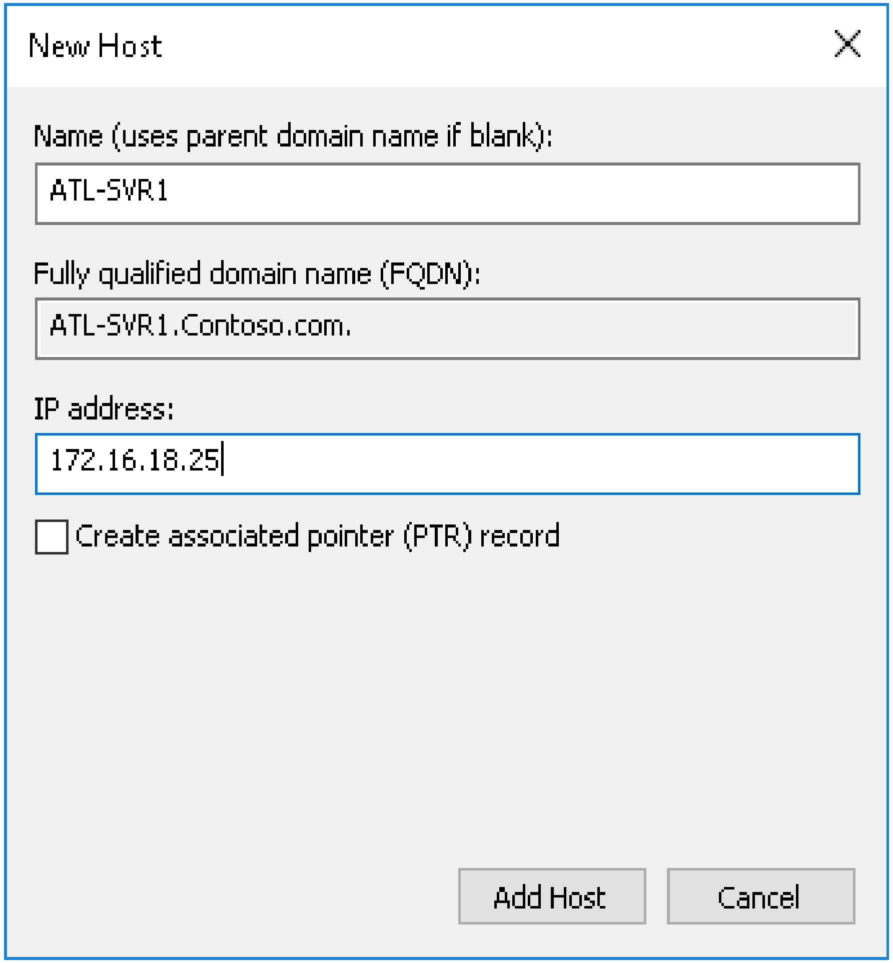
- DNS resource record types
- Creating records in DNS
- Configuring DNS zones
- What are primary and secondary zones?
- Configuring zone replication

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



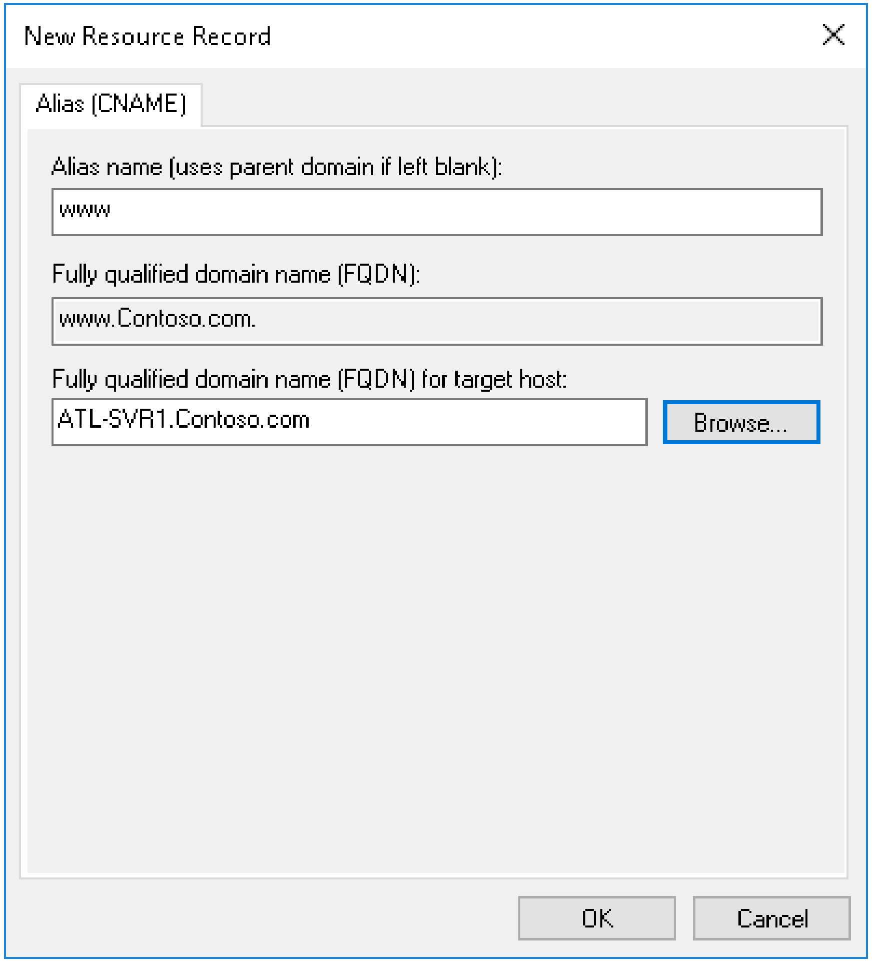
New Host

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



New Resource Record

Alias (CNAME)

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

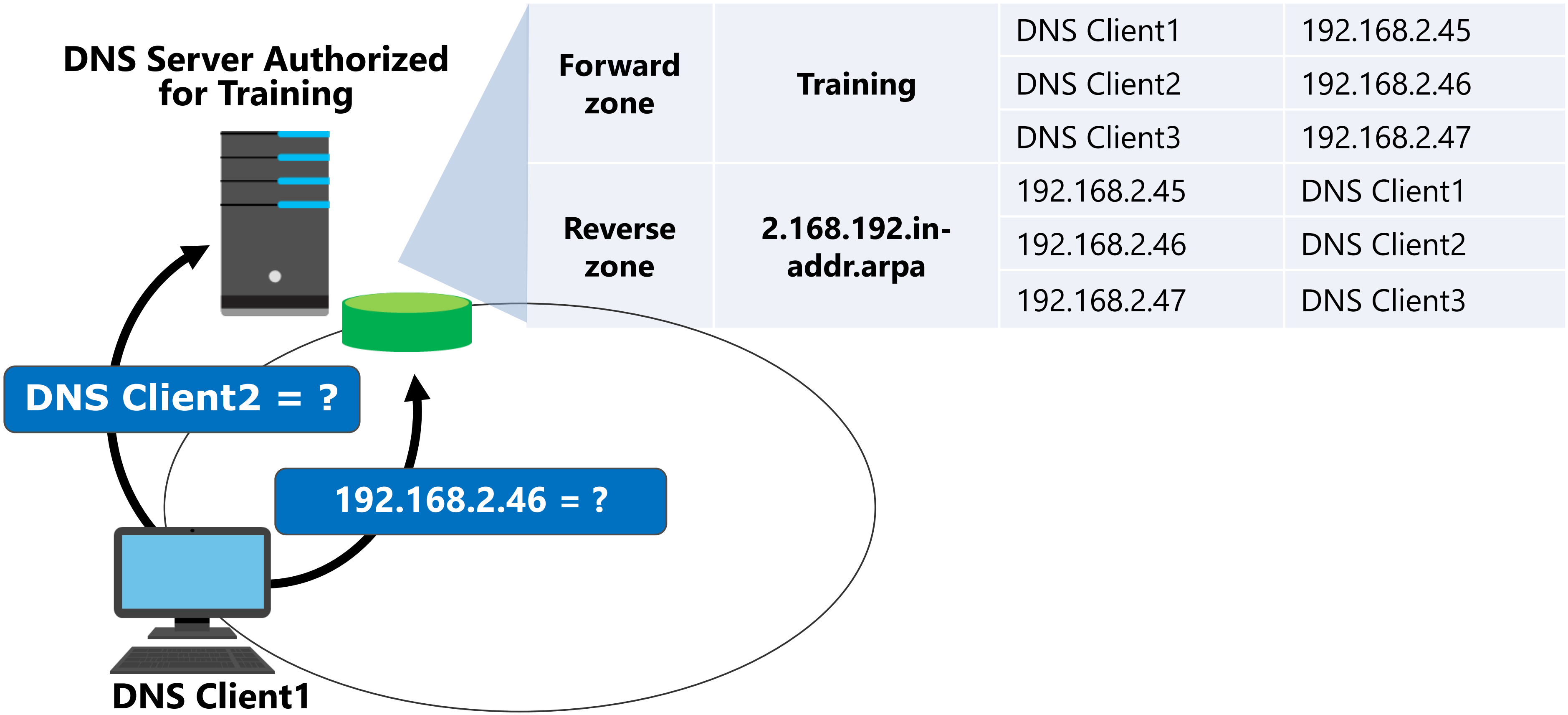
Fully qualified domain name (FQDN): www.Contoso.com.

