ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

NETWORK ADMINISTRATION

CH2. Implementing DNS and DHCP

Content

- Understanding DNS
- Installing and configuring DNS
- Understanding DHCP
- Installing and configuring DHCP

Understanding DNS

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

UNDERSTANDING DNS

- The Domain Name System (DNS) is a service that allows you to resolve a hostname to an Internet Protocol (IP) address.
- One of the inherent complexities of operating in networked environments is working with multiple protocols and network addresses.

UNDERSTANDING DNS

- Owing largely to the tremendous rise in the popularity of the Internet, however, most environments have transitioned to use TCP/IP as their primary networking protocol.
- To understand DNS easily, think about making a telephone call: If you do not know the target's phone number, input the name, and get the telephone number from your phone's contact list.

UNDERSTANDING DNS

TCP/IP is actually a collection of different technologies (protocols and services) that allow computers to function together on a single, large, and heterogeneous network.

Some of the major advantages of this protocol include widespread support for hardware, software, and network devices; reliance on a system of standards; and scalability. TCP handles tasks such as sequenced acknowledgments. IP involves many jobs, such as logical subnet assignment and routing.

UNDERSTANDING DNS

- The Form of an IP Address:

An IP address is a logical number that uniquely identifies a computer on a TCP/IP network. TCP/IP allows a computer packet to reach the correct host. An IPv4 address takes the form of four octets (eight binary bits), each of which is represented by a decimal number between 0 and 255. For example: 128.45.23.17; 230.212.43.100; 10.1.1.1

- address 11000000 10101000 00000001 00010101 maps to 192.168.1.21

- IPv6 expands the address space to 128 bits. The address is usually represented in hexadecimal notation asfollows:

2001:0DB8:0000:0000:1234:0000:A9FE:133E

IMPLEMENTING DNS SERVERS

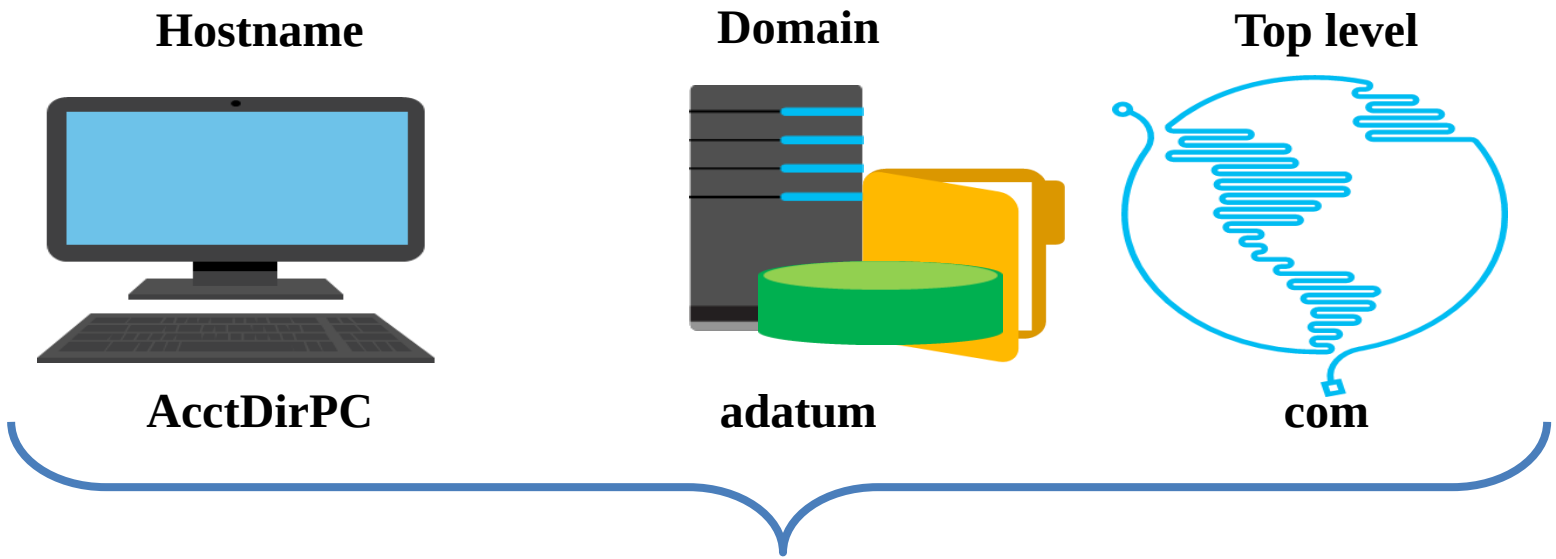
- Implementing DNS servers
- Configuring zones in DNS
- Configuring name resolution between DNS zones
- Configuring DNS integration with AD DS
- Configuring advanced DNS settings

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

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?

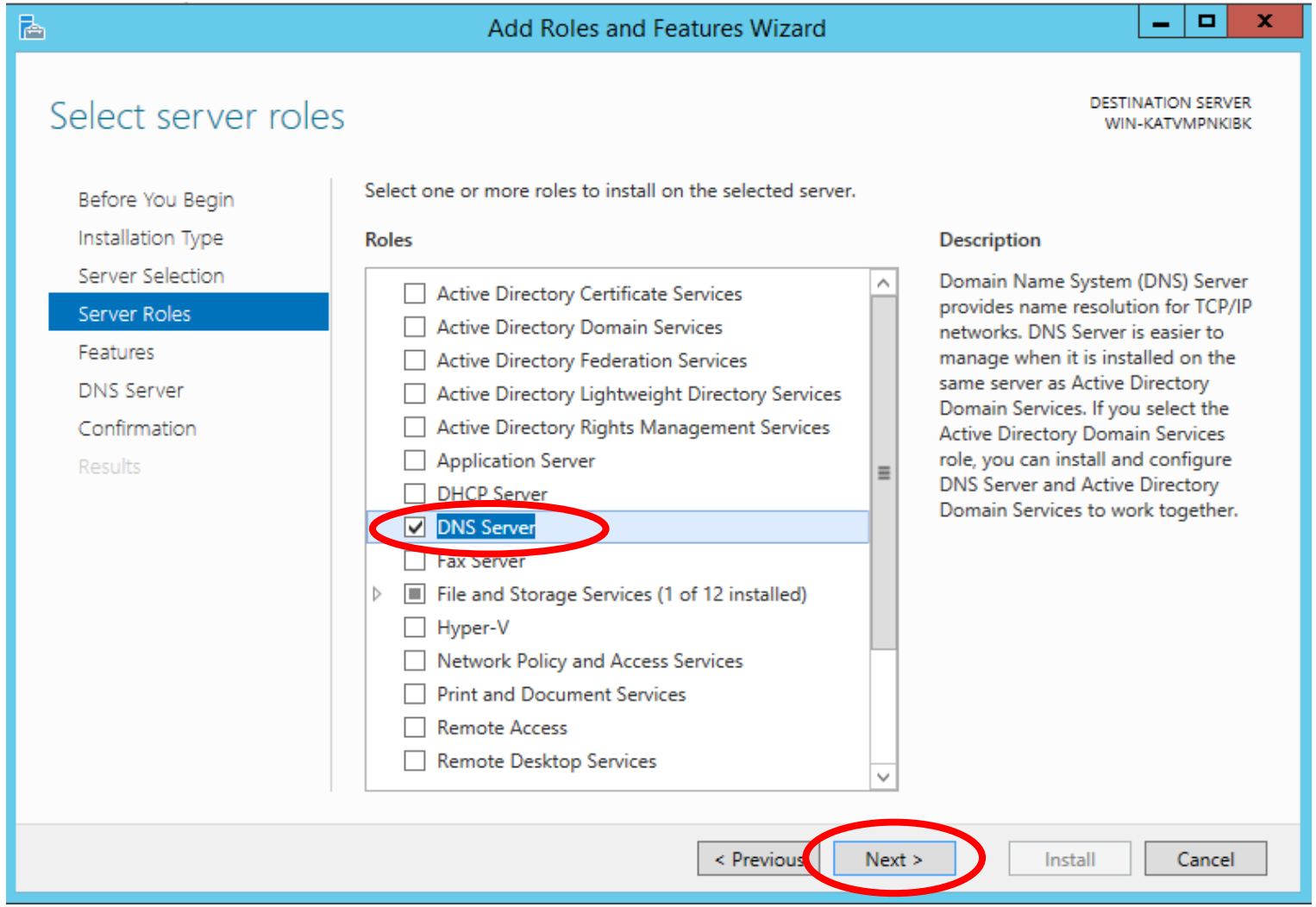
- A DNS zone is a specific portion of DNS namespace that contains DNS records
- Zone types:
  - Forward lookup zone
  - Reverse lookup zone
- Resource records in forward lookup zones include: A, MX, SRV, NS, SOA, and CNAME
- Resource records in reverse lookup zones include: PTR

Installing and configuring the DNS role

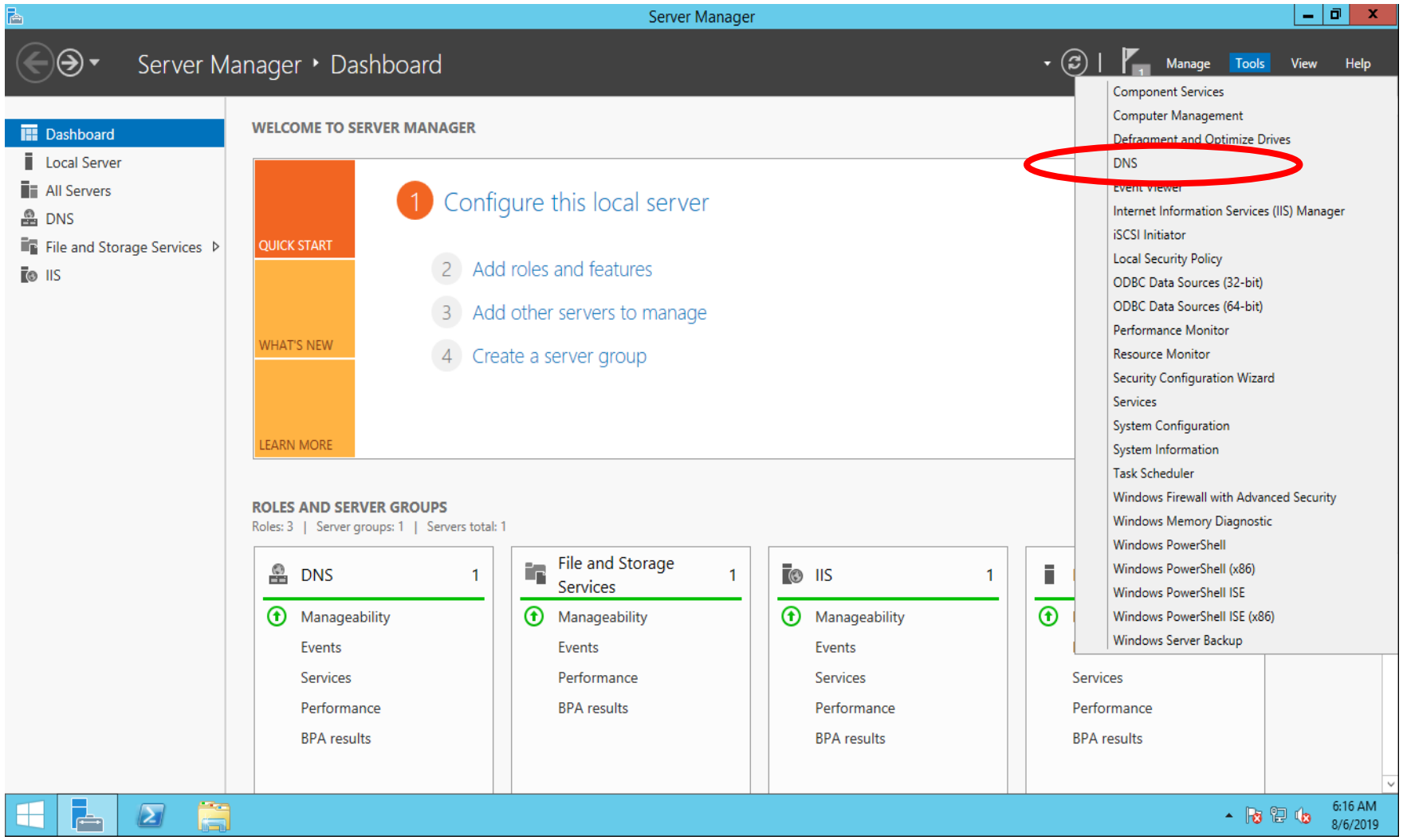
In this demonstration, you will learn how to:

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

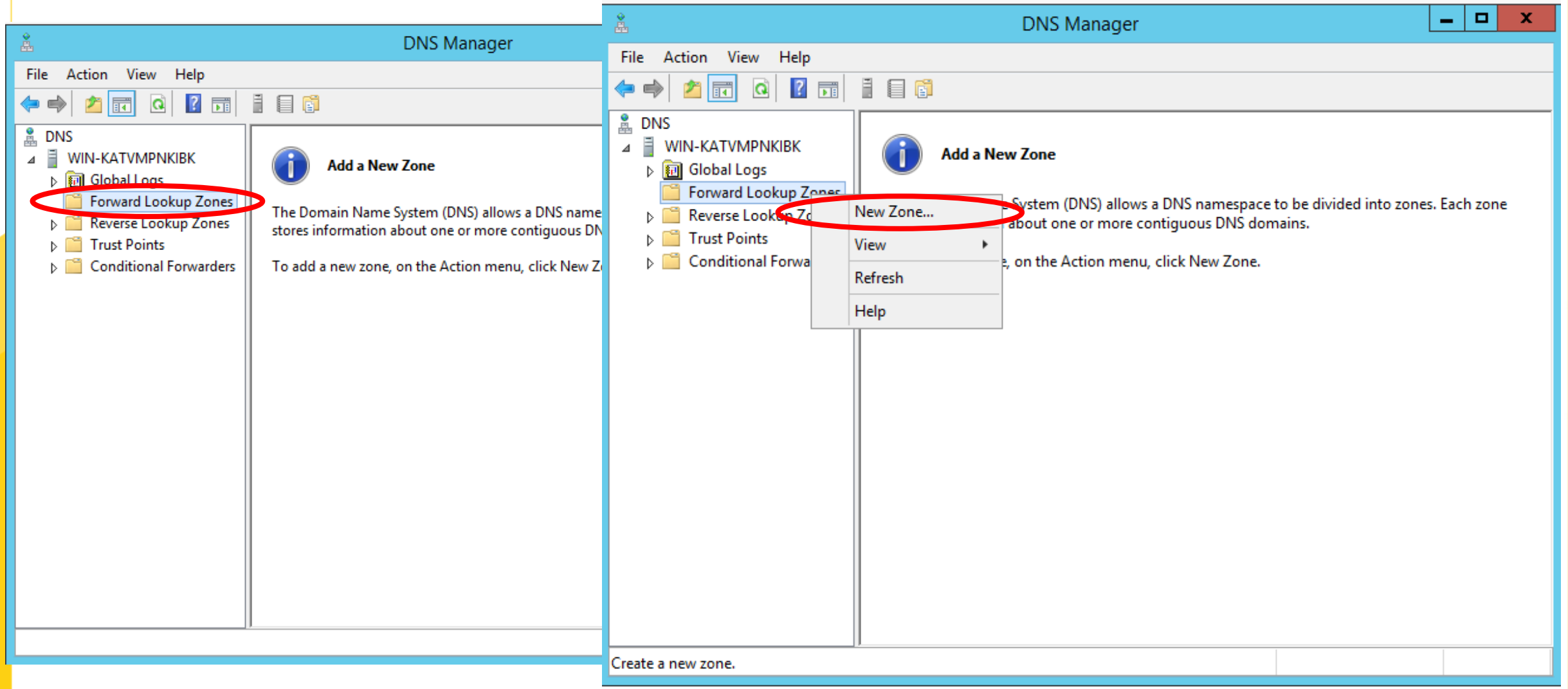
Installing and configuring the DNS role



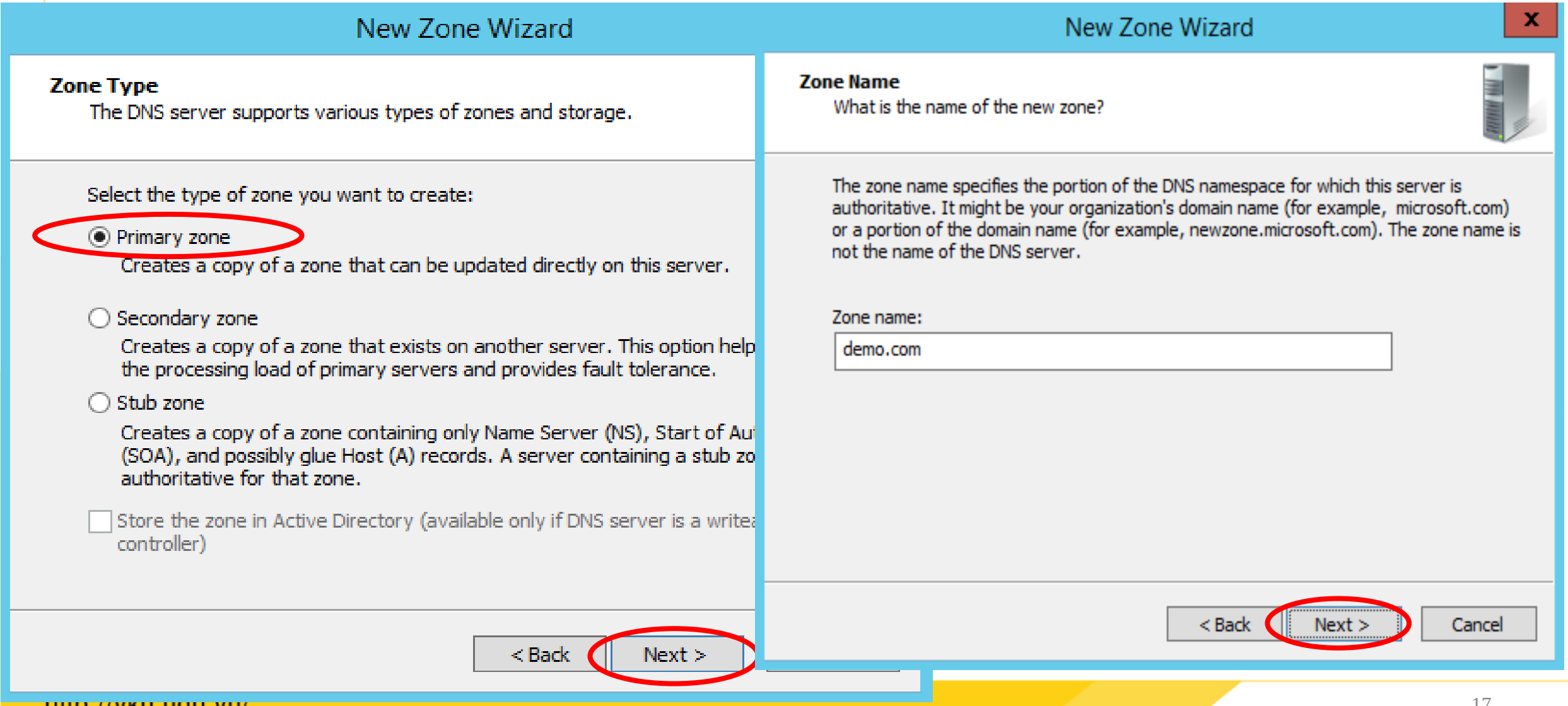
Installing and configuring the DNS role



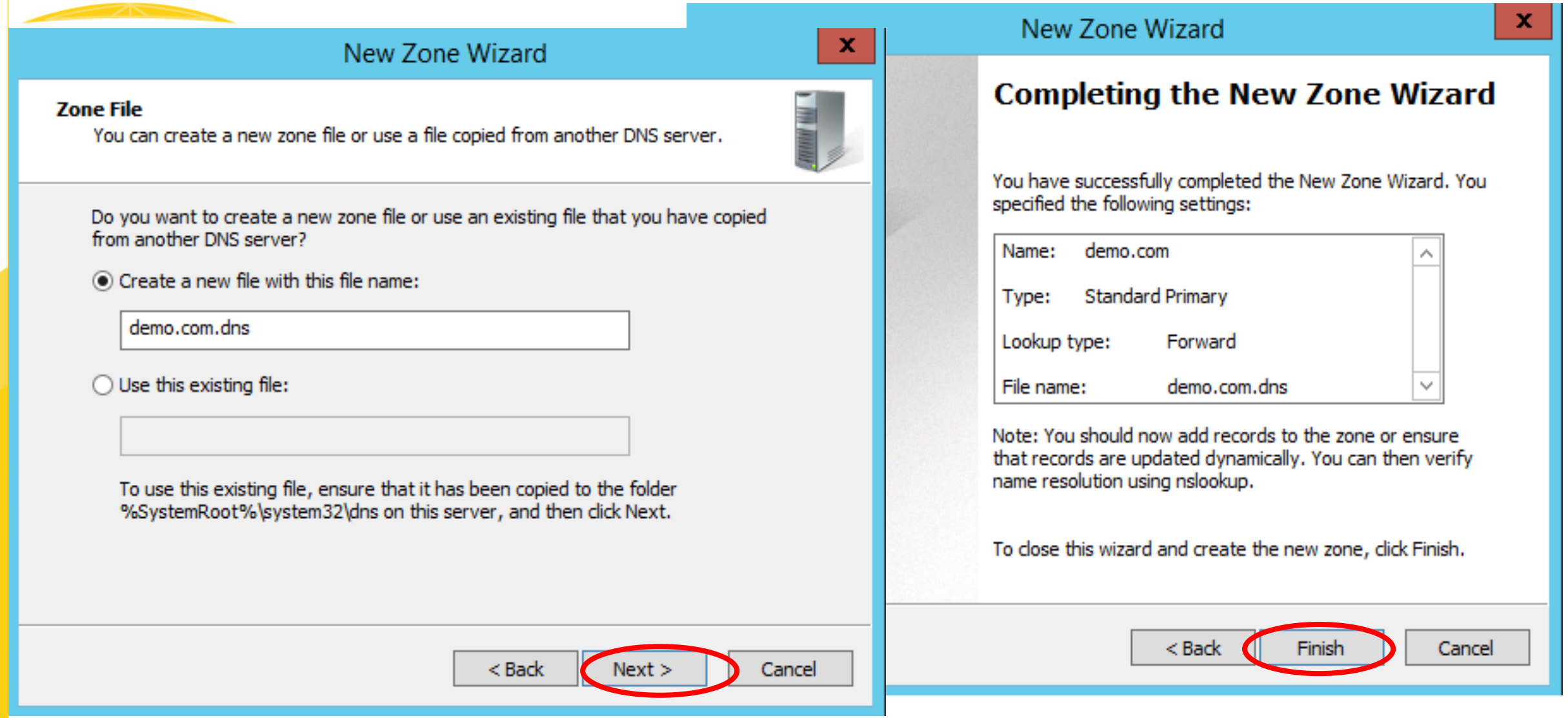
Installing and configuring the DNS role



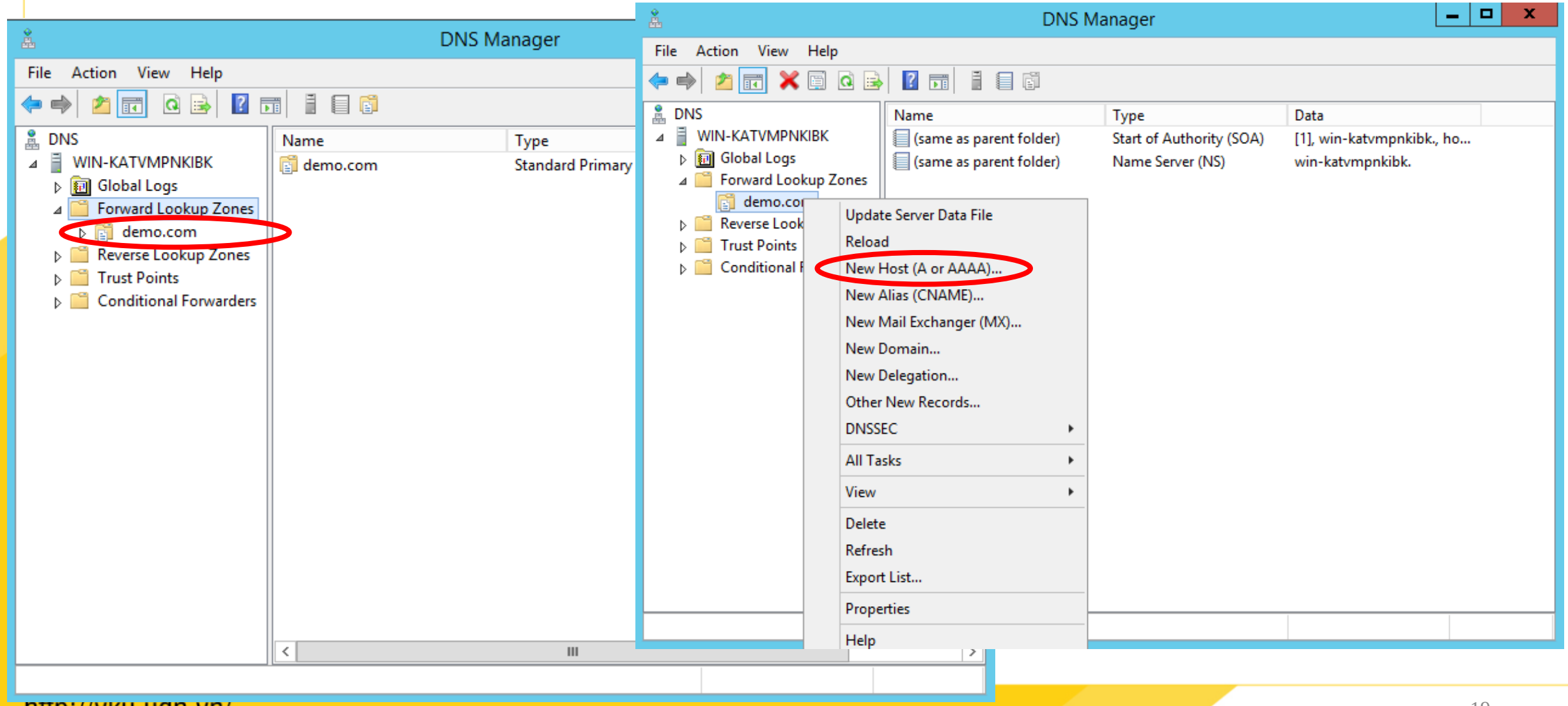
Installing and configuring the DNS role



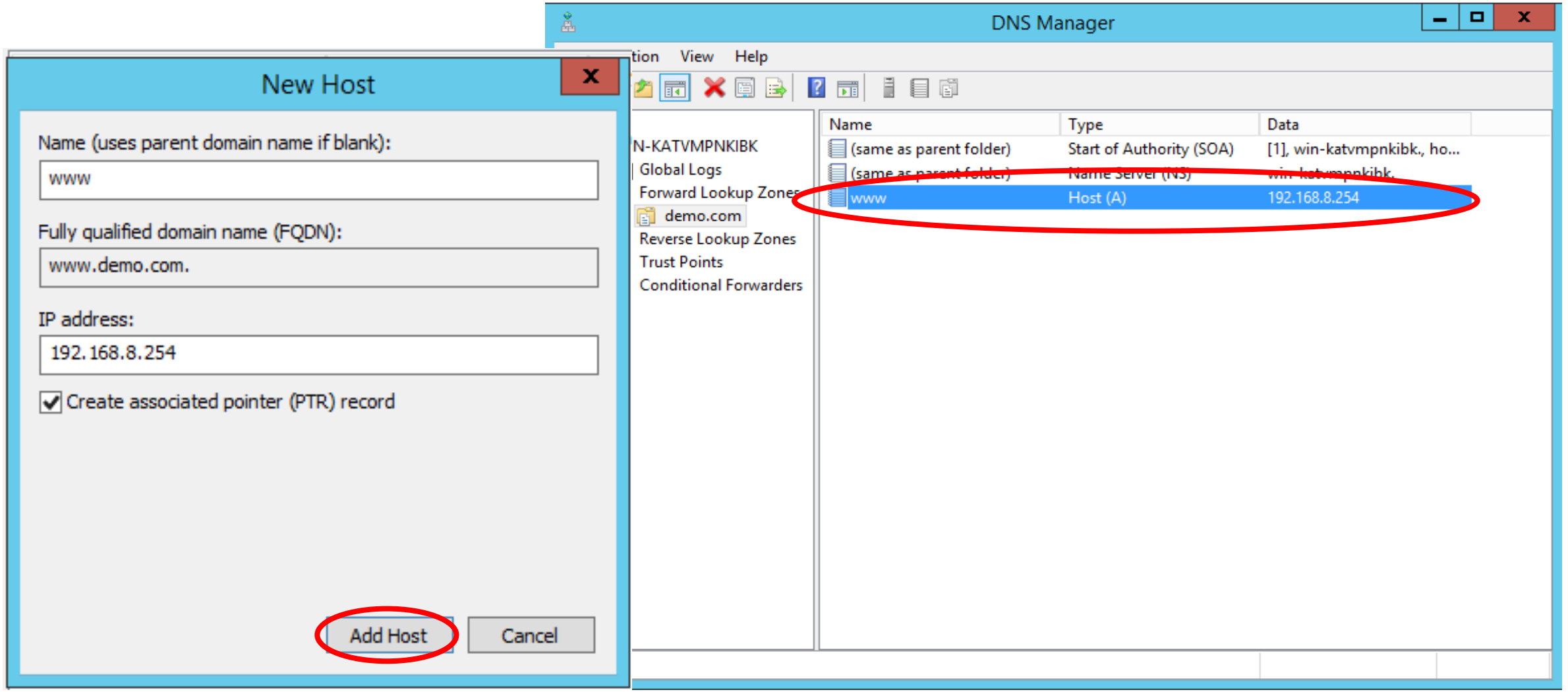
Installing and configuring the DNS role



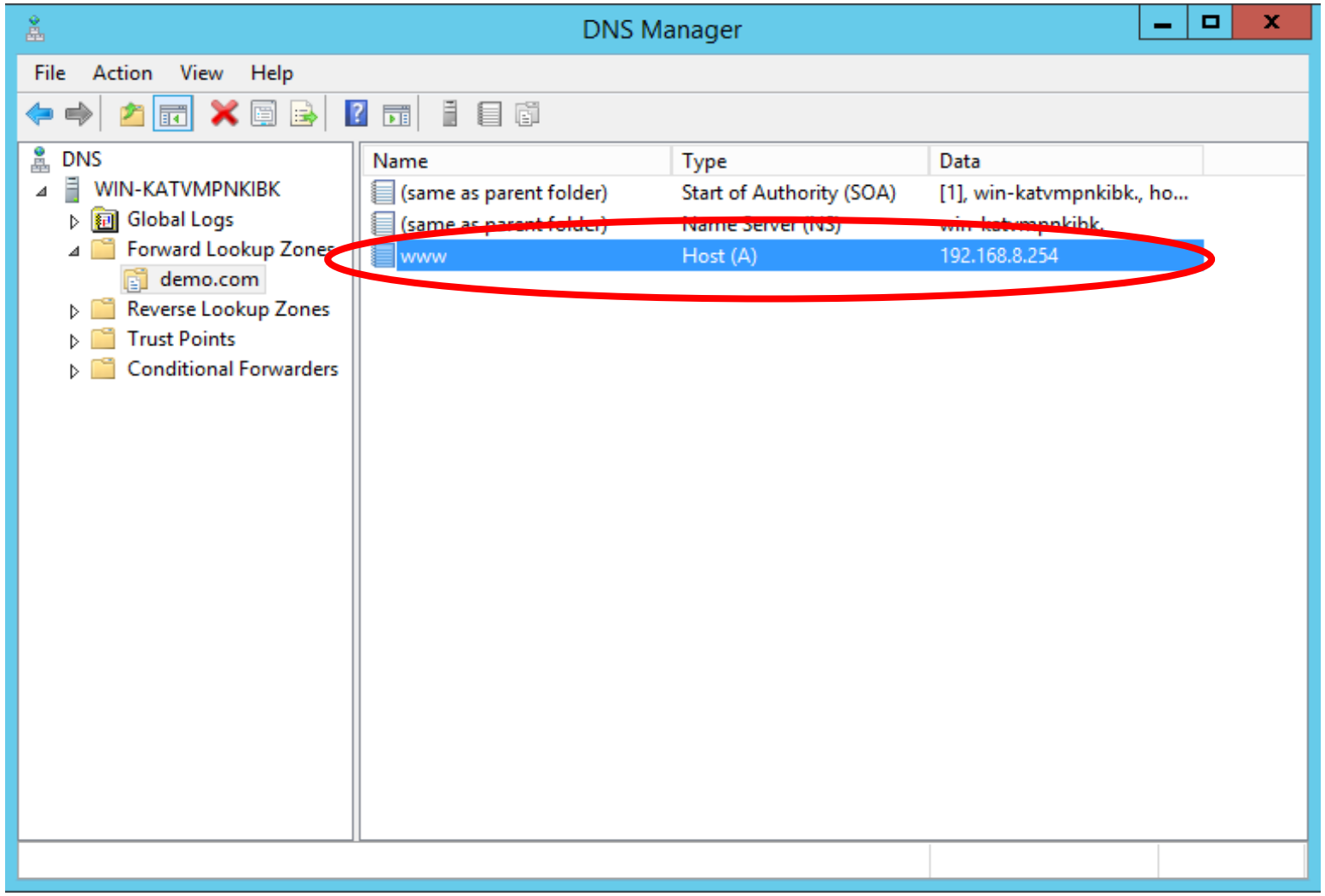
Installing and configuring the DNS role



Installing and configuring the DNS role

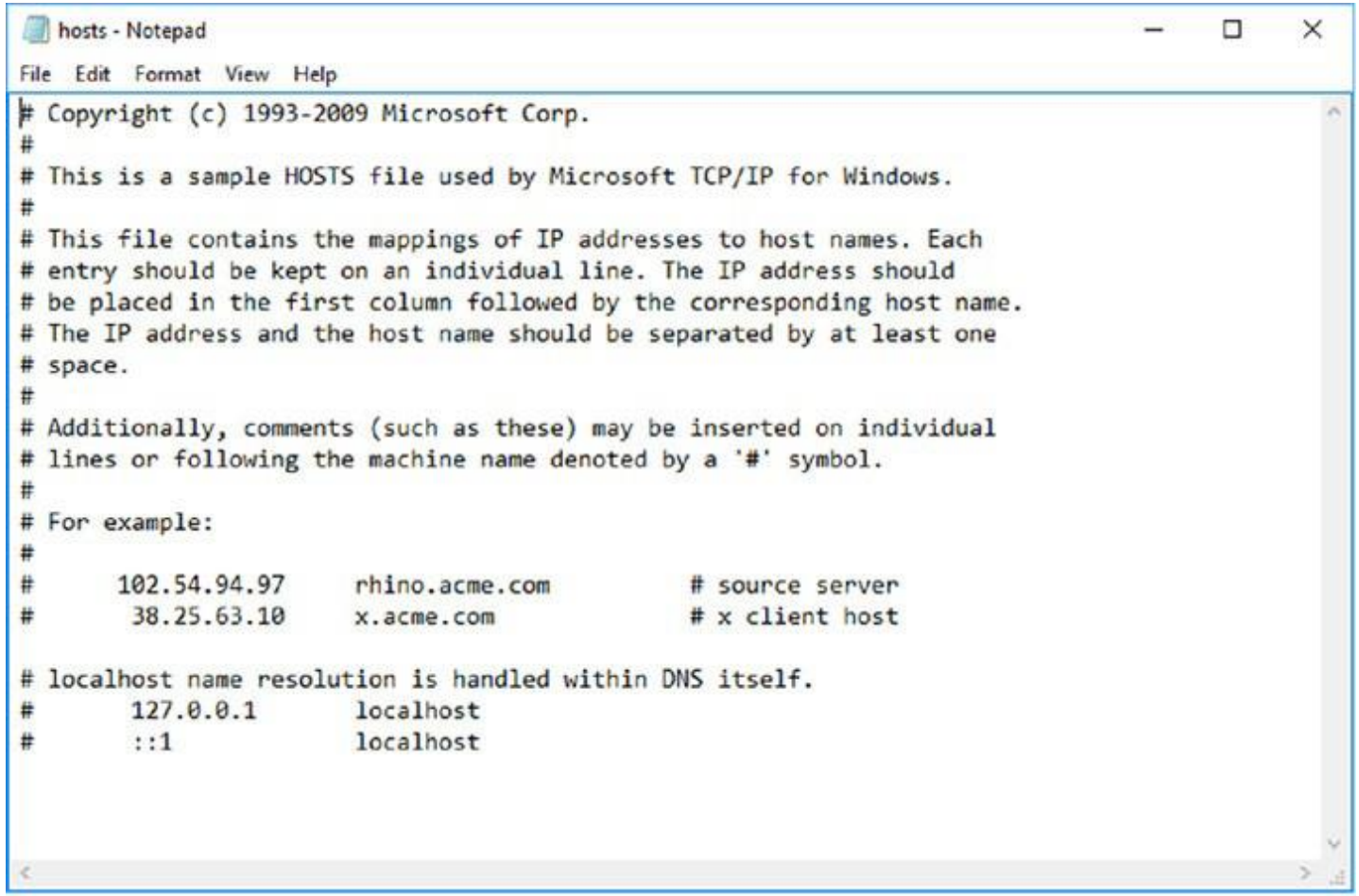


Installing and configuring the DNS role

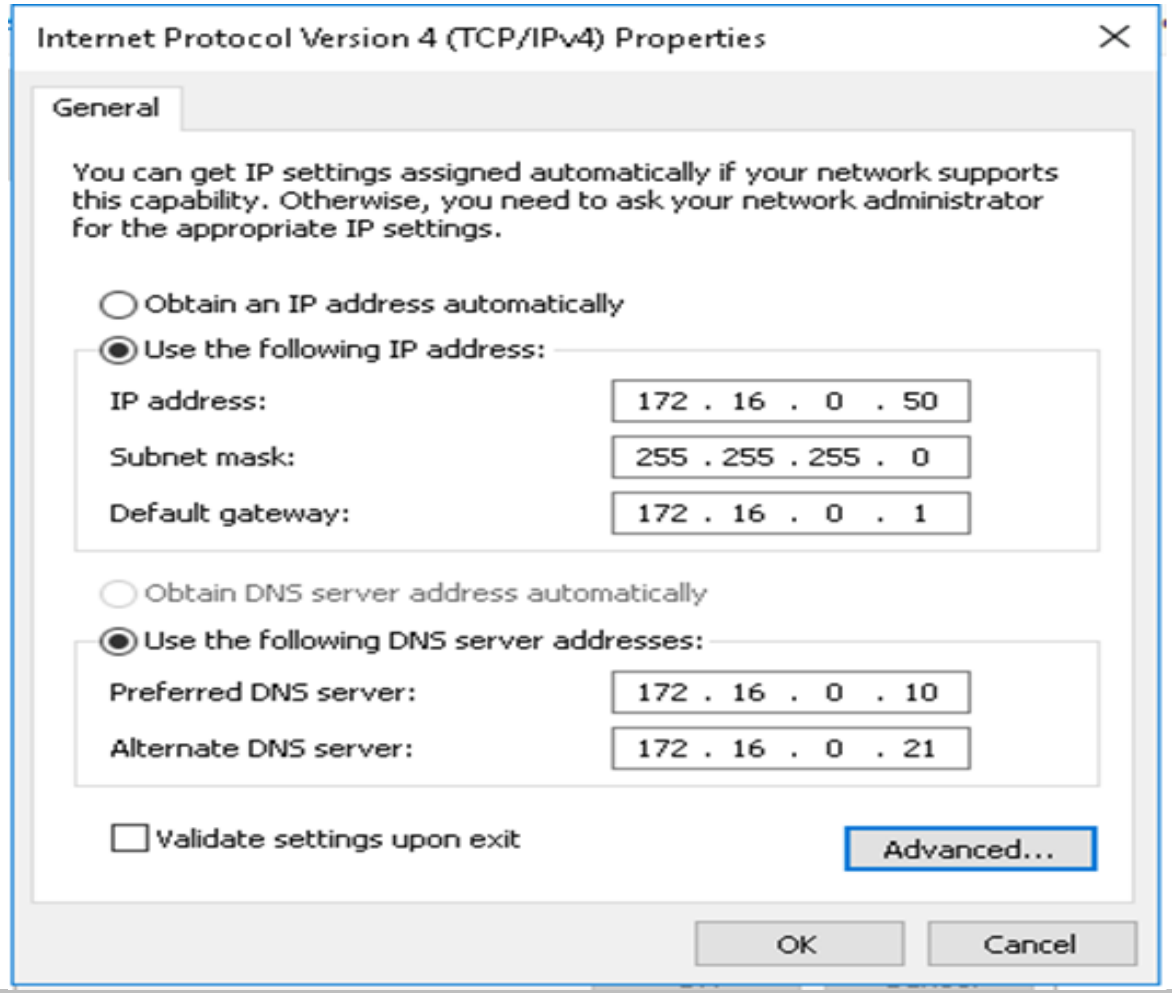