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

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

Configuring DNS zones

Namespace: training.contoso.com

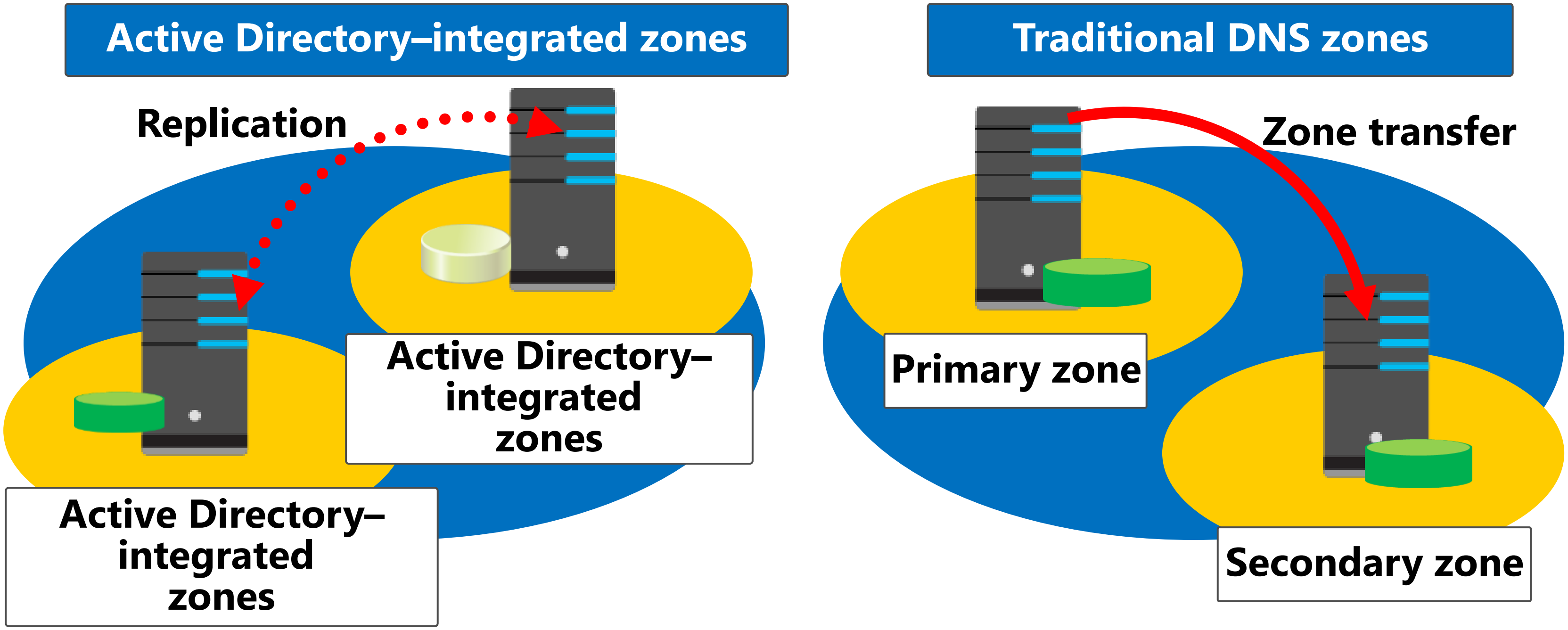


Forward zone	**Training**	DNS Client1	192.168.2.45
		DNS Client2	192.168.2.46
		DNS Client3	192.168.2.47
Reverse zone	**2.168.192.in-addr.arpa**	192.168.2.45	DNS Client1
		192.168.2.46	DNS Client2
		192.168.2.47	DNS Client3

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

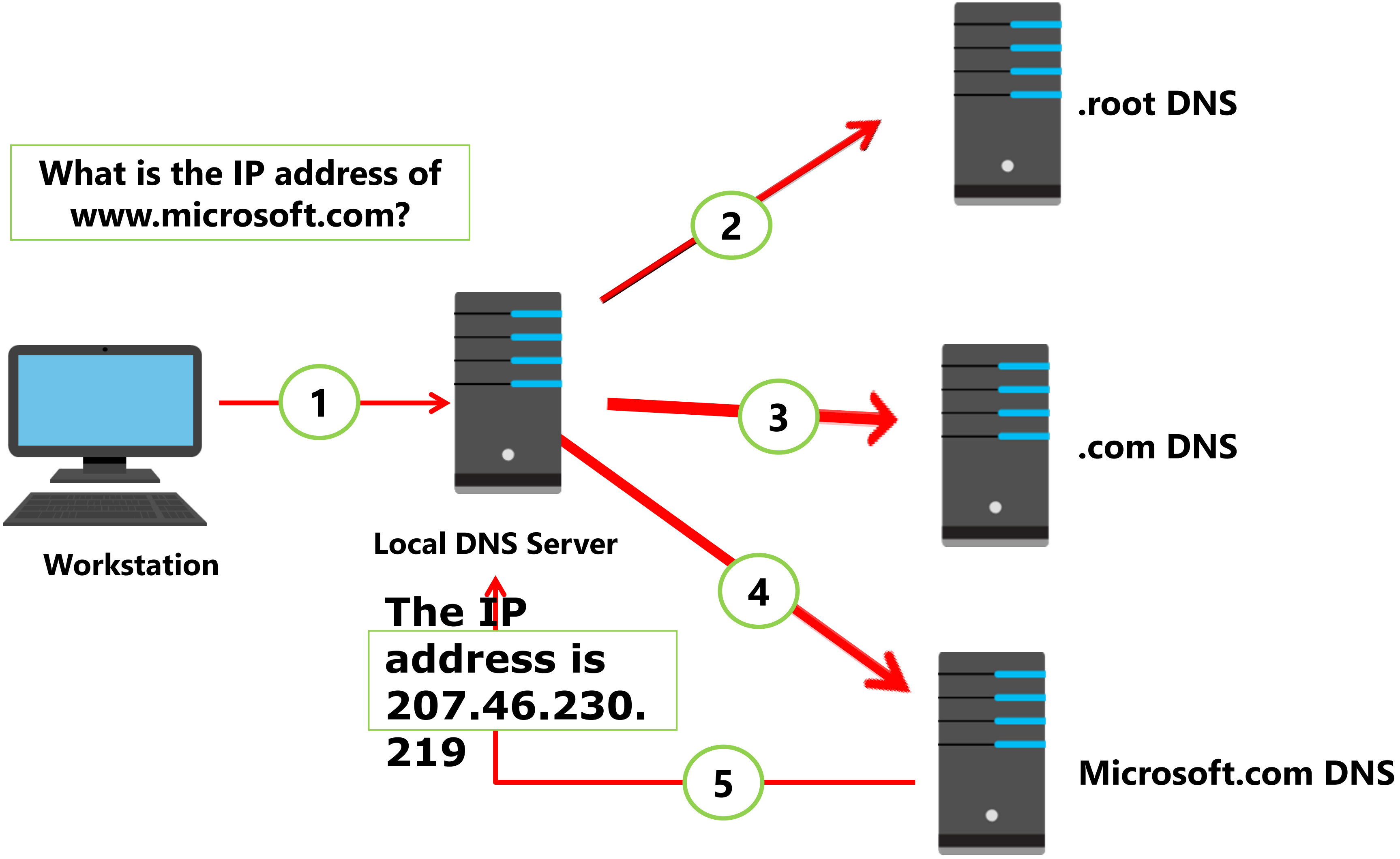

Active Directory–integrated zones
Traditional DNS zones
Replication
Zone transfer
Active Directory–integrated zones
Active Directory–integrated zones
Primary zone
Secondary zone

Zones	Description
Active Directory–integrated zones	• Perform incremental replication between DNS servers • Adjust the Active Directory replication schedule
Traditional DNS zones	• Replicate between primary and secondary zones • Perform an incremental rather than a complete zone transfer

Lesson 3: Configuring name resolution between DNS zones

- Resolving DNS names between zones
- What is a stub zone?
- What is DNS caching?
- What is DNS forwarding?
- DNS forwarding and stub zone guidance
- Discussion: When to use DNS forwarding
- Configuring delegation

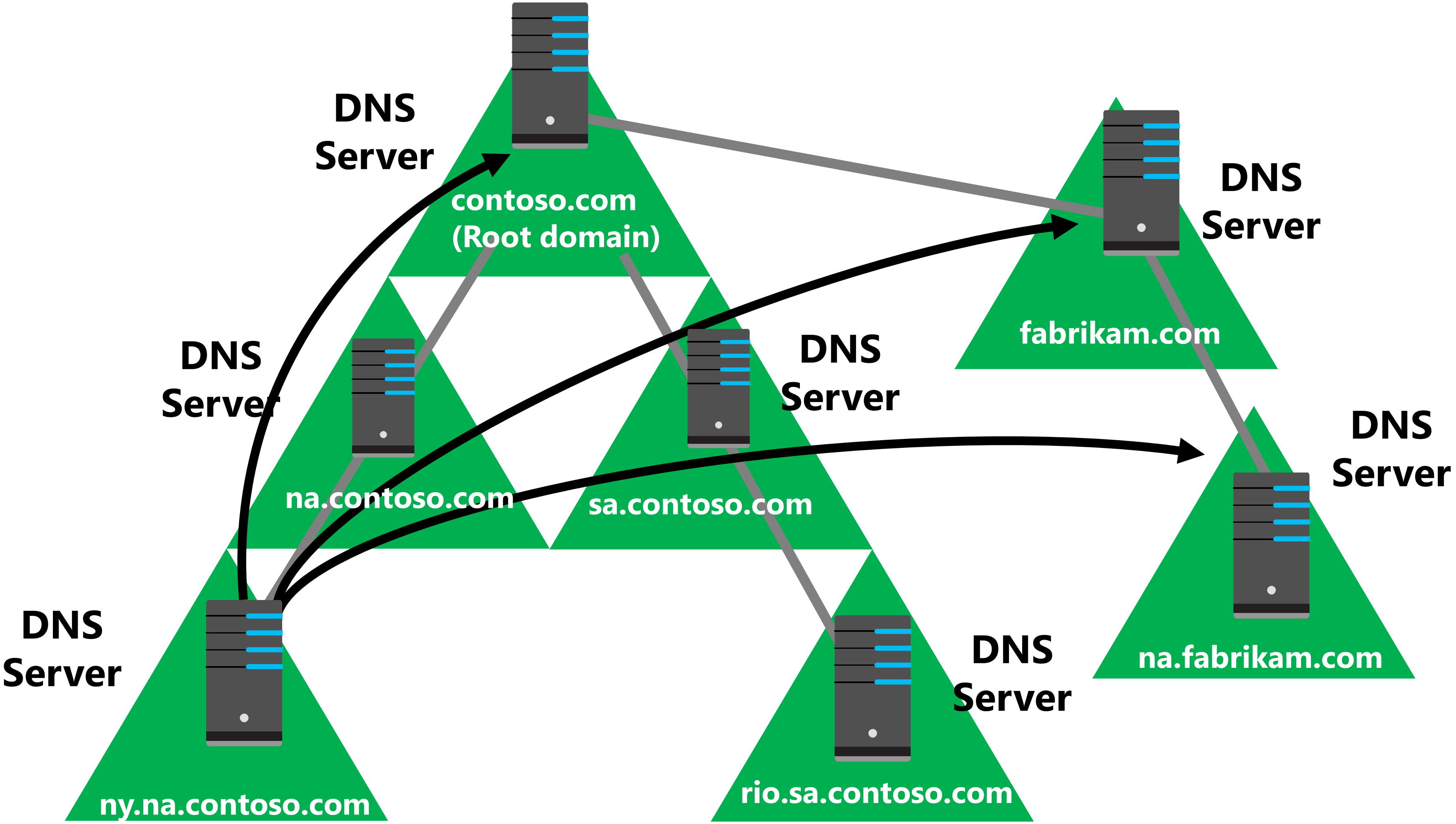
Resolving DNS names between zones



What is the IP address of www.microsoft.com?
Workstation
1
Local DNS Server
2
.root DNS
3
.com DNS
4
Microsoft.com DNS
5
The IP address is 207.46.230.219

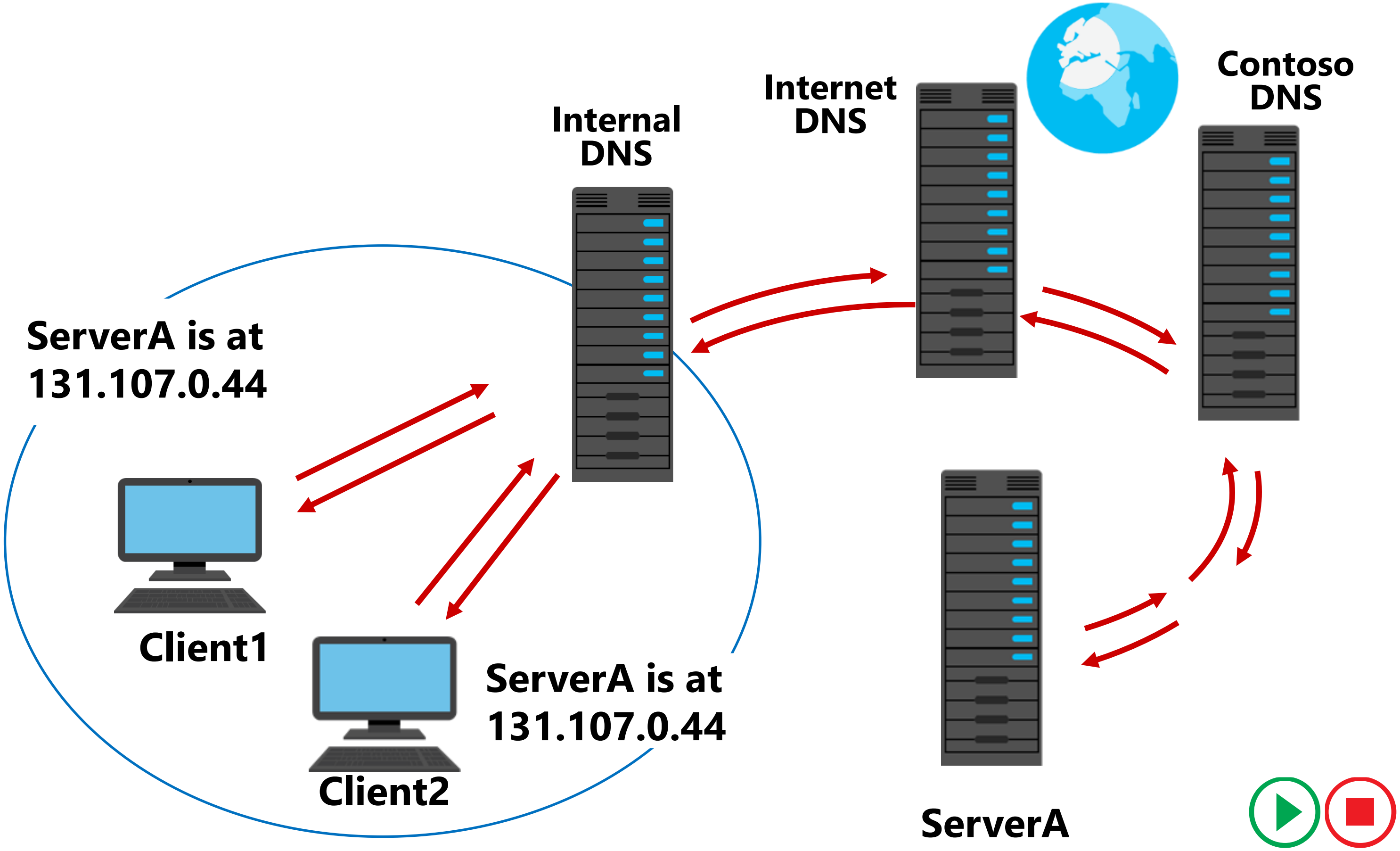
What is a stub zone?

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



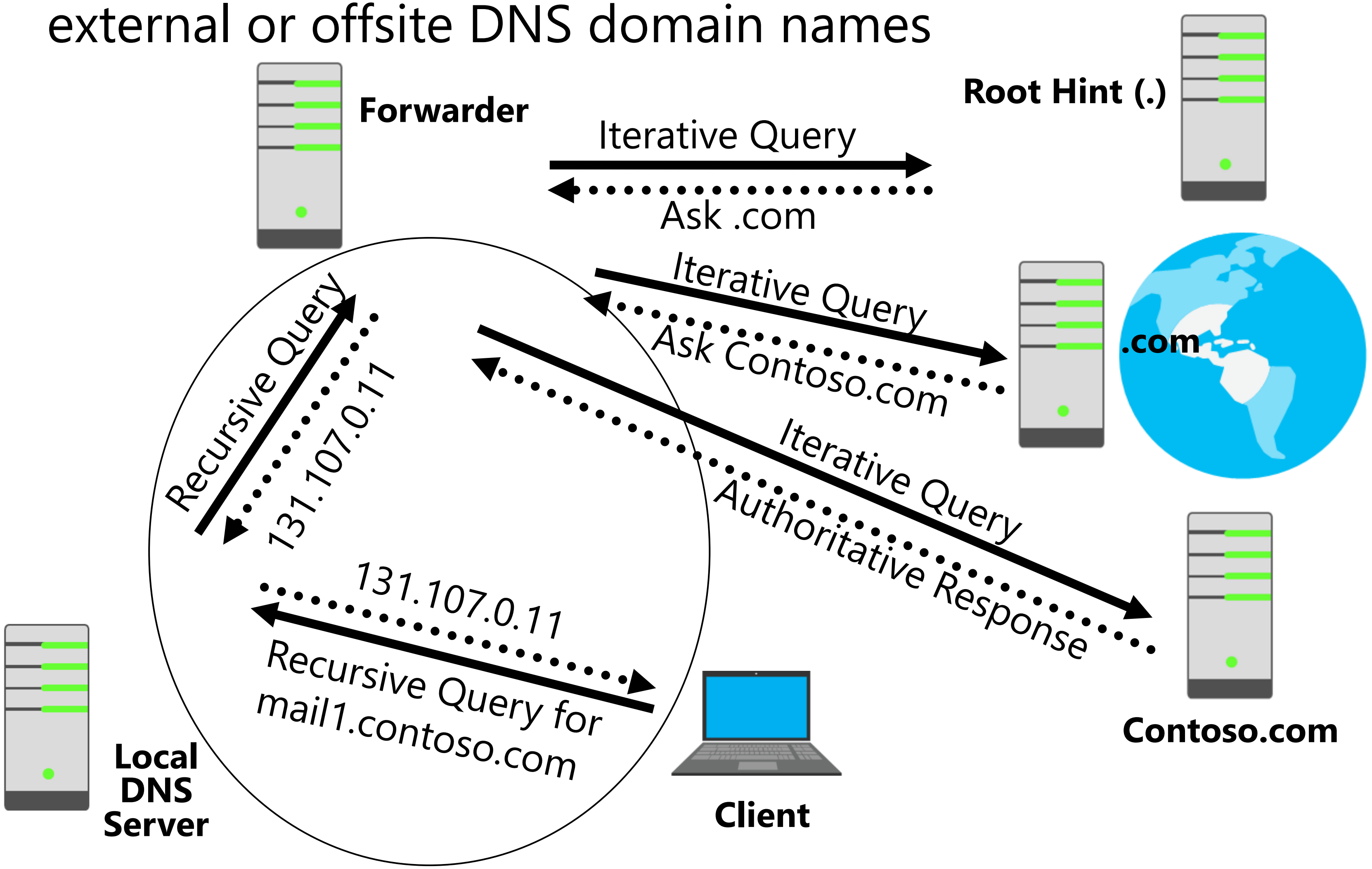
What is DNS caching?