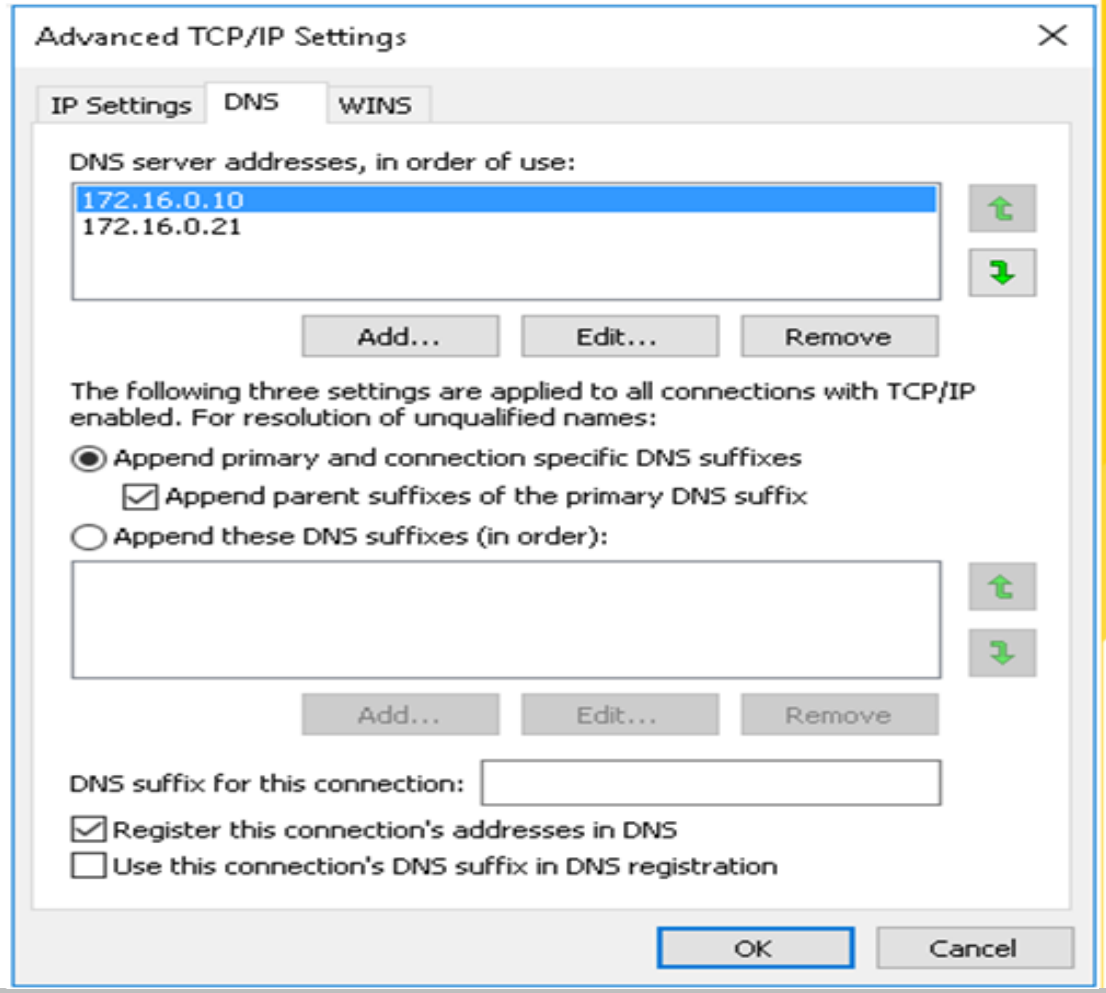
Installing and configuring the DNS role

- 1. Open the HOSTS file: C:\Windows\Systems32\drivers\etc.
- 2. Add the IP-address-to-hostname mapping.
- 3. Try to ping the server using the hostname to verify that you can reach it using an easy-to-remember name.



Configuring DNS clients






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

Managing DNS services

- Manage DNS services:
  - 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

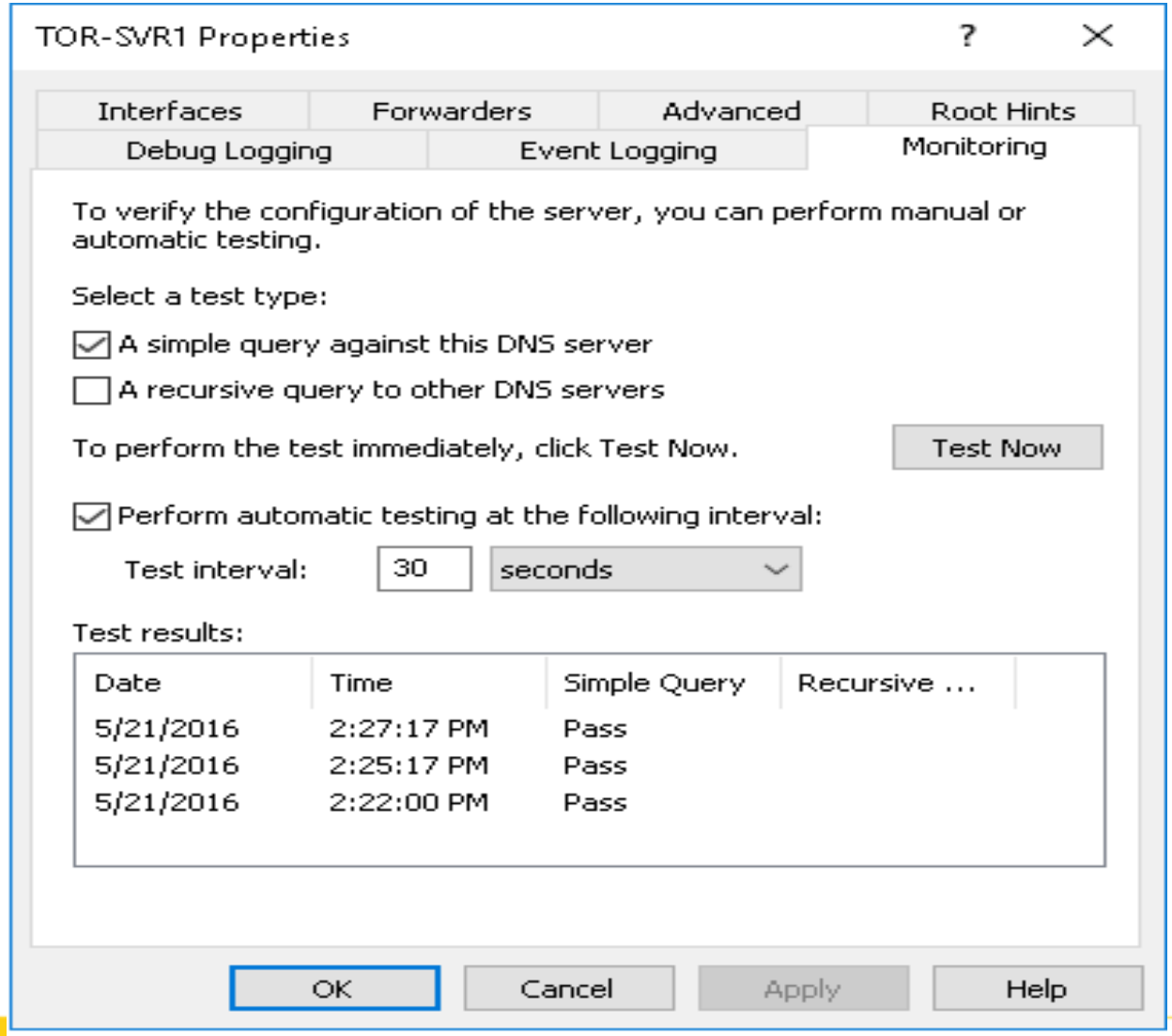
Troubleshooting name resolution

In this demonstration, you will learn how to:

- Use Windows PowerShell cmdlets to troubleshoot DNS <*page* 528>
- Use command-line tools to troubleshoot DNS <*page* 541>