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

Discussion: When to use DNS forwarding

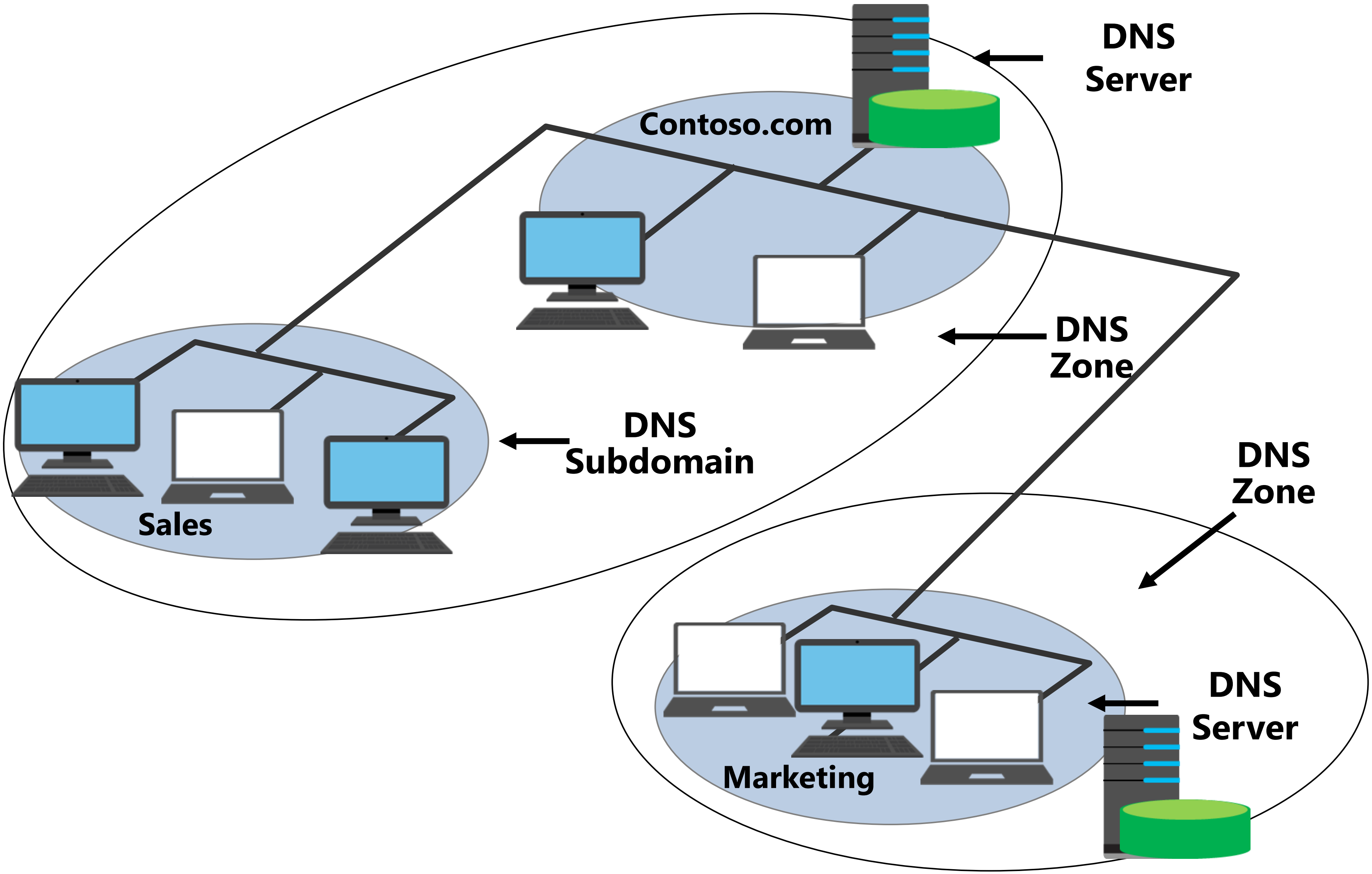
What DNS resolution method do you use?

Scenario 1: Northwind Traders Inc., has recently acquired the Beyond Blue Airline Corporation and you are tasked with setting up the DNS infrastructure. You will have an Active Directory Domain Services (AD DS) forest named Northwind.com, and a separate tree named Beyondblueair.com. Users will regularly need to resolve names to IP addresses for servers within each domain name. You want to ensure that the DNS queries remain within the corporate infrastructure.

Scenario 2: Contoso LTD has diversified into several product lines, and the AD DS domain structure is being extended. Contoso.com has three existing sub domains: NA.contoso.com, EU.contoso.com and Asia.contoso.com. Plans are under way to create sub domain in each of the geographical domains, with an automotive domain under each with a two separate subdomains under each automotive domain. You need to ensure the faster possible name resolution path for internal clients.

10 minutes

Configuring delegation



Lab A: Planning and implementing name resolution by using DNS

- Exercise 1: Planning DNS name resolution
- Exercise 2: Implementing DNS servers and zones

Logon Information

Virtual machines:	**20741A-LON-DC1**
	20741A-EU-RTR
	20741A-INET
	20741A-LON-SVR1
	20741A-SYD-SVR1
User name:	**Adatum\Administrator**
Password:	**Pa$$w0rd**

Estimated Time: 60 minutes

Lab Scenario

Users in the A. Datum Corporation's Sydney office have been complaining about slowness and errors when connecting to internal and external websites and servers. Currently, the Sydney office only hosts client computers. Wide area network (WAN) communication between Sydney and London, where infrastructure servers are hosted, has been intermittent and is the primary cause of the issues. You have been asked to implement DNS infrastructure in Sydney by using one server that will resolve the majority of these issues.

The current DNS structure for A. Datum Corporation is as follows:

- Your Internet service provider's DNS server (131.107.0.100) provides DNS resolution and forwarding for Internet-based domain names.
- The Contoso.com domain namespace hosts web and mail services that are accessible from the Internet. These servers are also accessible from inside the A. Datum Corporation network.
- The Treyresearch.net namespace contains resources used by A. Datum Corporation employees. However, the DNS records for the Treyresearch.net zone are not located on the DNS server that clients are configured to use. They are located on **LON-SVR1**.
- **LON-DC1** provides DNS resolution for Adatum.com.

Lab Scenario (Continued)

You must configure a DNS server in the Sydney location to enable more efficient name resolution for Sydney clients. The DNS server must resolve queries for local clients, and provide access to name resolution for the Internet sites, as provided by **LON-SVR1**. Sydney clients should be forwarded to an authoritative server for Adatum.com to resolve internal queries.

The requirements are as follows:

- Configuring forwarding for all DNS lookups for Internet access from Sydney to your ISP's DNS server
- Configuring conditional forwarding on **SYD-SVR1** for the Treyresearch.net zone
- Hosting and resolving queries for the Adatum.com domain within the Sydney location

Lab Scenario (Continued)

The virtual machines used in this lab provide the following services:

- **INET** (131.107.0.100). DNS server providing name resolution for Internet-based DNS names
- **LON-DC1** (172.16.0.10). Domain controller and DNS server hosting the Adatum.com namespace
- **LON-SVR1** (172.16.0.11). DNS server hosting the Treyresearch.net namespace
- **SYD-SVR1** (172.16.19.20). The server that you will configure with DNS to provide name resolution for client computers in Sydney

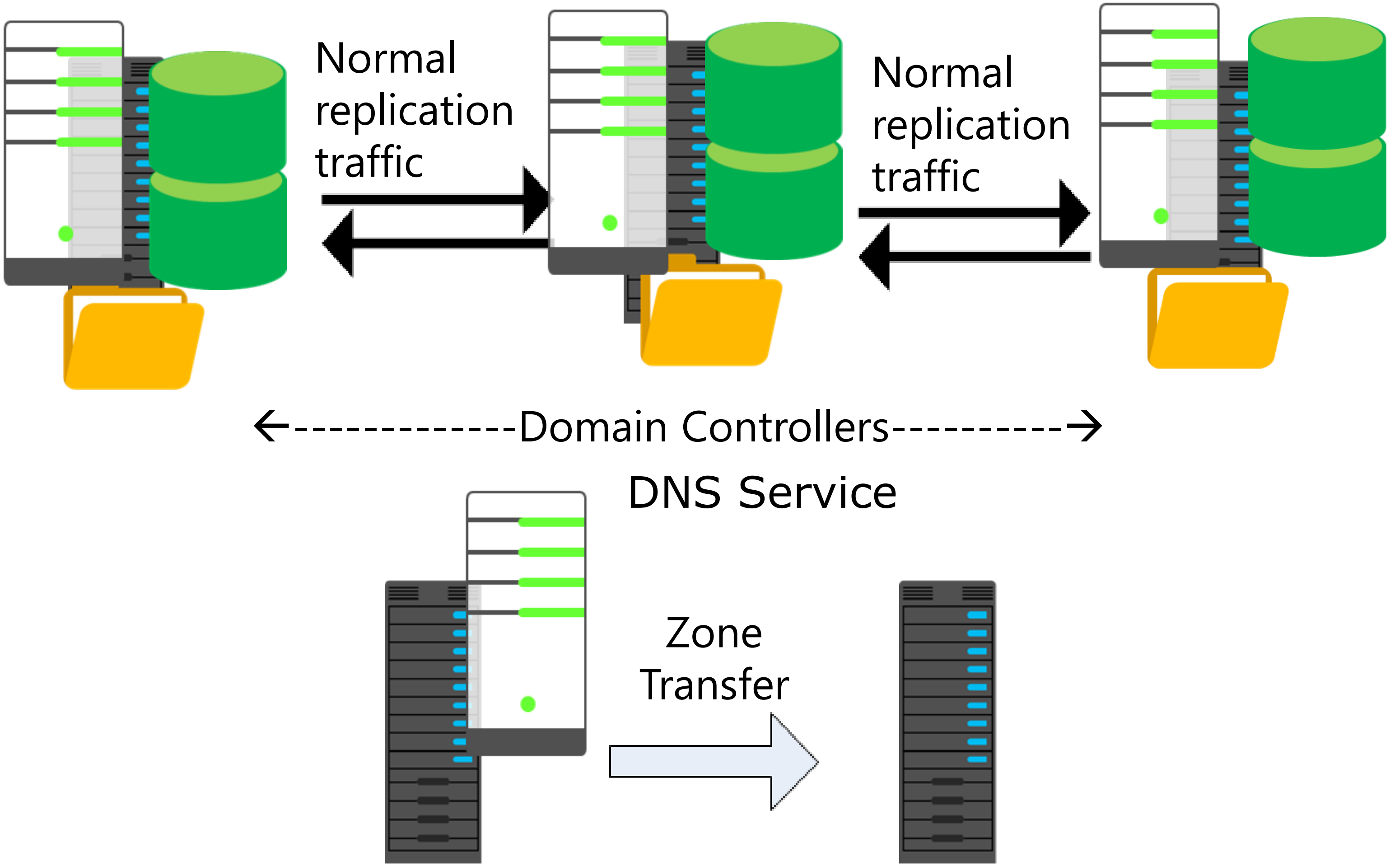
Lab Review

- Can you install the DNS Server role on a server that is not a domain controller? If yes, are there any limitations?
- What is the most common way to carry out Internet name resolution on a local DNS?
- How can you browse the content of the DNS resolver cache on a DNS server?

Lesson 4: 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



Normal replication traffic

Normal replication traffic

←-------------Domain Controllers----------→

DNS Service

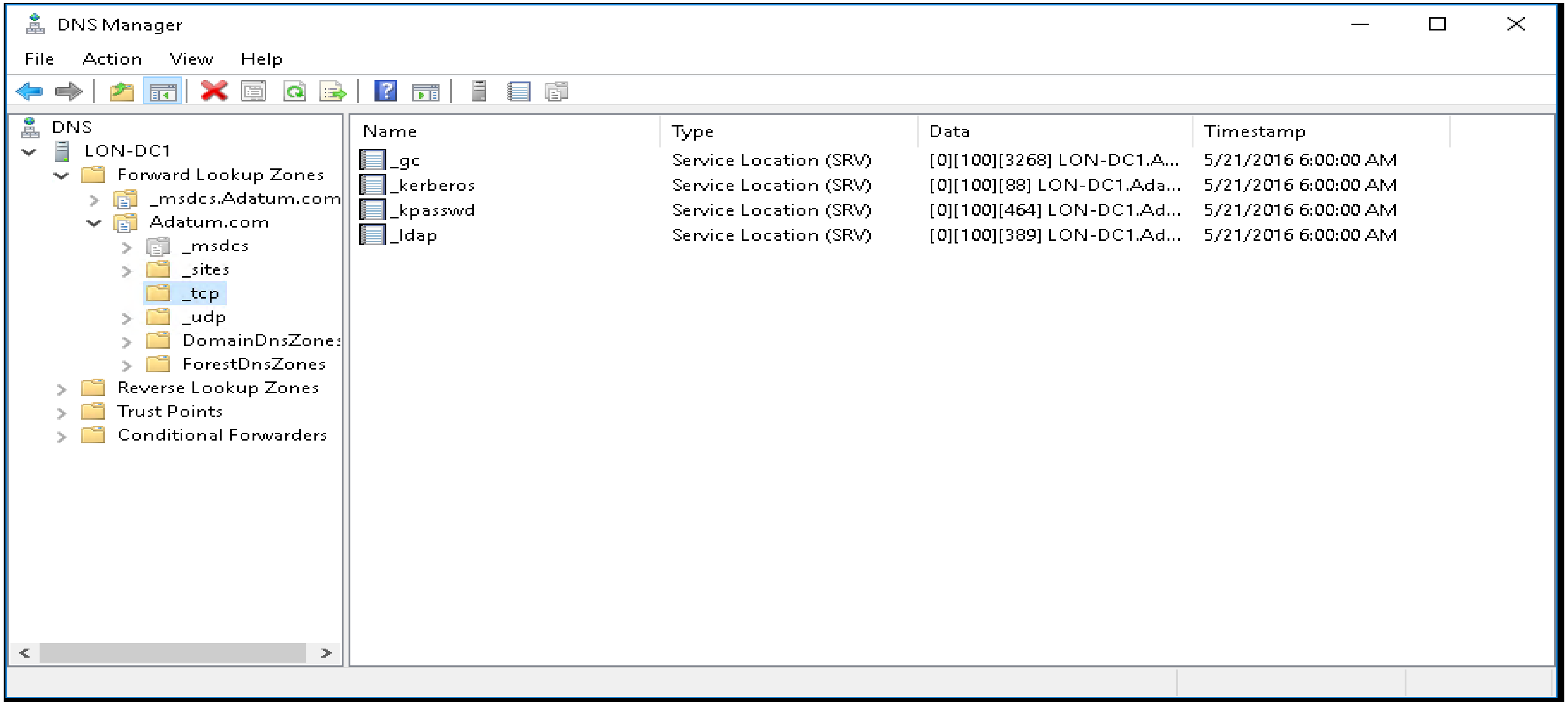
Zone Transfer

Primary DNS Server

Secondary DNS Server

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



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

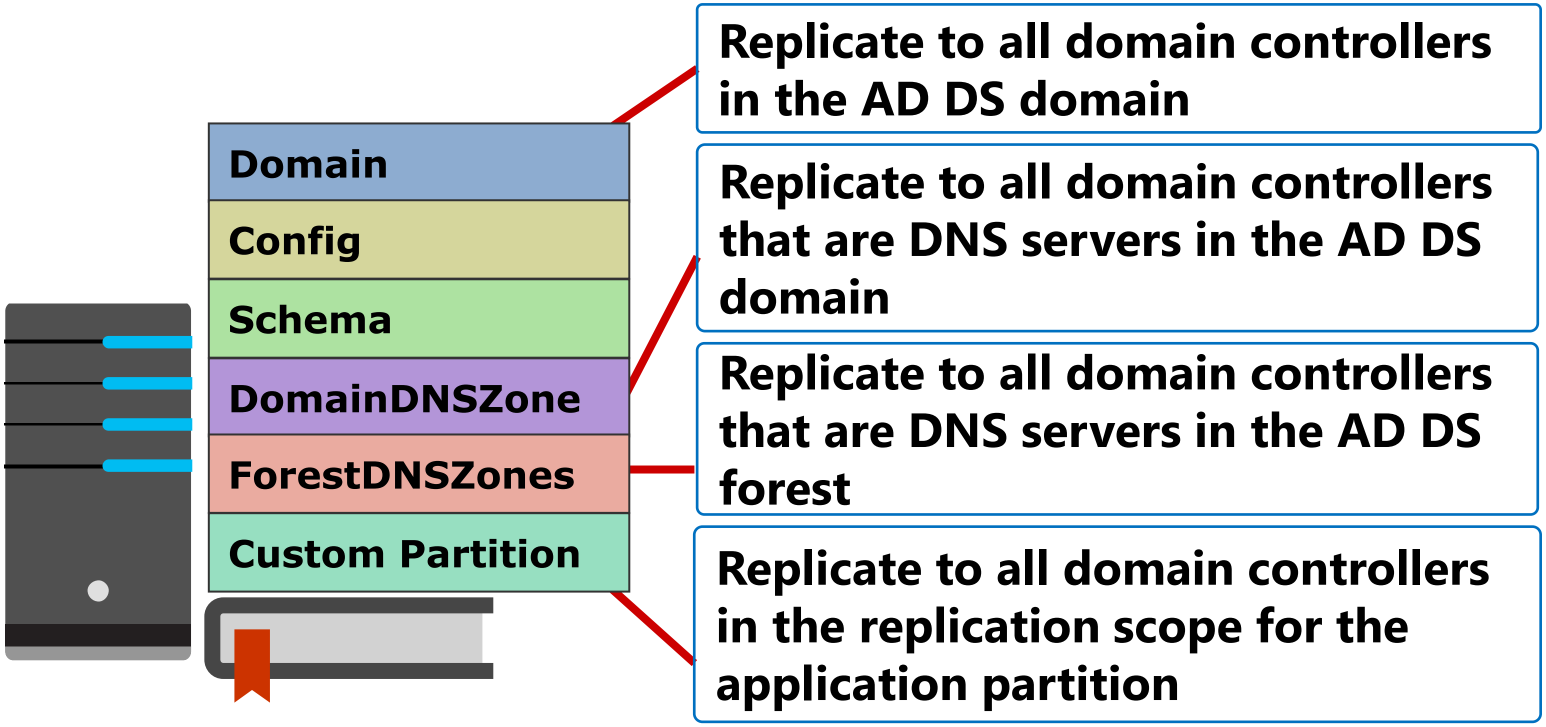
- Domain controllers register their SRV resource records dynamically, by service and site location
- Client systems in sites use SRV resource records recorded in a site to find domain controllers in their own site before attempting to connect to domain controllers across wide area network links
- Keeps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