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



Configuring zones in DNS

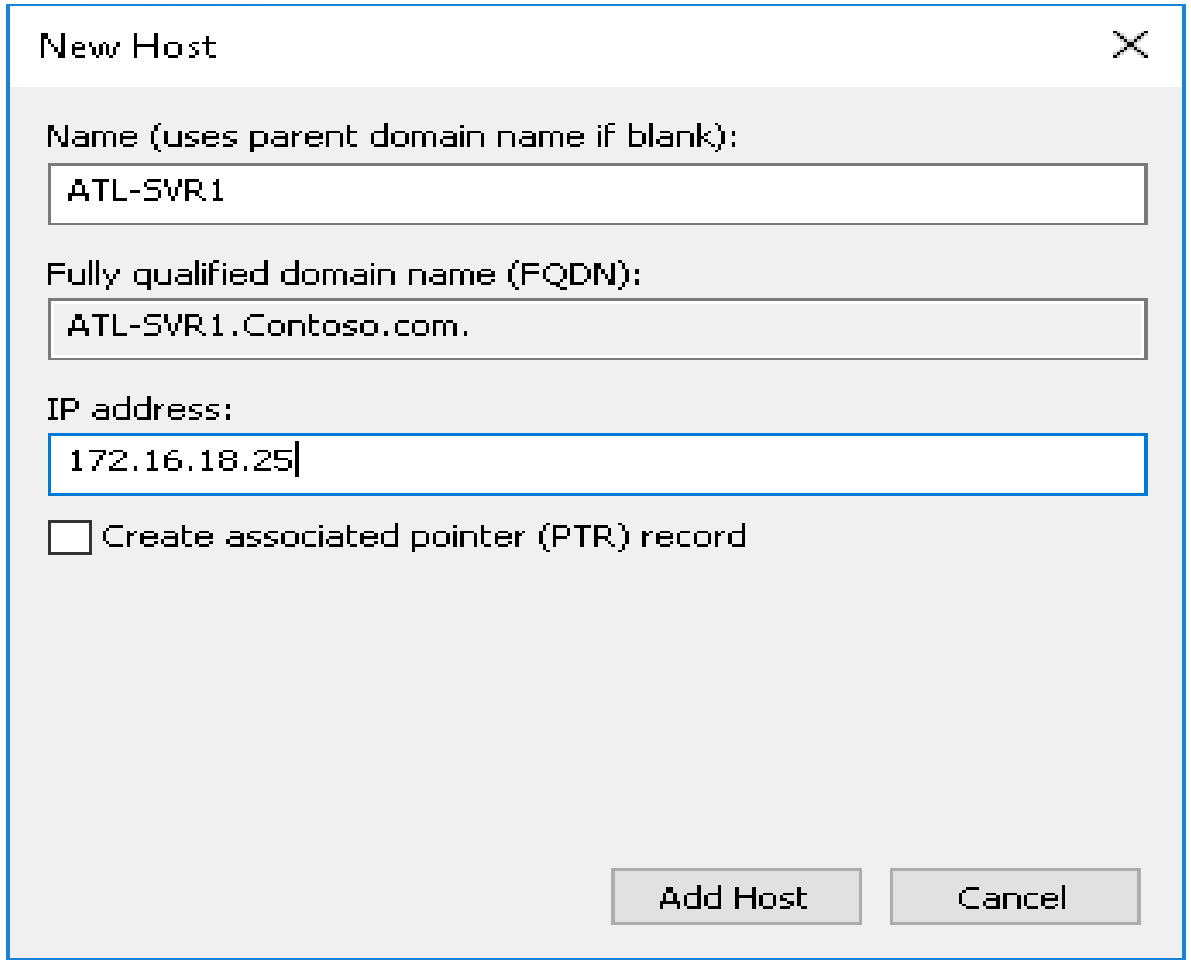
- DNS resource record types
- Creating records in DNS
- Configuring DNS zones
- What are primary and secondary zones?
- Configuring zone replication

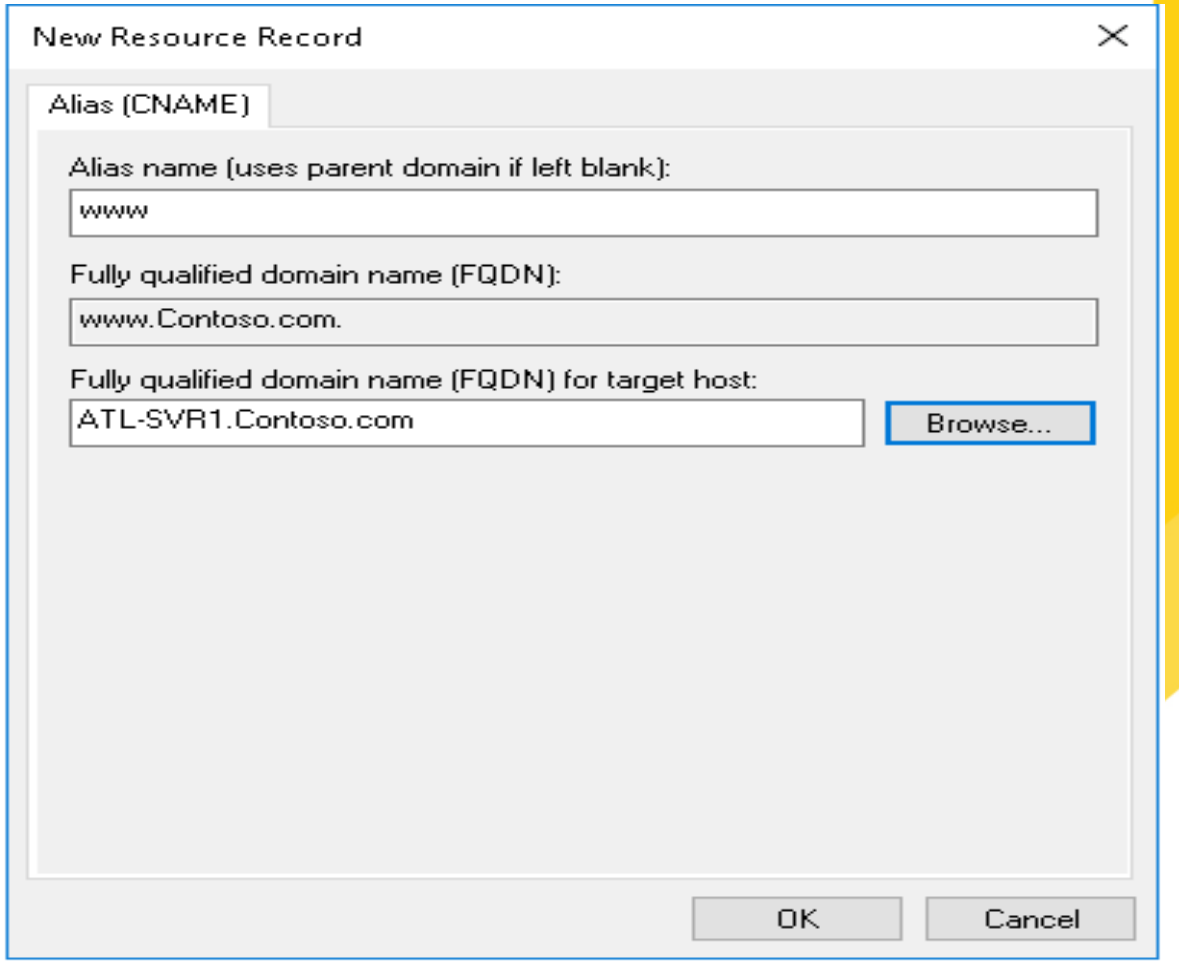
DNS resource record types

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

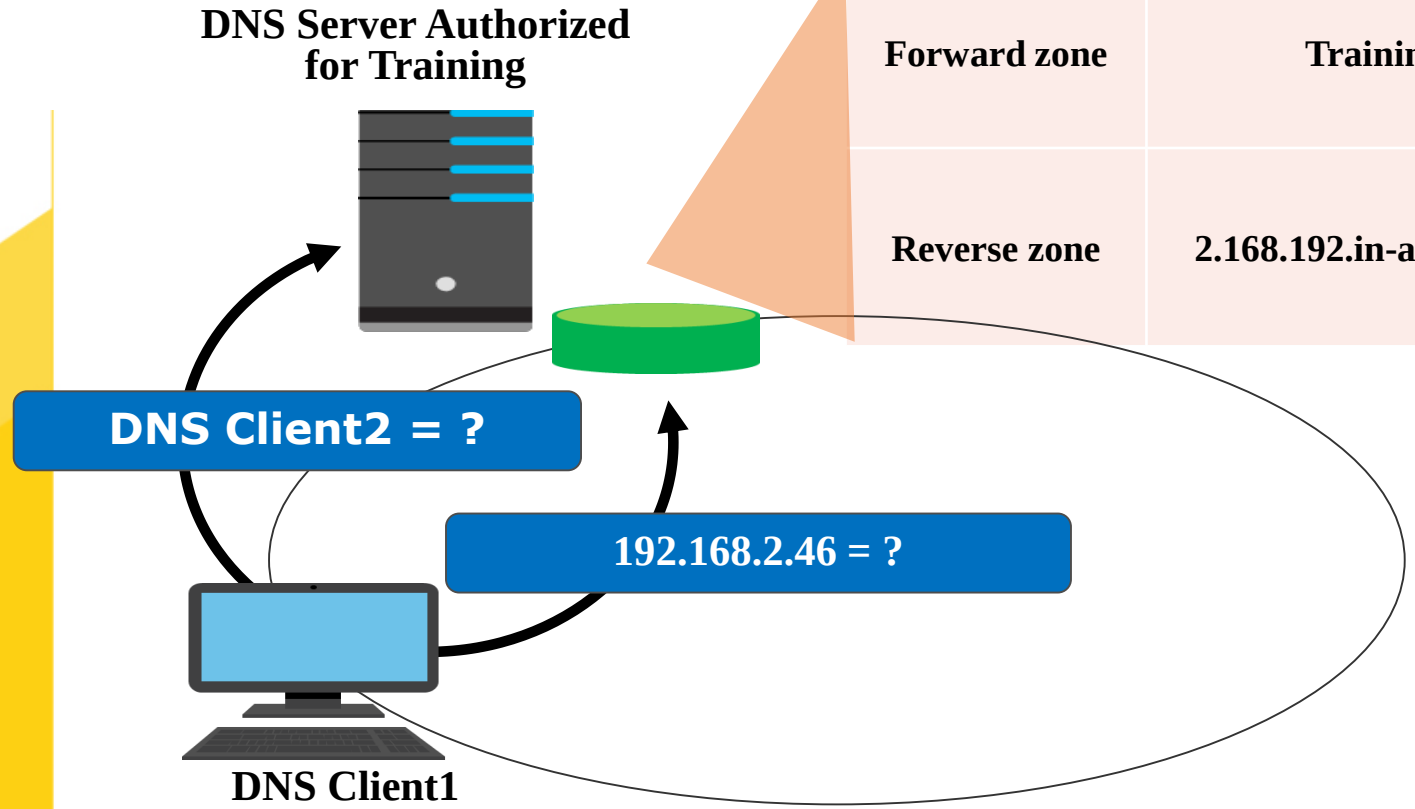




Add-DnsServerResourceRecordA -ZoneName Contoso.com -Name ATL-SVR1 -IpAddress 172.16.18.25

Configuring DNS zones

Namespace: training.contoso.com

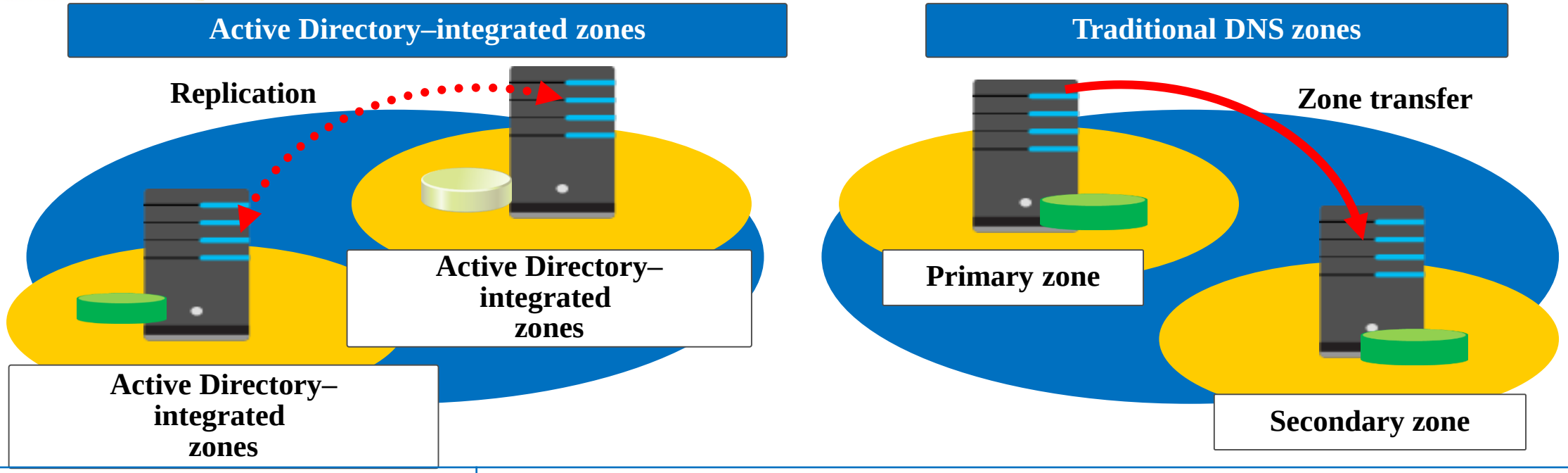


Forward zone	**Training**	DNS Client1	192.168.2.45
		DNS Client2	192.168.2.46
		DNS Client3	192.168.2.47
Reverse zone	**2.168.192.in-addr.arpa**	192.168.2.45	DNS Client1
		192.168.2.46	DNS Client2
		192.168.2.47	DNS Client3

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

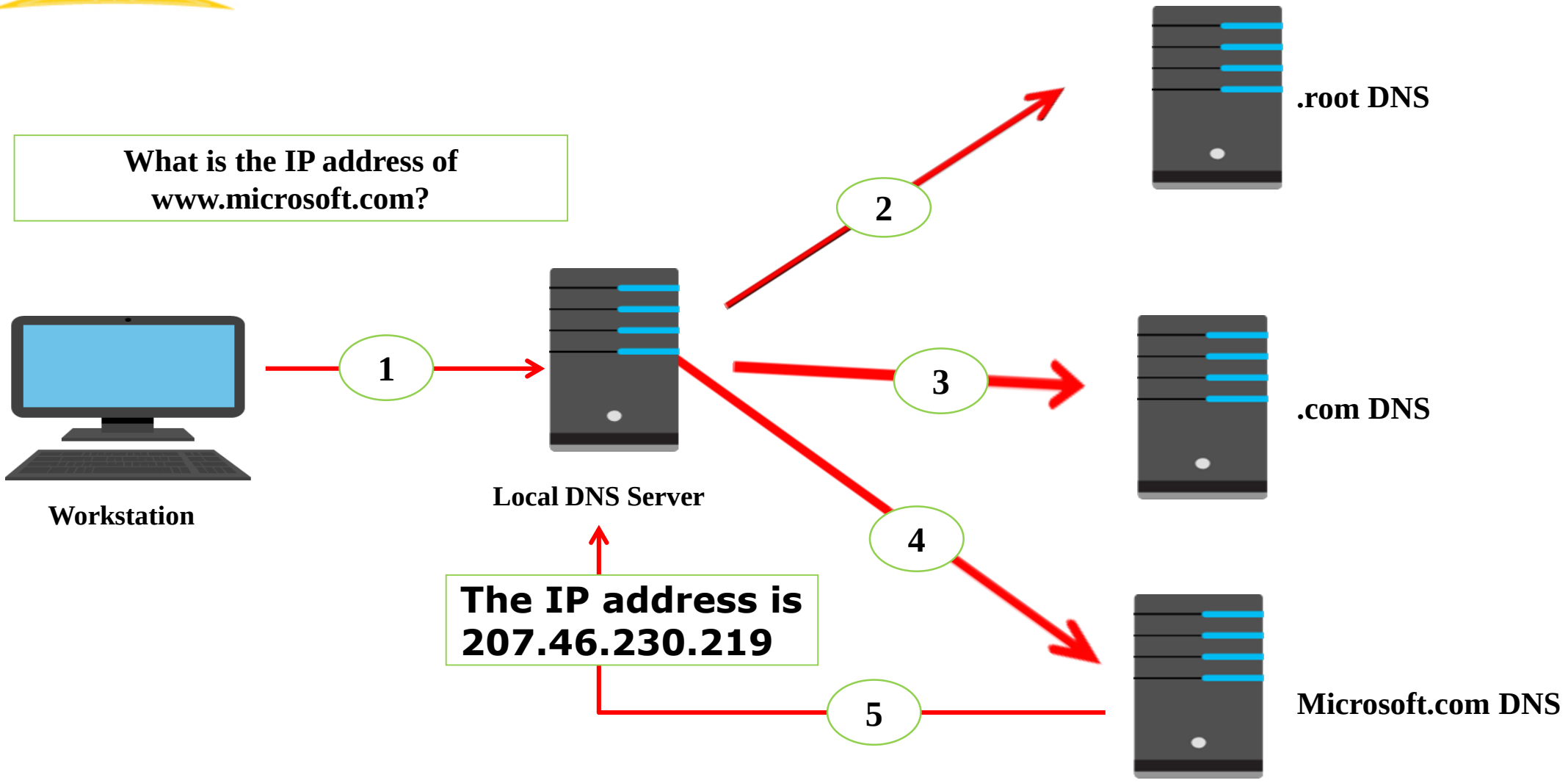


Zones	Description
Active Directory–integrated zones	• Perform incremental replication between DNS servers • Adjust the Active Directory replication schedule
Traditional DNS zones	• Replicate between primary and secondary zones • Perform an incremental rather than a complete zone transfer

Configuring name resolution between DNS zones

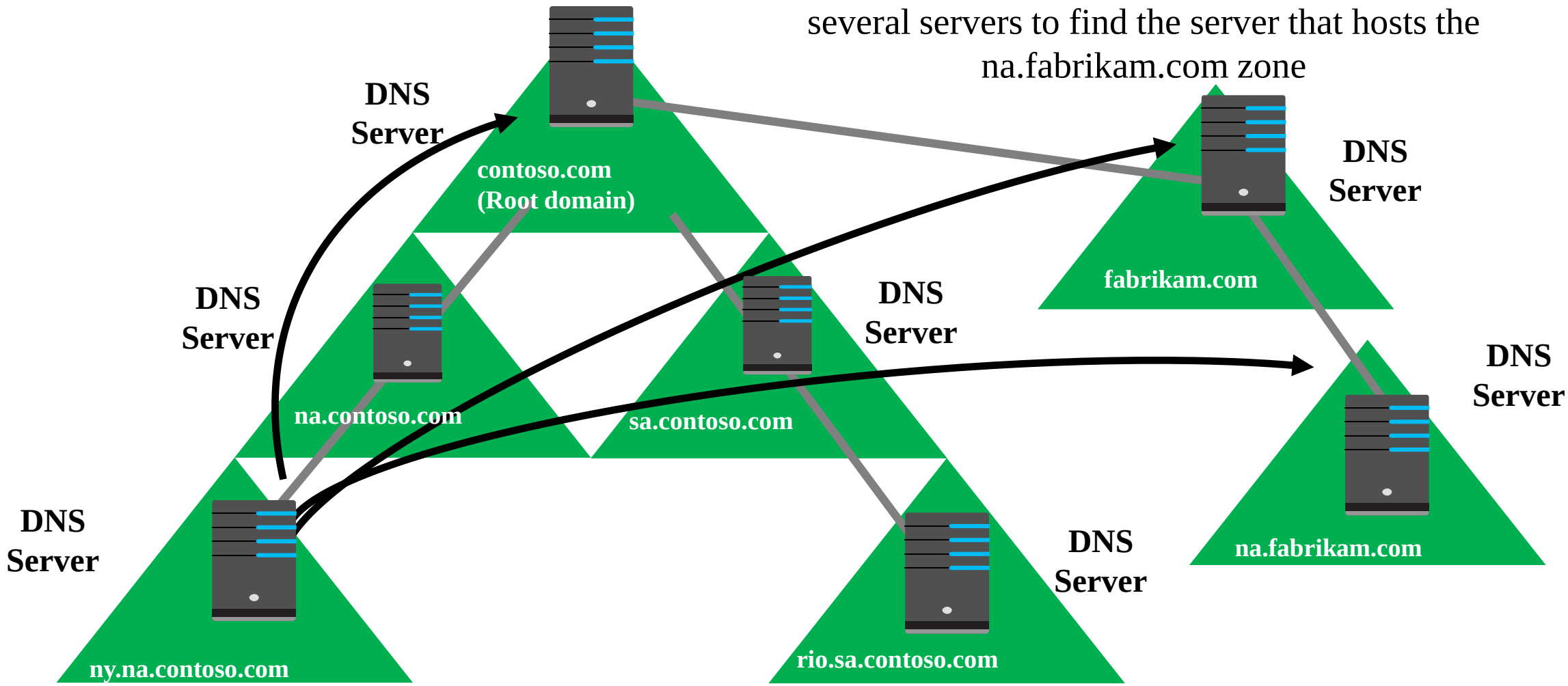
- Resolving DNS names between zones
- What is a stub zone?
- What is DNS caching?
- What is DNS forwarding?
- DNS forwarding and stub zone guidance
- Discussion: When to use DNS forwarding
- Configuring delegation

Resolving DNS names between zones



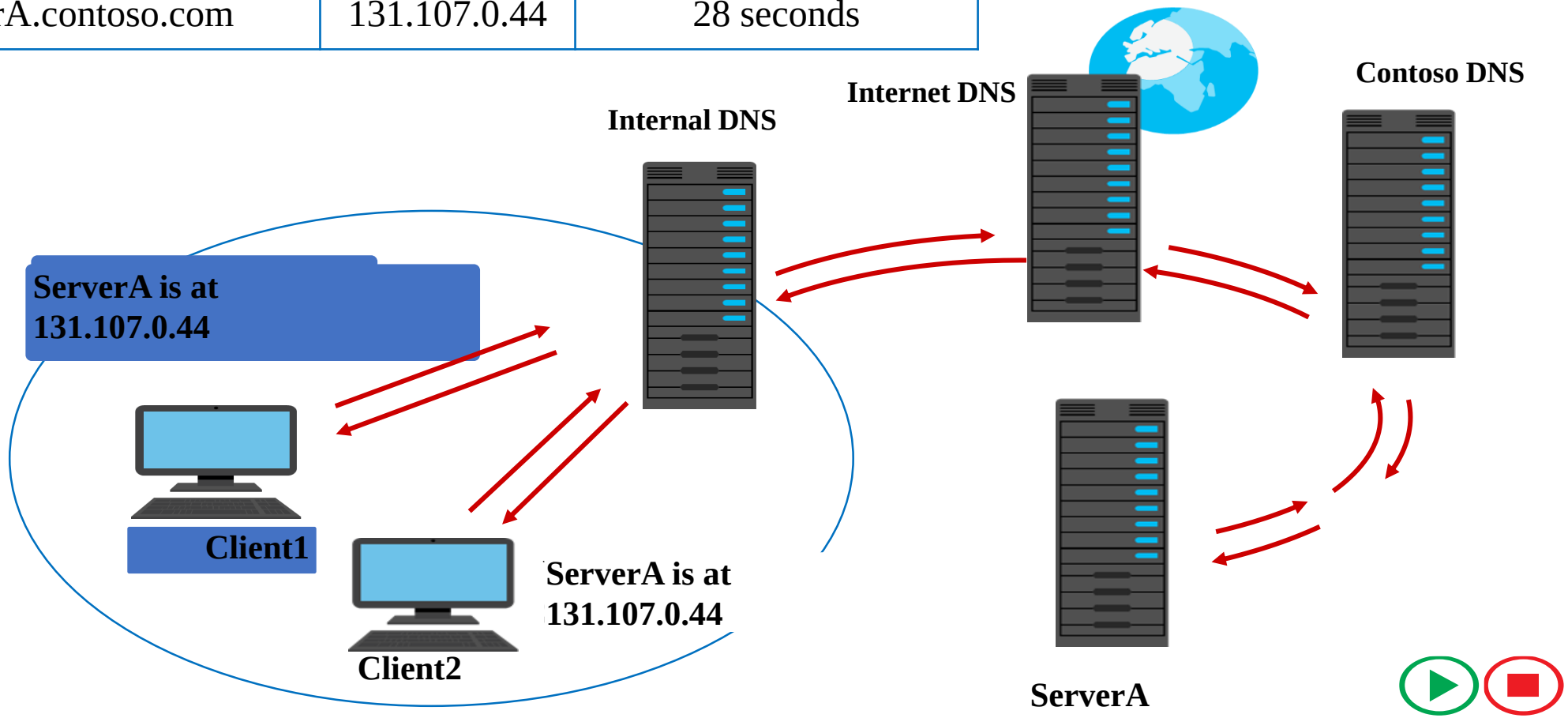
What is a stub zone?

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



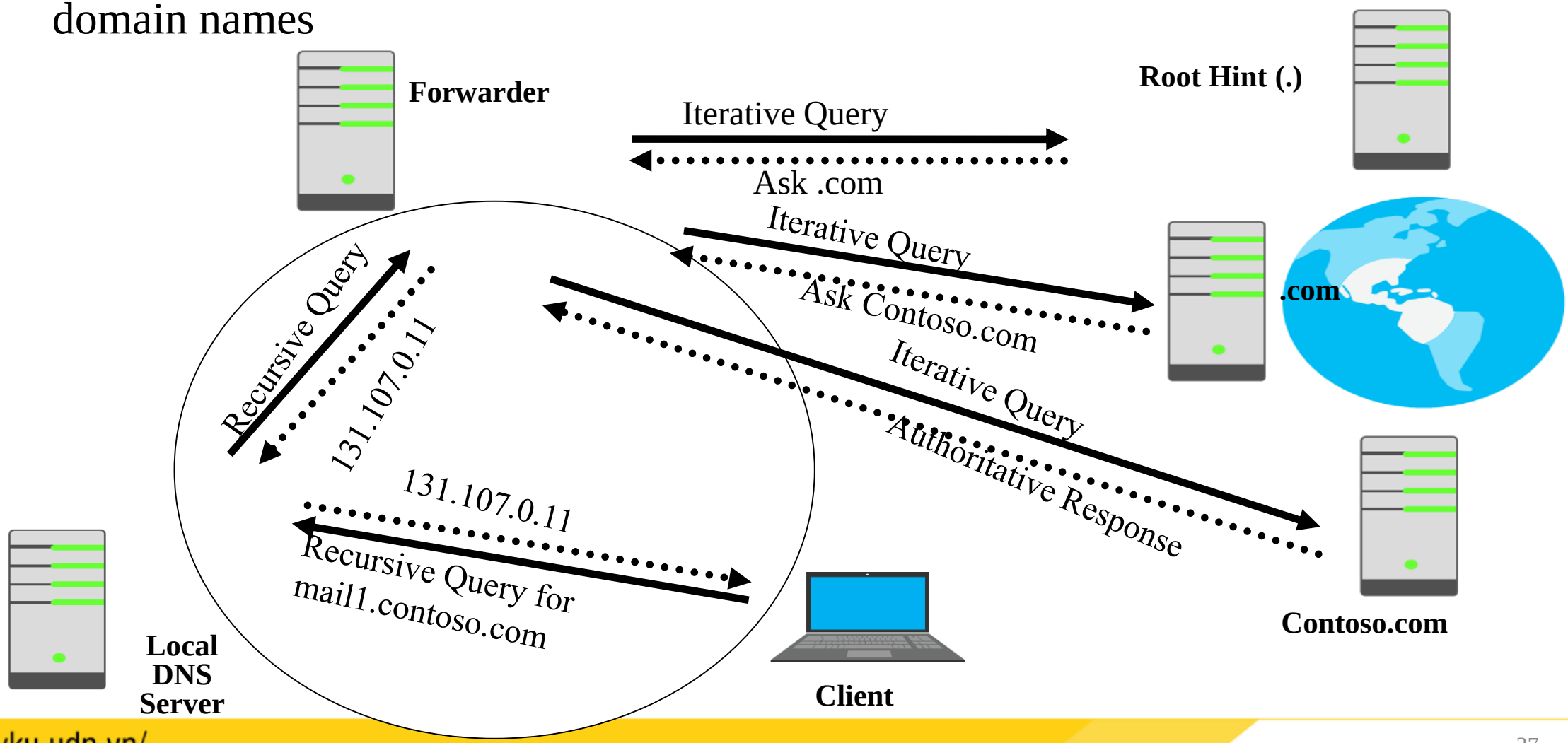
What is DNS caching?

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



What is DNS forwarding?

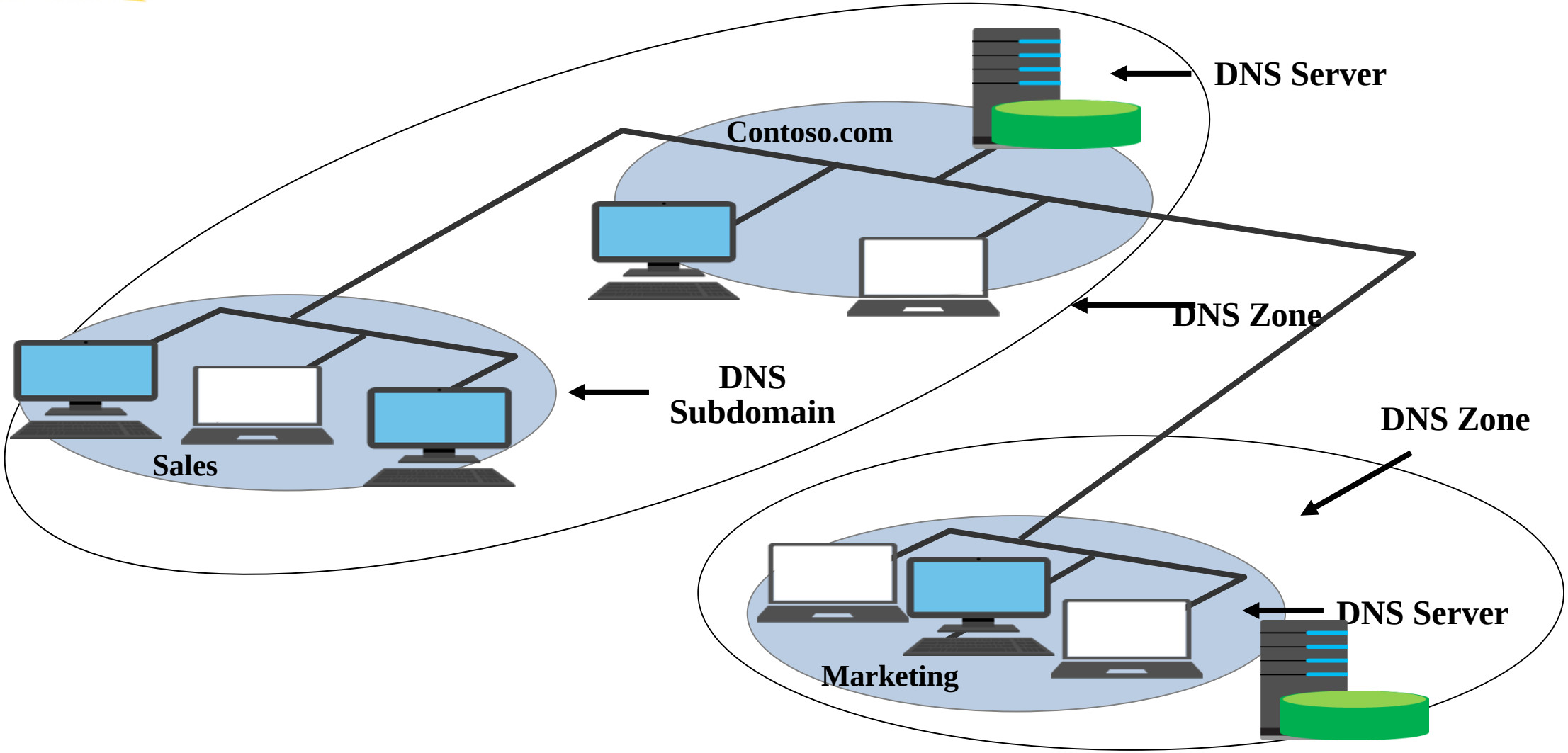
A forwarder is a DNS server that is designated to resolve external or offsite DNS domain names