- Domain
- Config
- Schema
- DomainDNSZone
- ForestDNSZones
- Custom Partition

Replicate to all domain controllers in the AD DS domain

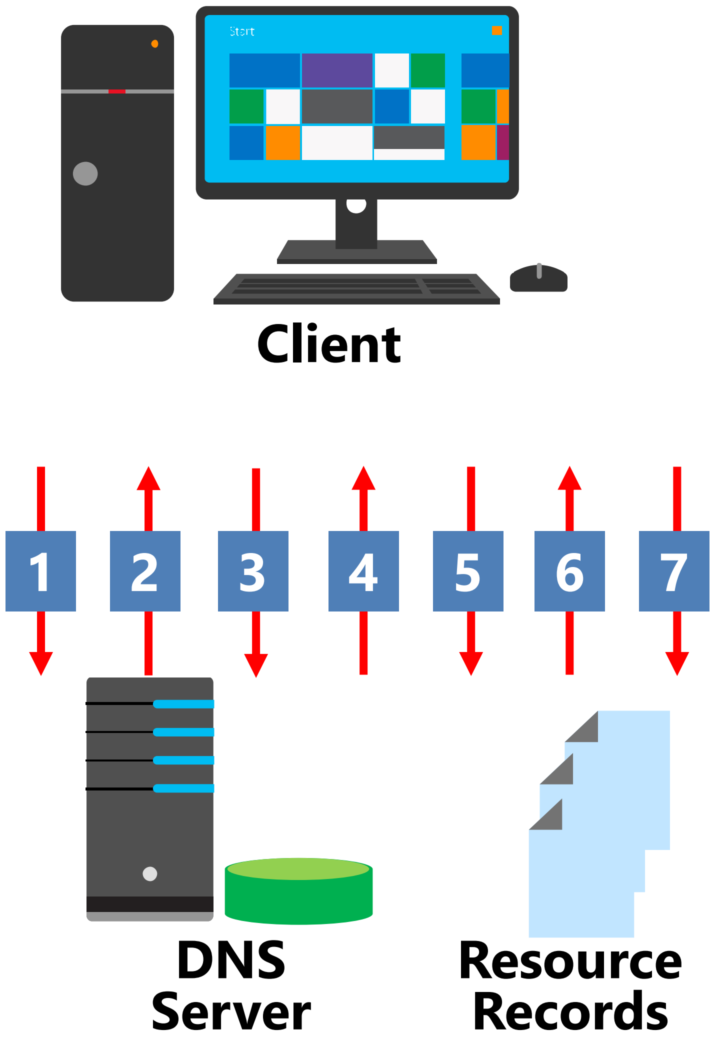
Replicate to all domain controllers that are DNS servers in the AD DS domain

Replicate to all domain controllers that are DNS servers in the AD DS forest

Replicate to all domain controllers in the replication scope for the application partition

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

Lab B: Integrating DNS with AD DS

- Exercise 1: Integrating DNS with AD DS

Logon Information

Virtual machines:	**20741A-LON-DC1** **20741A-LON-SVR1** **20741A-EU-RTR** **20741A-SYD-SVR1**
User name:	**Adatum\Administrator**
Password:	**Pa$$w0rd**

Estimated Time: 20 minutes

Lab Scenario

After making additional improvements to the WAN connection between London and Sydney locations, you have been asked to enable **SYD-SVR1** to update and replicate records for the Adatum.com domain.

Lab Review

- Why did you promote SYD-SVR1 to a domain controller?

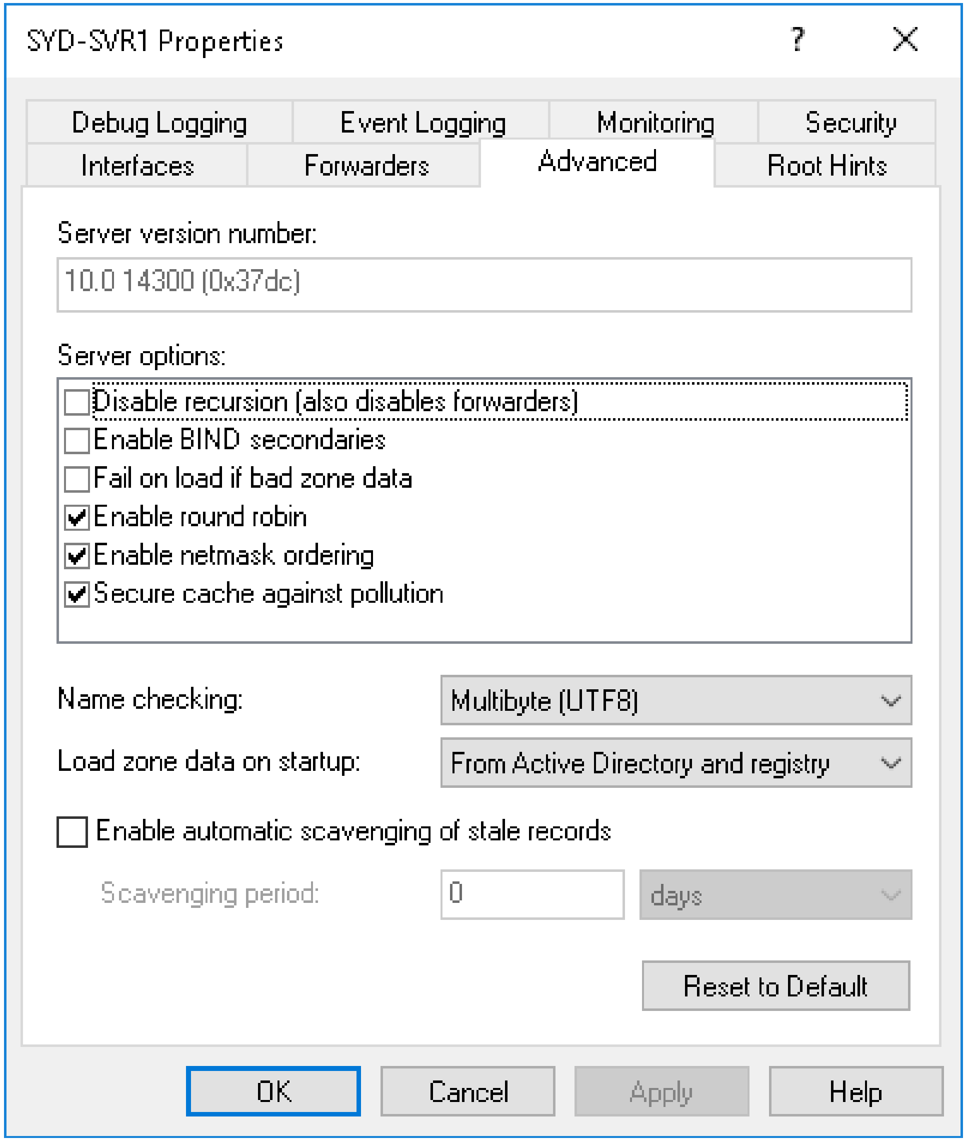
Lesson 5: Configuring advanced DNS settings

- Configuring advanced DNS name resolution
- Configuring root hints
- What is the GlobalNames zone?
- Demonstration: Configuring the GlobalNames zone
- Understanding split DNS
- Implementing split DNS
- DNS policies
- Demonstration: Configuring DNS policies
- Implementing DNS security
- Implementing DNSSEC
- Demonstration: Configuring DNSSEC
- DNS on Nano Server

Configuring advanced DNS name resolution

Advanced DNS name resolution:

- DNS round robin
- Netmask reordering
- Recursion



SYD-SVR1 Properties

Server version number:

10.0 14300 (0x37dc)

Server options:

☐ Disable recursion (also disables forwarders)
☐ Enable BIND secondaries
☐ Fail on load if bad zone data
☑ Enable round robin
☑ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

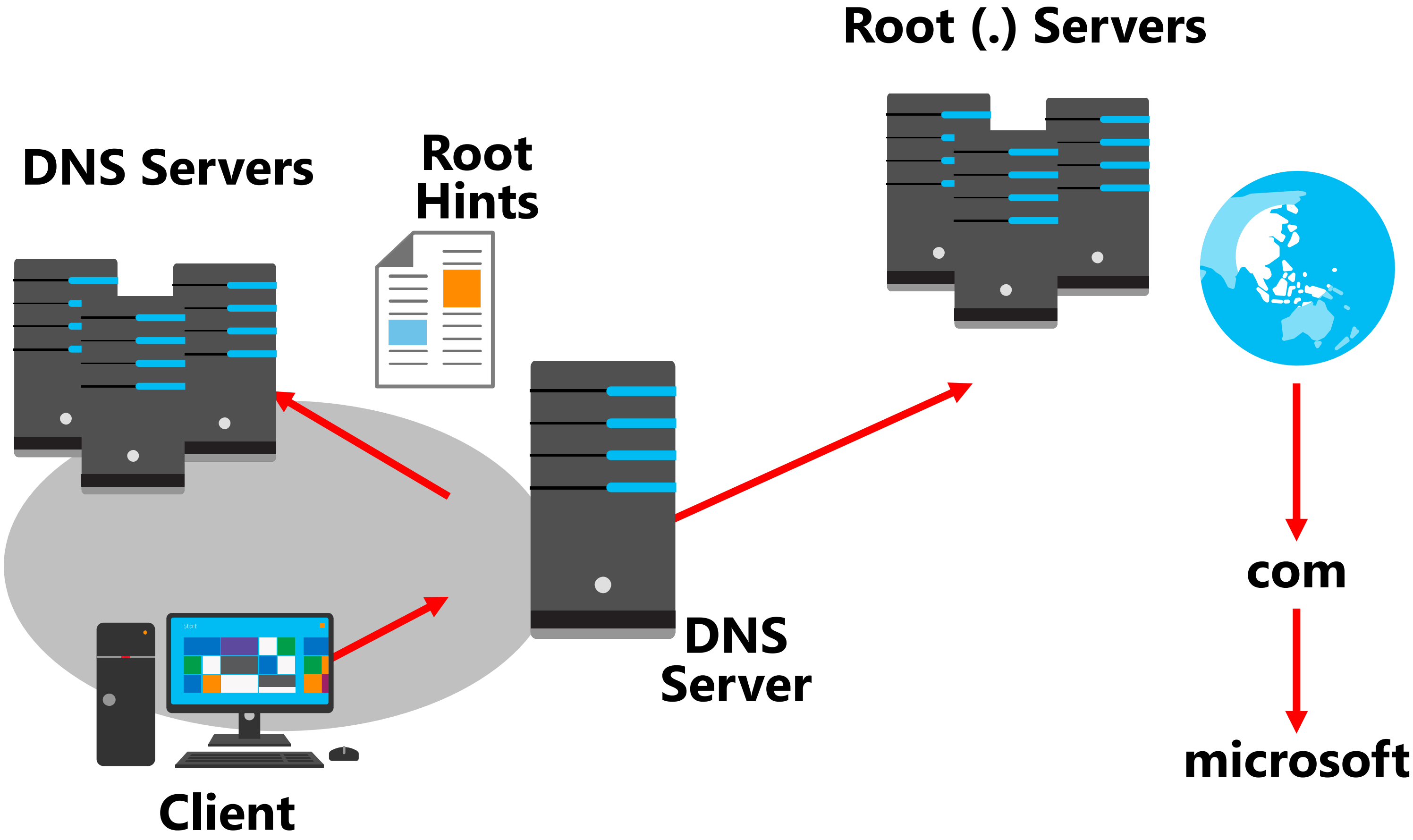
Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