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

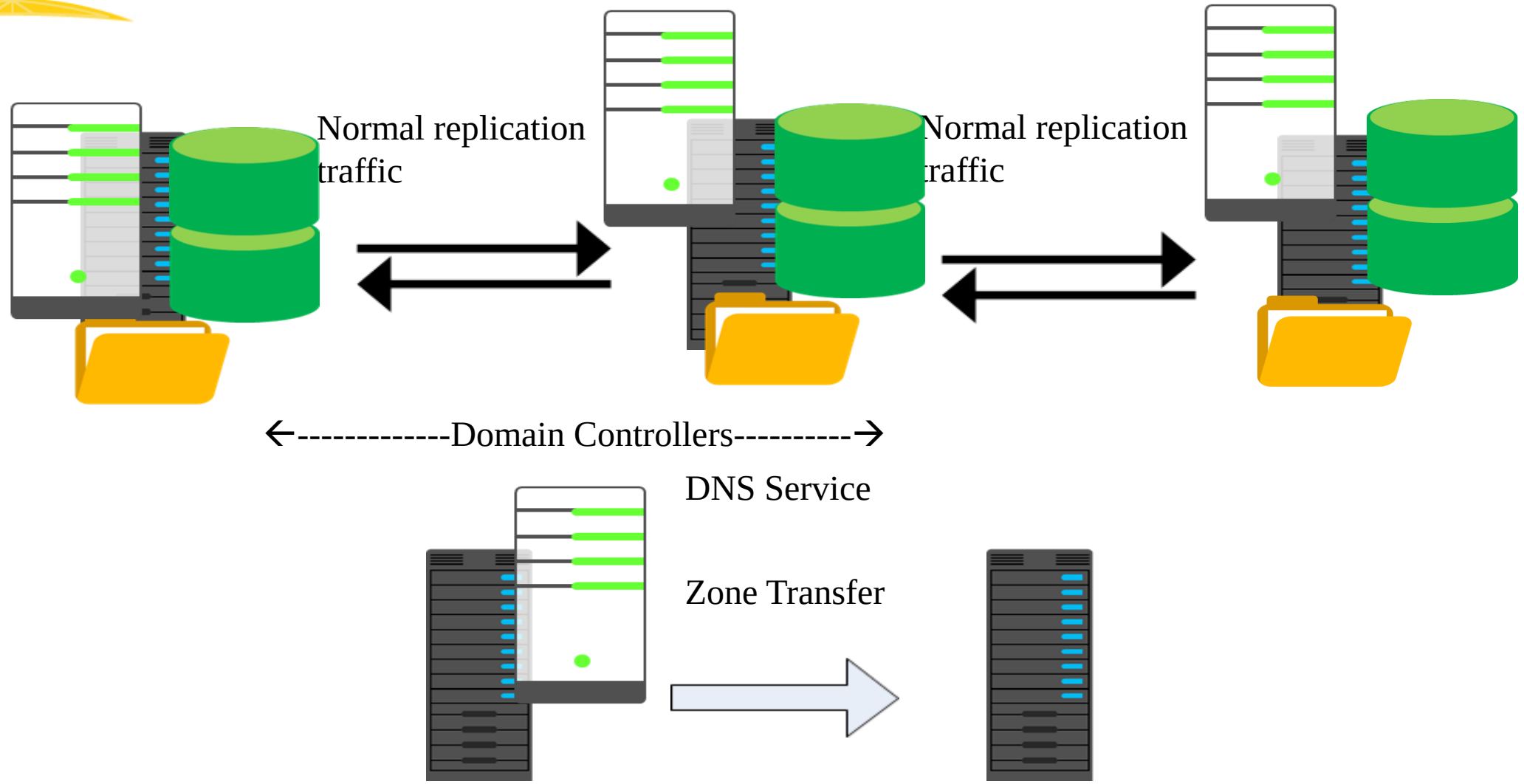
Configuring delegation



Configuring DNS integration with AD DS

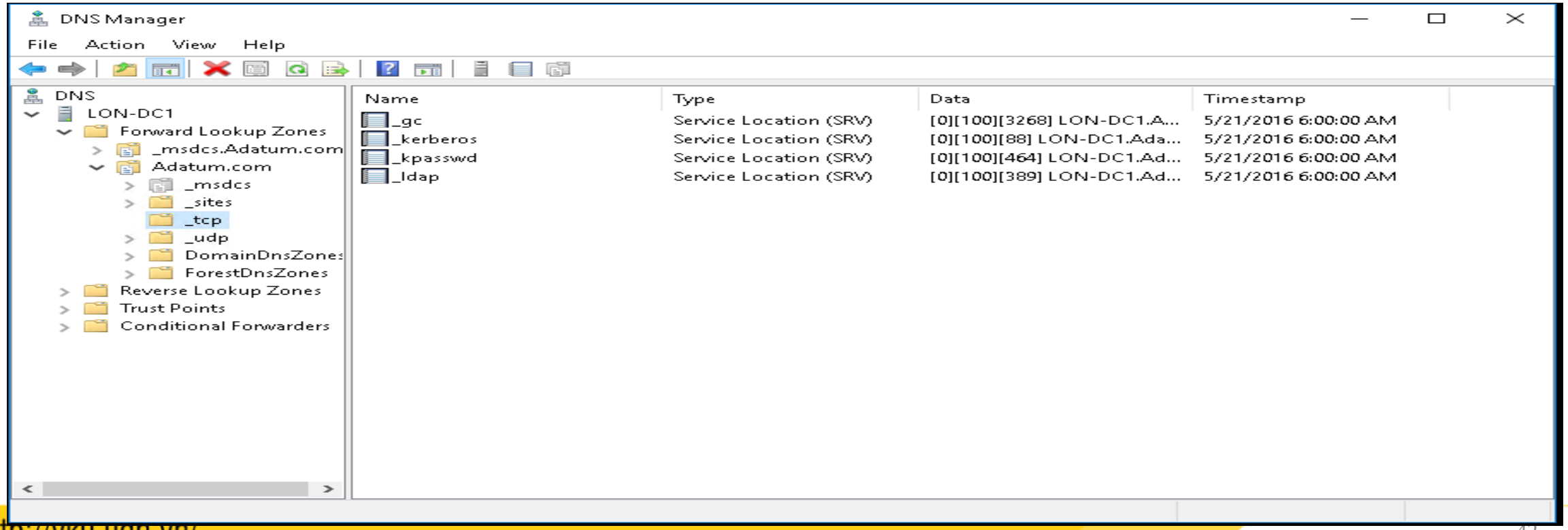
- Overview of AD DS and DNS integration
- What are Service Resource Locator records?
- Benefits of Service Resource Locator records
- What are Active Directory–integrated zones?
- Application partitions in AD DS
- Dynamic updates
- Demonstration: Configuring AD DS–integrated zones

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



Benefits of Service Resource Locator records

Benefits of SRV Resource Records

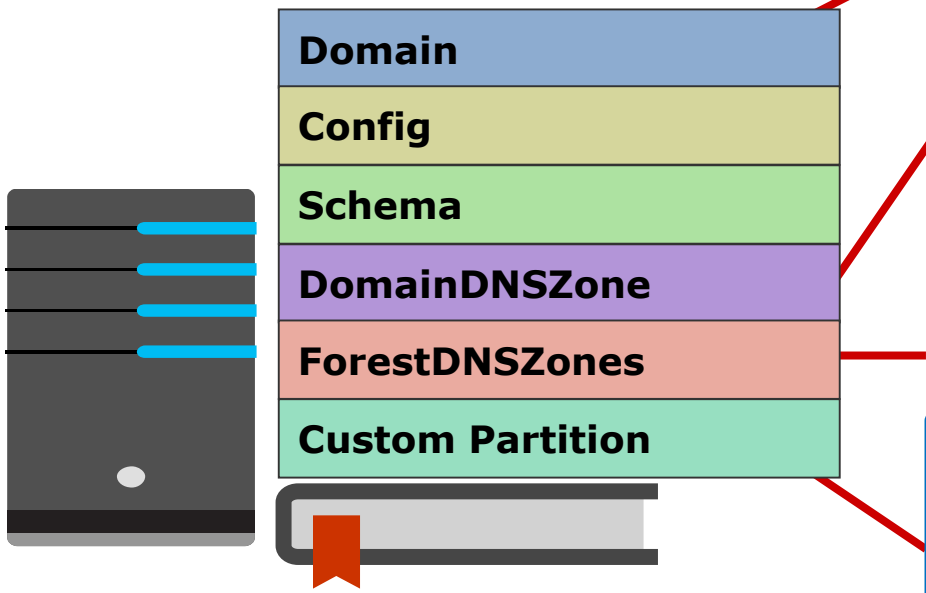
- Domain controllers register their SRV resource records dynamically, by service and site location
- Client systems in sites use SRV resource records recorded in a site to find domain controllers in their own site before attempting to connect to domain controllers across wide area network links
- Keeps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



Replicate to all domain controllers in the AD DS domain

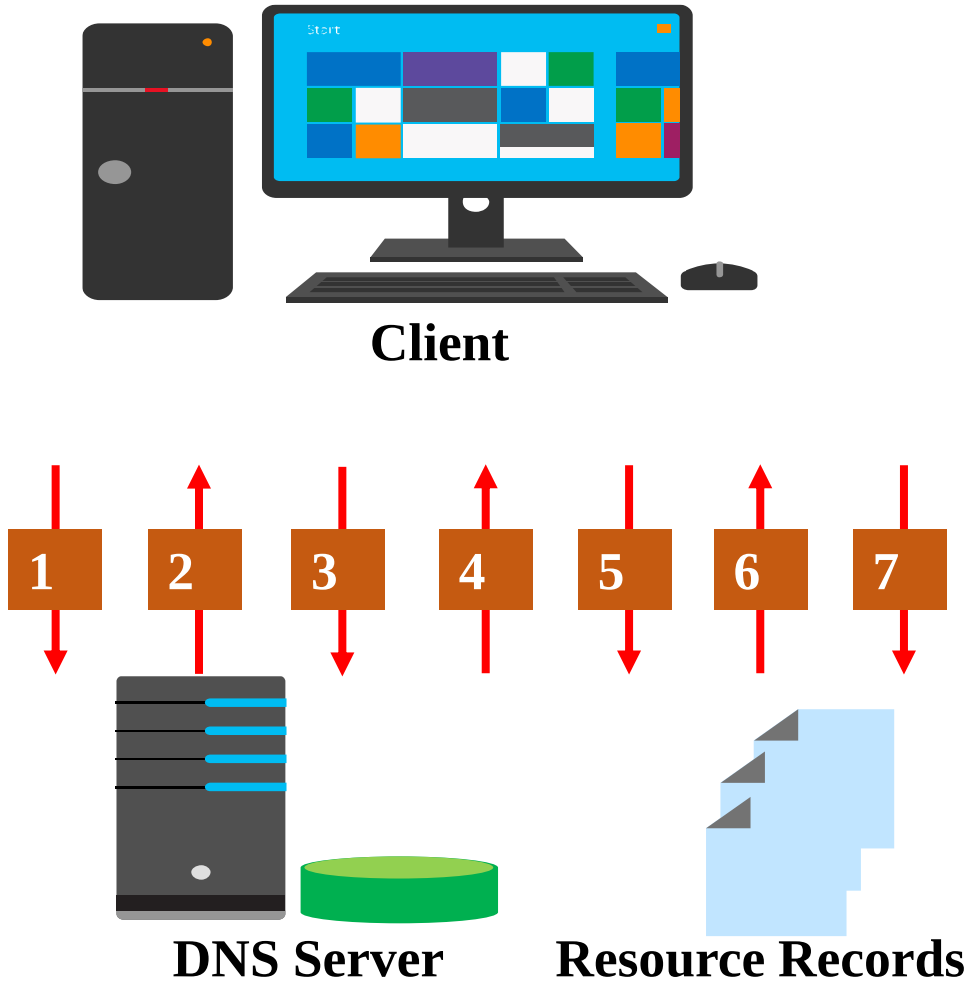
Replicate to all domain controllers that are DNS servers in the AD DS domain

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



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

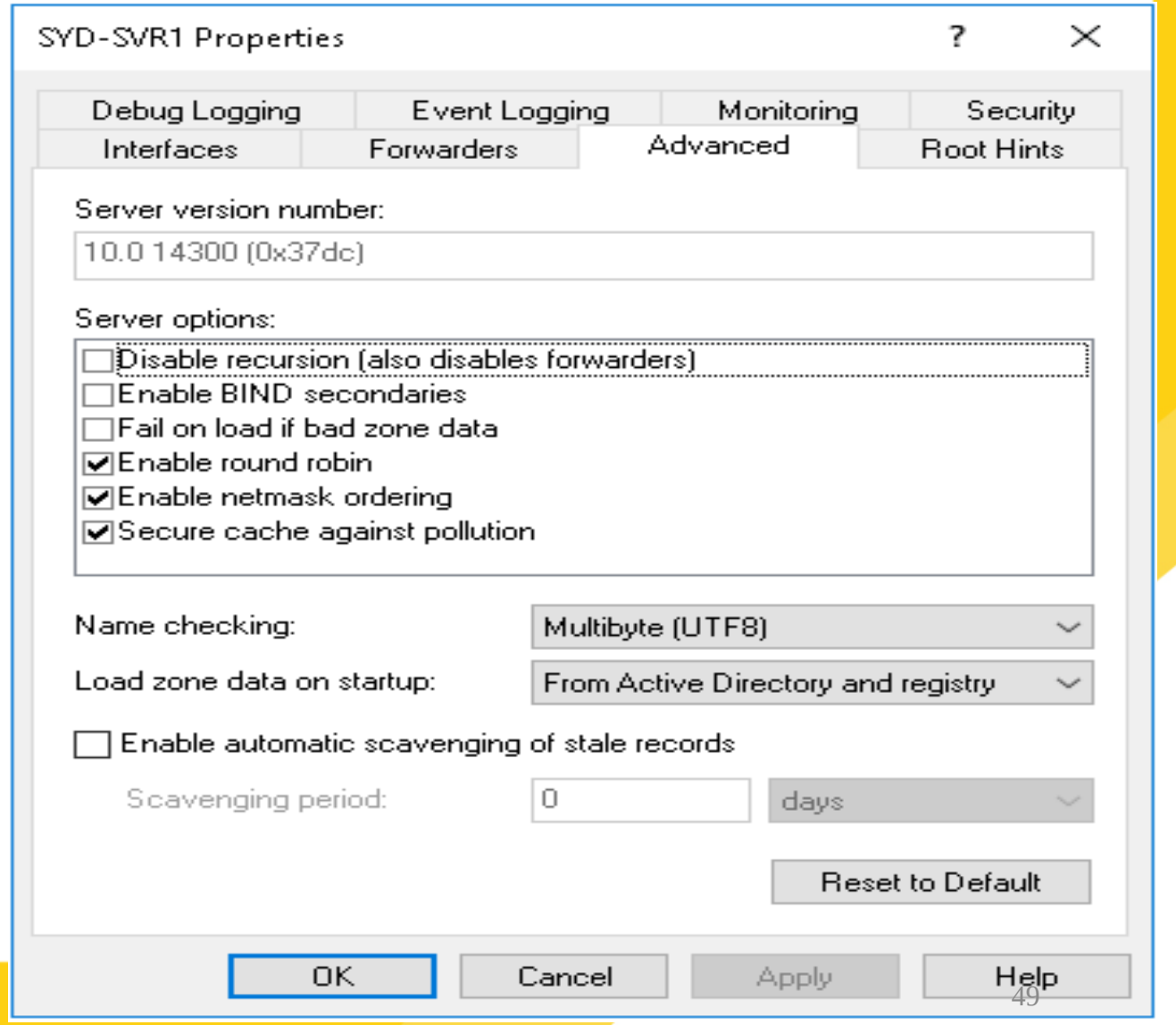
Configuring advanced DNS settings

- 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

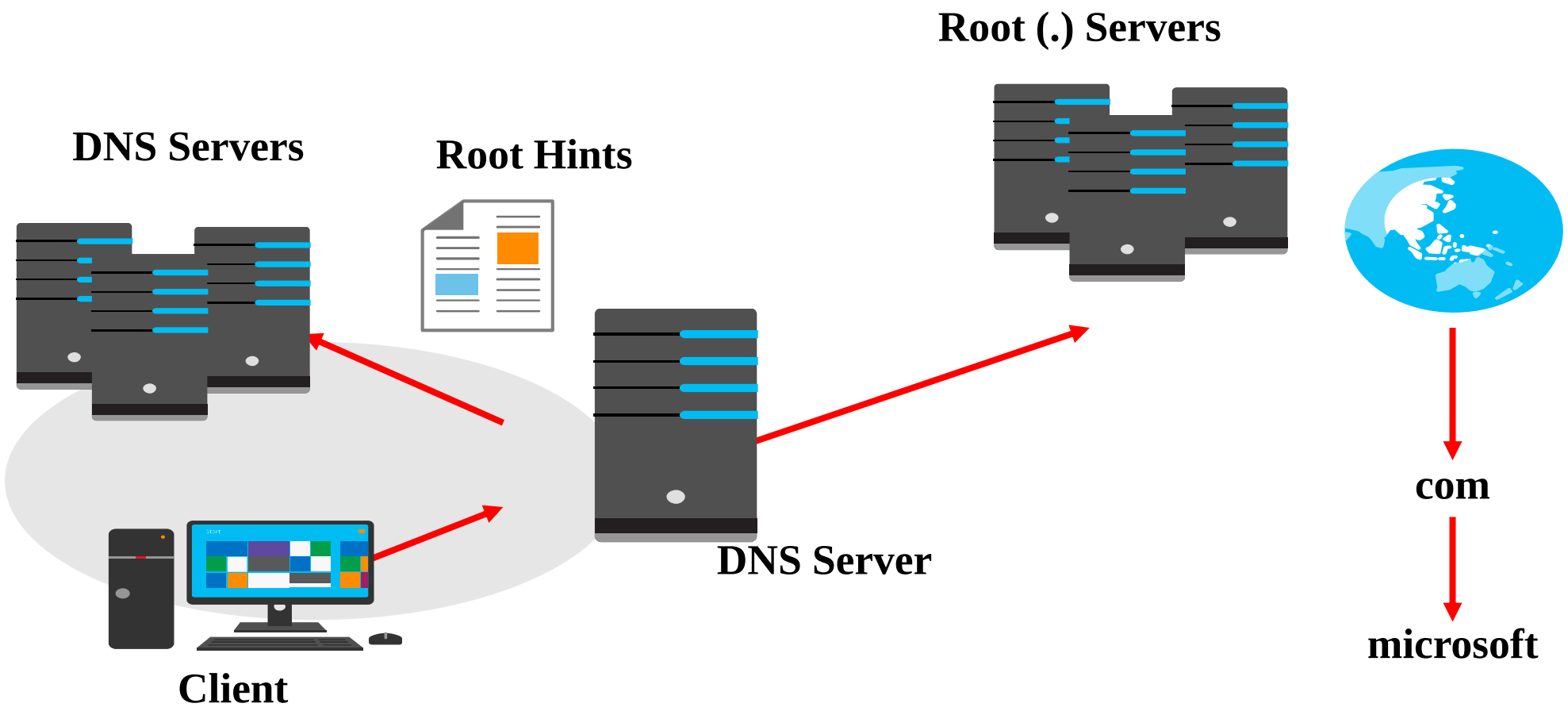
Advanced DNS name resolution:

- DNS round robin
- Netmask reordering
- Recursion



Configuring root hints

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

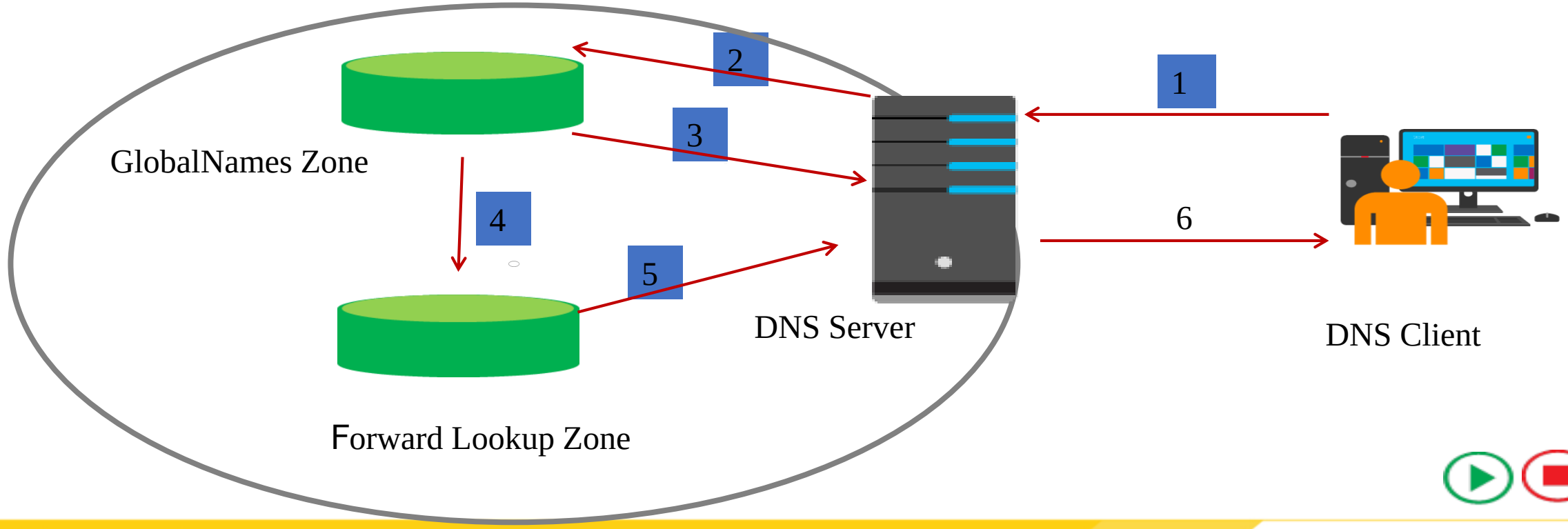


What is the GlobalNames zone?

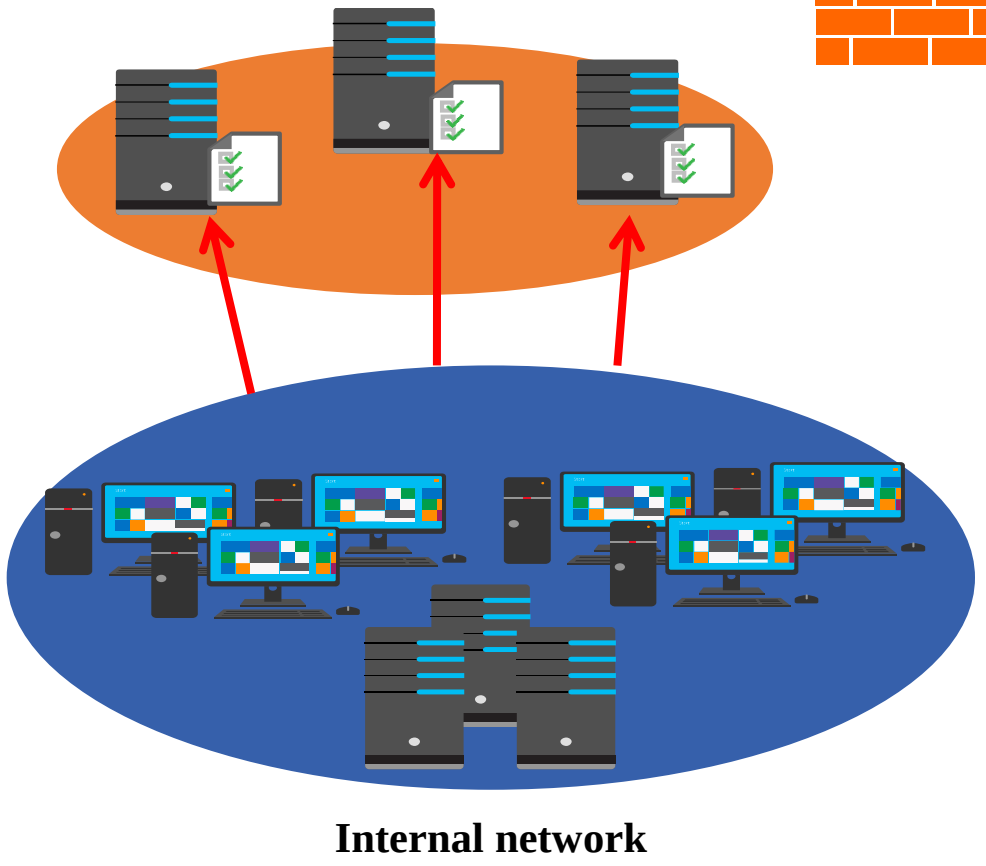
The GlobalNames zone allows single-label names to be resolved in multiple DNS domain environments

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

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

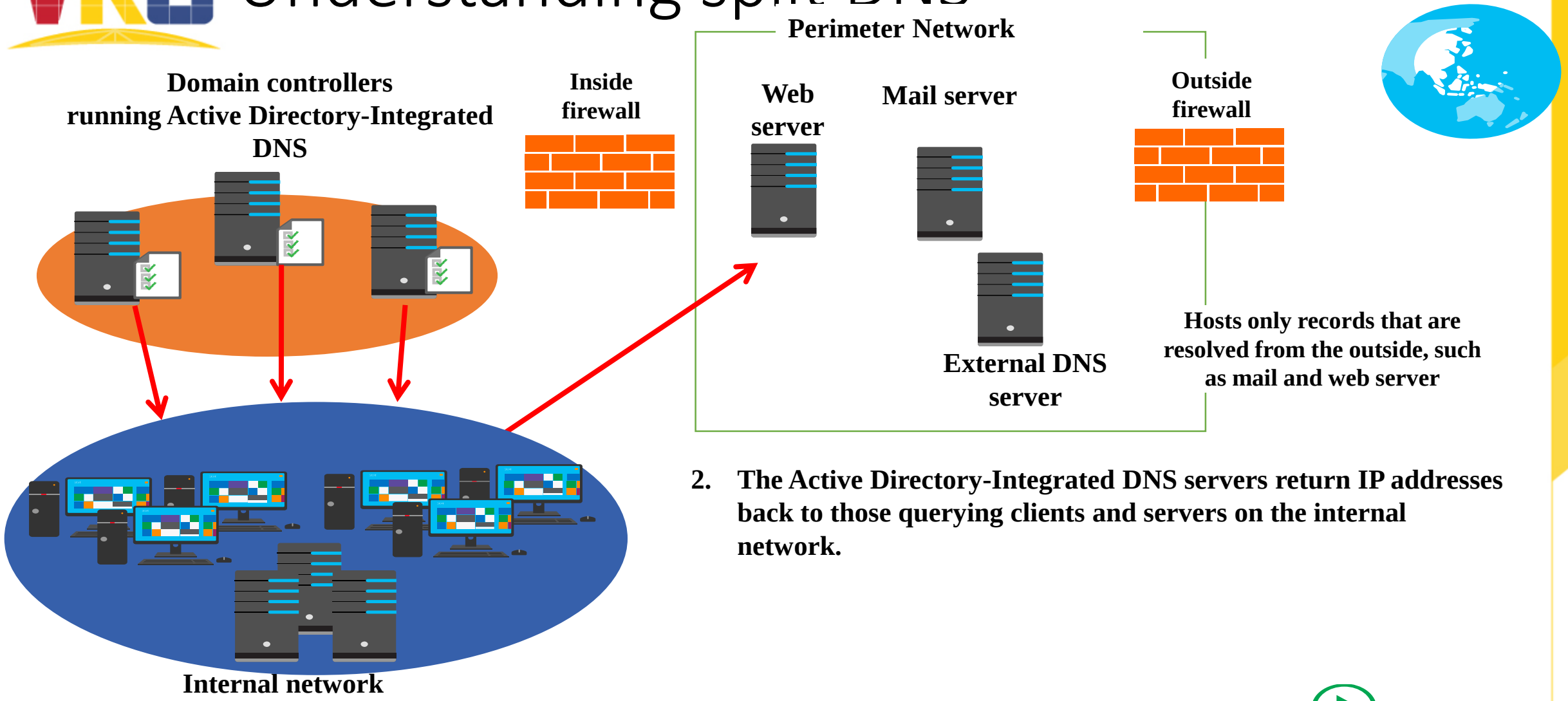


Understanding split DNS



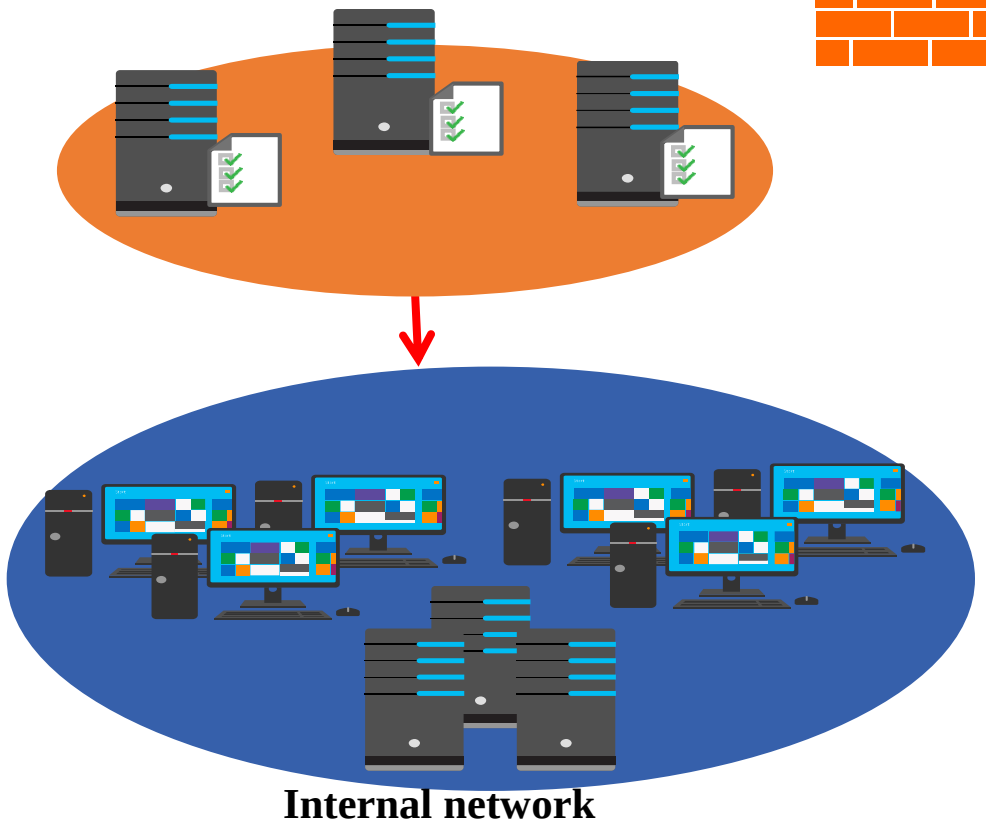
1. Clients and servers on the internal network send all DNS queries to Active Directory-integrated DNS servers.

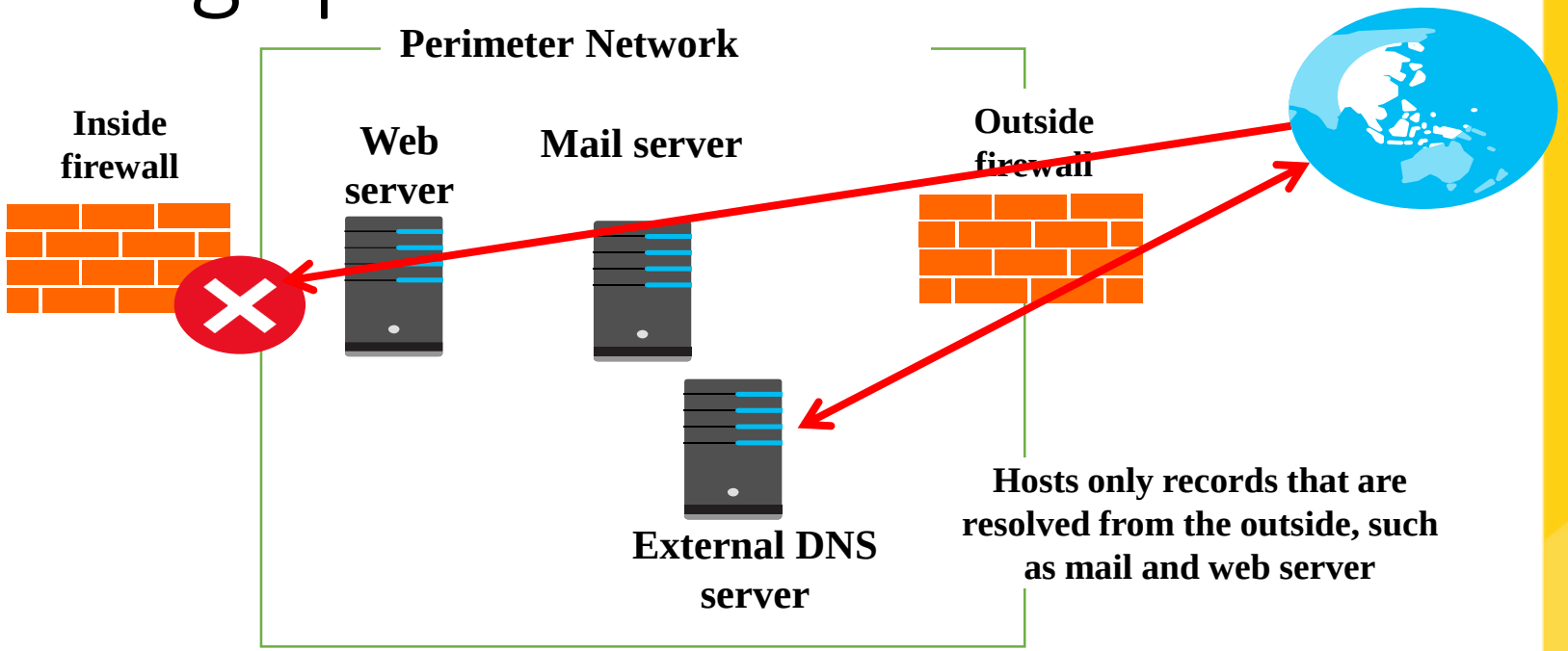
Understanding split DNS



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

Understanding split DNS





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

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

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

Understanding DHCP

- Overview of the DHCP server role
- Deploying DHCP, Managing and troubleshooting DHCP

Overview of the DHCP server role

- Benefits of using DHCP
- How DHCP allocates addresses
- How DHCP lease generation works
- How DHCP lease renewal works