Configuring root hints

Root hints **contain the IP addresses for DNS root servers**

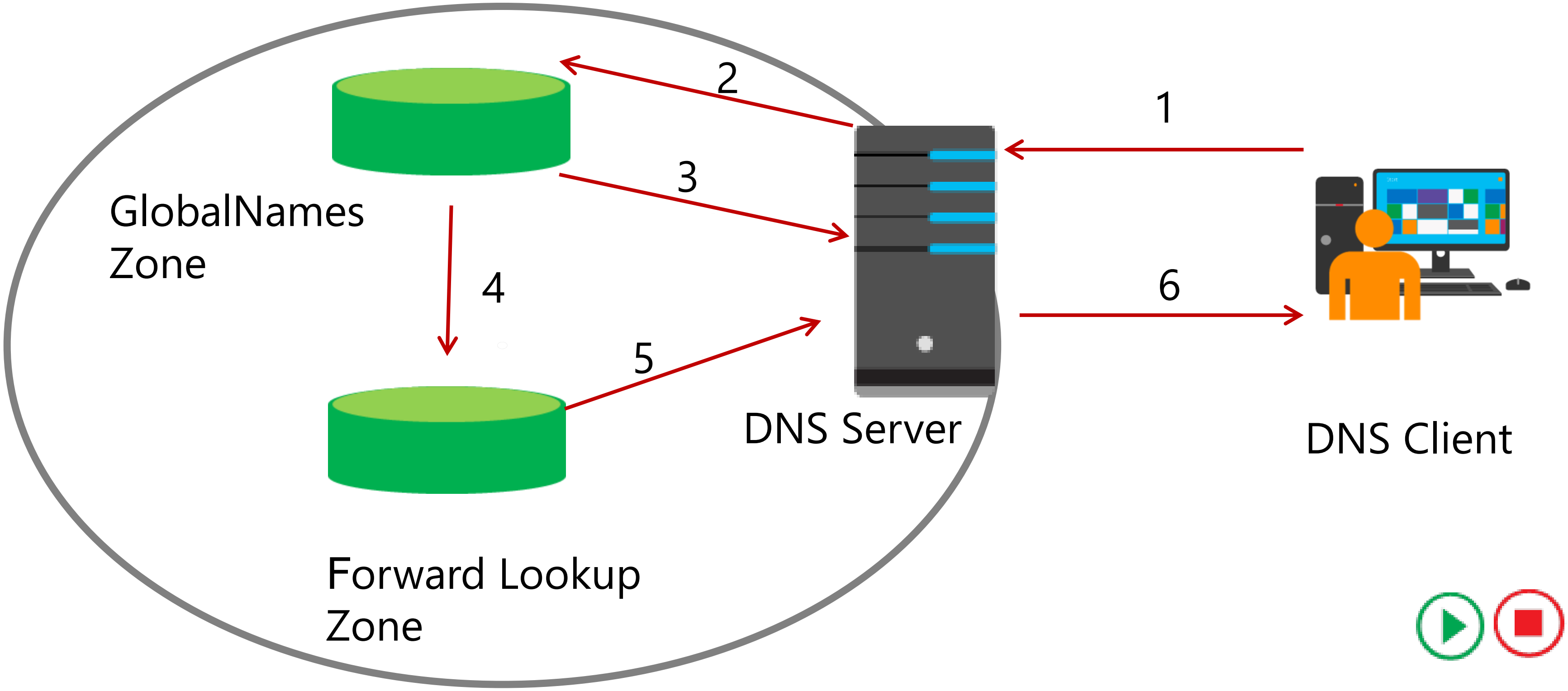


What is the GlobalNames zone?

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:

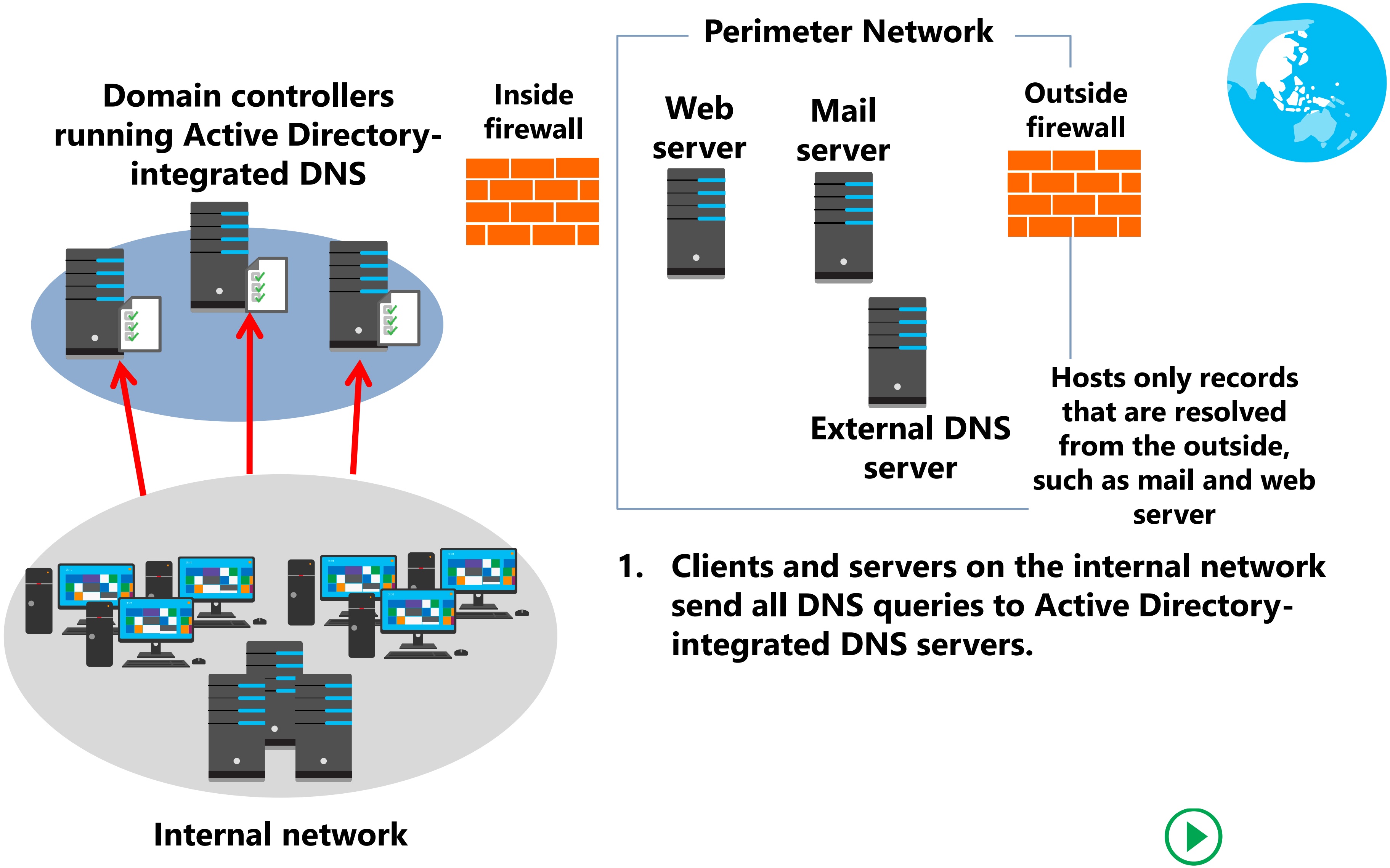
- **Get-DnsServerGlobalNameZone**
- **Set-DnsServerGlobalNameZone**



Demonstration: Configuring the GlobalNames zone

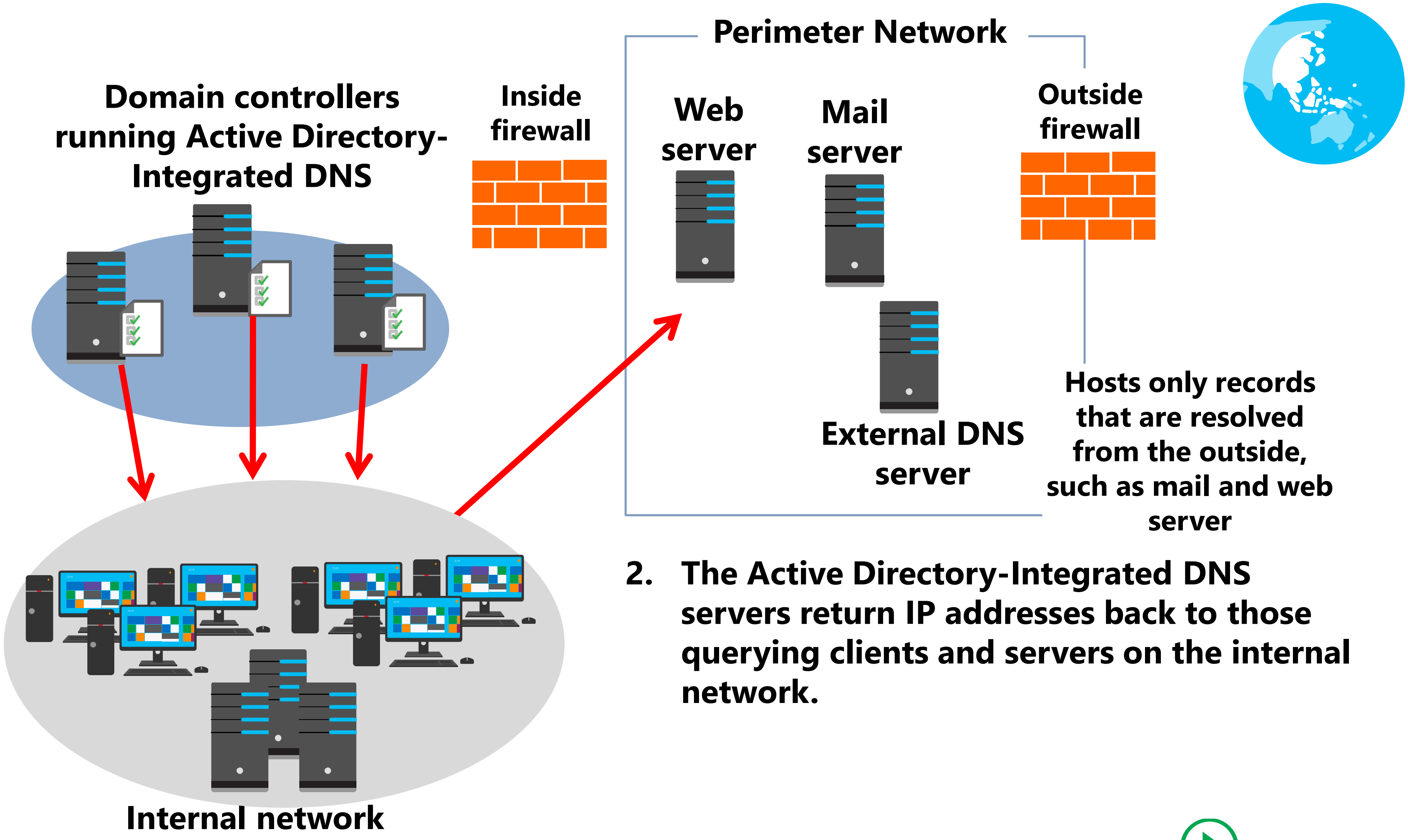
In this demonstration, you will learn how to create a GlobalNames zone

Understanding split DNS


Perimeter Network
Domain controllers running Active Directory-integrated DNS
Inside firewall
Web server
Mail server
Outside firewall
External DNS server
Hosts only records that are resolved from the outside, such as mail and web server
Internal network

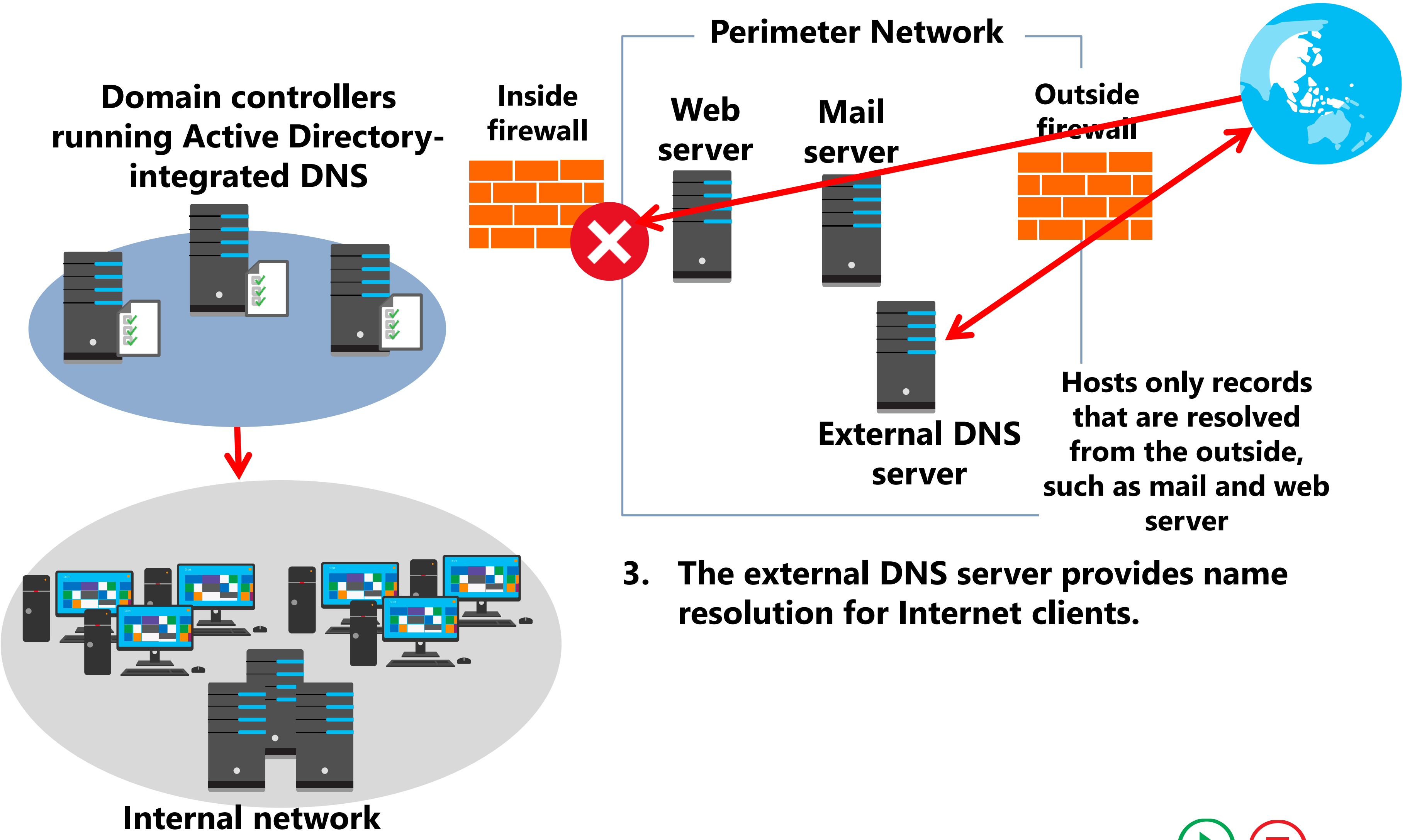
1. **Clients and servers on the internal network send all DNS queries to Active Directory-integrated DNS servers.**

Understanding split DNS


Perimeter Network
Domain controllers running Active Directory-Integrated DNS
Inside firewall
Web server
Mail server
Outside firewall
External DNS server
Hosts only records that are resolved from the outside, such as mail and web server
Internal network

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

Understanding split DNS


Perimeter Network
Domain controllers running Active Directory-integrated DNS
Inside firewall
Web server
Mail server
Outside firewall
External DNS server
Hosts only records that are resolved from the outside, such as mail and web server
Internal network

3. The external DNS server provides name resolution for Internet clients.

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 the cache from being overwritten until a percentage of the 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

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

DNS on Nano Server

To use Nano Server as a DNS Server:

- Install the NanoServer Package
- Create a VHD with the **Microsoft-NanoServer-DNS-Package**
- Import the VHD into Hyper-V as a virtual machine
- Configure networking settings and enable the remote management firewall ports
- Connect remotely to the server running Nano Server by using Windows PowerShell 5.0 on a Windows client or a server
- Run the command **Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role**
- Manage DNS remotely by using the Windows PowerShell 5.0 DNS commands

Lab C: Configuring advanced DNS settings

- Exercise 1: Configuring DNS policies
- Exercise 2: Validating the DNS implementation
- Exercise 3: Troubleshooting DNS

Logon Information

Virtual machines:	**20741A-LON-DC1**
	20741A-LON-SVR1
	20741A-INET
	20741A-EU-RTR
	20741A-SYD-SVR1
	20741A-TOR-SVR1
	20741A-LON-CL1
User name:	**Adatum\Administrator**
Password:	**Pa$$w0rd**

Estimated Time: 40 minutes

Lab Scenario

You want to make DNS zone management easier. You want to configure DNS policies in Windows Server 2016, so that users in different geographical areas can connect to a different web server. You must then test and troubleshoot the DNS configuration you have created.

Module Review and Takeaways

- Best Practices
- Common Issues and Troubleshooting Tips
- Review Questions
- Tools