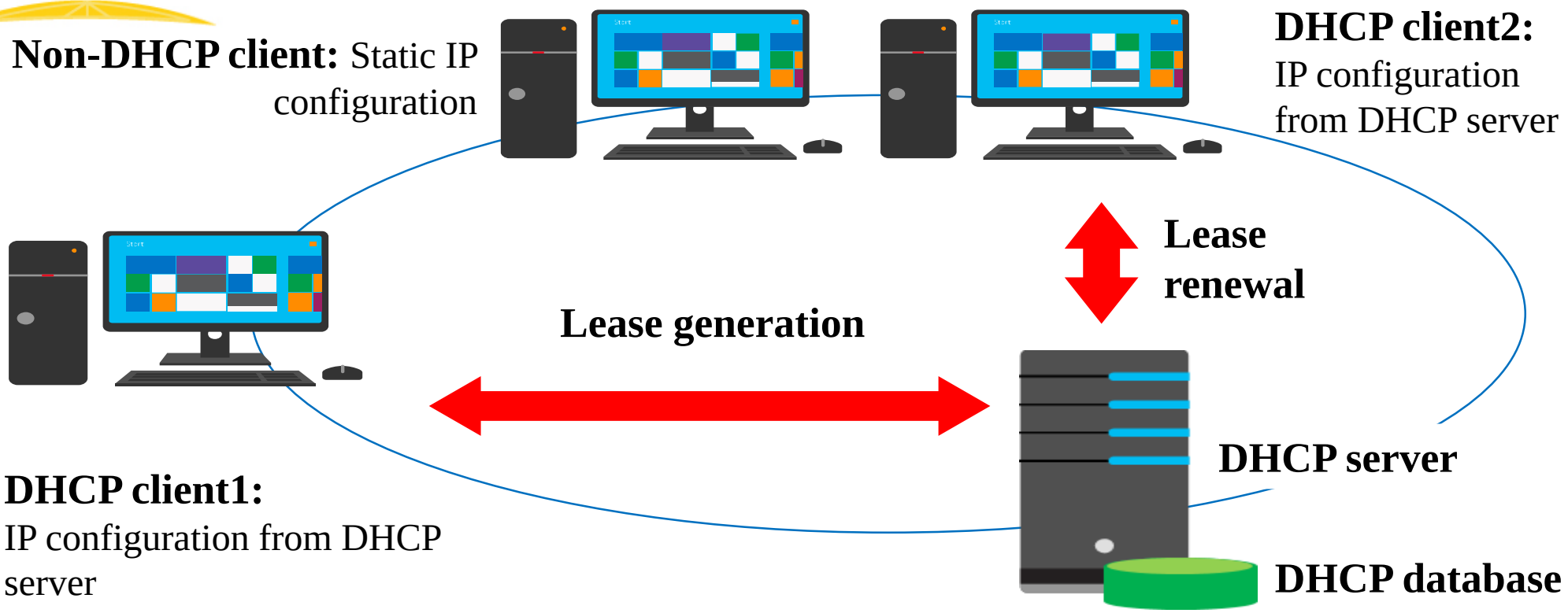
Benefits of using DHCP

DHCP reduces the complexity and amount of administrative work by using automatic IP configuration

Automatic IP configuration	Manual IP configuration
Supplies IP addresses automatically	Type IP addresses manually
Ensures correct configuration information	Typing incorrect IP address is a possibility
Updates client configuration automatically	Can result in possible communication and network issues
Eliminates a common source of network problems	Frequent computer moves increase administrative effort

IPv6 is also supported by Microsoft DHCP service

How DHCP allocates addresses

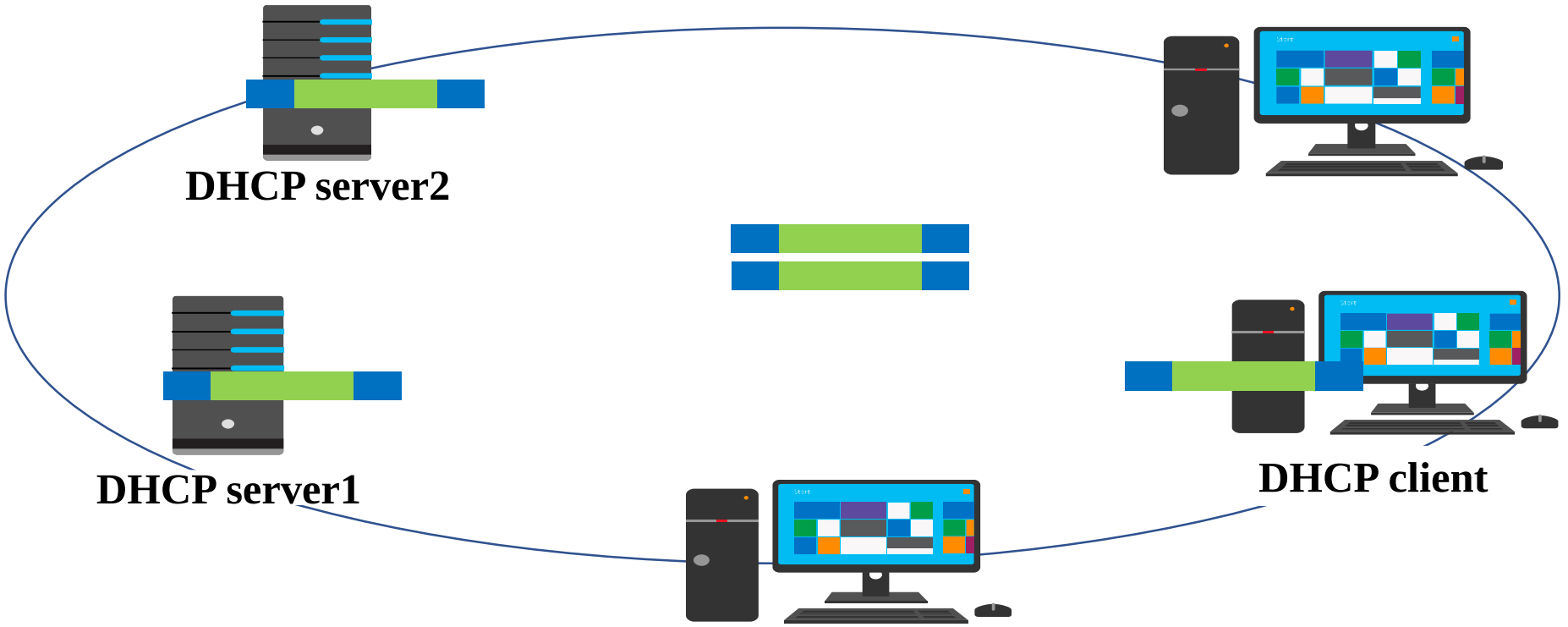


IP Address1: Leased to DHCP Client1

IP Address2: Leased to DHCP Client2

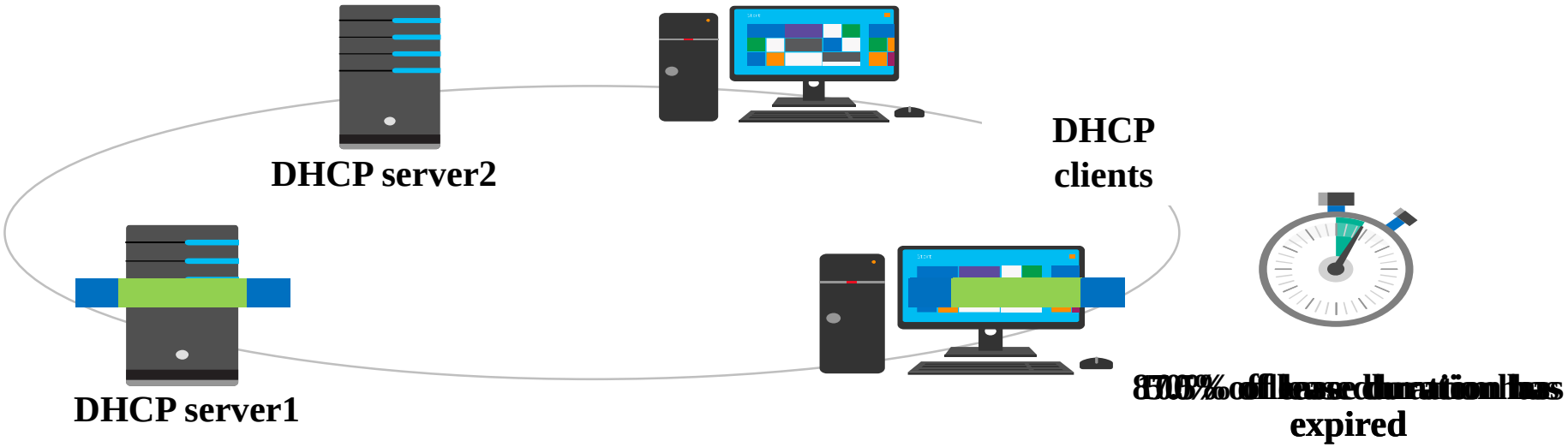
IP Address3: Available for lease

How DHCP lease generation works



1. DHCP client broadcasts a DHCPDISCOVER packet
2. DHCP servers broadcast a DHCPOFFER packet
3. DHCP client broadcasts a DHCPREQUEST packet
4. DHCP Server1 broadcasts a DHCPACK packet

How DHCP lease renewal works



1. DHCP client sends a DHCPREQUEST packet
2. DHCP Server1 sends a DHCPACK packet
3. If the client fails to renew its lease after 50% of the lease duration has expired, the DHCP lease renewal process begins again after 87.5% of the lease duration has expired
4. If the client fails to renew its lease after 87.5% of the lease has expired, the DHCP lease generation process starts over again with a DHCP client broadcasting a DHCPDISCOVER

Deploying DHCP

- Installing and configuring the DHCP server role
- DHCP server authorization
- Demonstration: Install a DHCP server and performing post-installation tasks
- Allocating and managing IPv4 addresses with DHCP
- Configuring DHCP options
- Demonstration: Configure a DHCP server
- What is a DHCP relay agent?

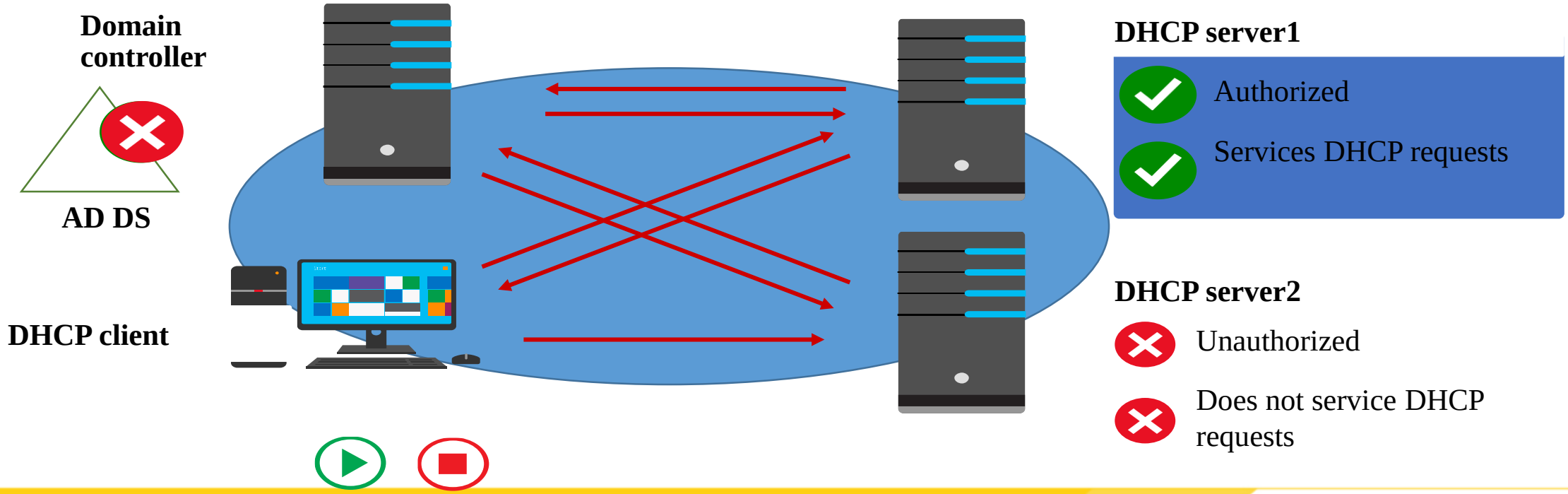
Installing & configuring the DHCP server role

- You can install the DHCP server role by using:
  - The Add Roles and Features Wizard in server manager
  - Windows PowerShell:
    - **Add-WindowsFeature DHCP**
- The server hosting DHCP requires a static IP address
- Post installation tasks include:
  - Creating DHCP security groups
  - Restarting the DHCP Server service
  - Authorizing the DHCP server in AD DS

DHCP server authorization

DHCP authorization registers the DHCP Server service in the Active Directory domain to support DHCP clients

If DHCP Server1 finds its IP address on the list, the service starts and supports DHCP clients



Demonstration: Install a DHCP server and perform post-installation tasks

In this demonstration you will learn how to:

- Install the DHCP server role
- Perform post-installation tasks

Demonstration: Install a DHCP server and perform post-installation tasks

Installing DHCP

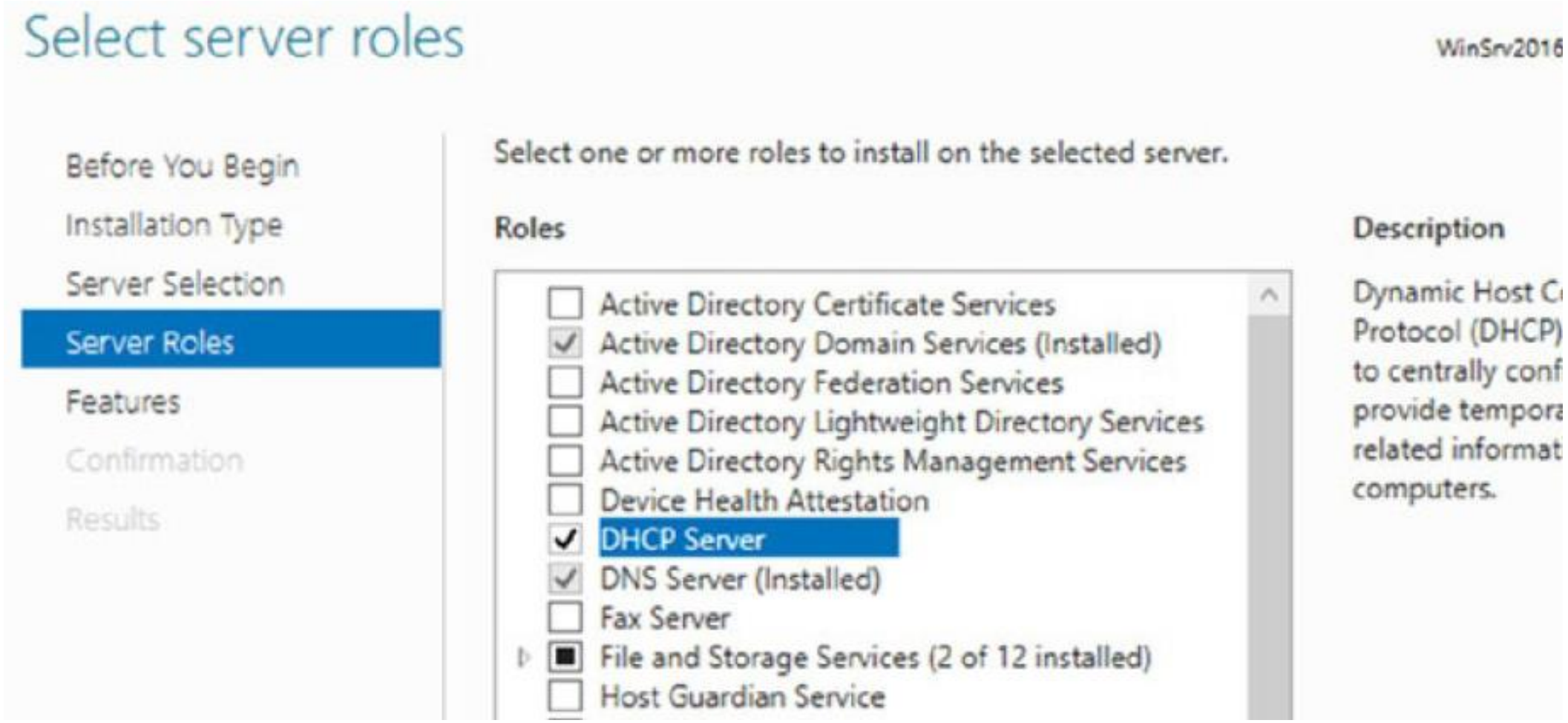
Exercise 12.1 shows you how to install a DHCP Server using Server Manager. This exercise was completed on a Windows Server 2016 Member Server since Active Directory is not installed yet.

EXERCISE 12.1

Installing the DHCP Service

1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. Choose DHCP (as shown in Figure 12.1) and click Next.

Demonstration: Install a DHCP server and perform post-installation tasks



Demonstration: Install a DHCP server and perform post-installation tasks

6. At the Features screen, click Next.
7. Click Next at the DHCP screen.
8. At the DHCP confirmation screen, click the Install button.
9. When the installation is complete, click the Close button.
10. On the left side, click the DHCP link.
11. Click the More link next to Configuration Required For DHCP Server.
12. Under Action, click Complete DHCP Configuration.
13. At the DHCP Description page, click Commit.
14. Click Close at the Summary screen.
15. Close Server Manager.

Allocating & managing IPv4 addresses with DHCP

Create scopes to define the network information that will be distributed to clients

- A scope must contain:
  - A range of IP addresses
  - A subnet mask
  - A lease duration

Allocating & managing IPv4 addresses with DHCP

- A scope might contain:
  - Default gateway address
  - DNS server and suffix
  - Other network options
- IP addresses can be reserved based on the MAC address of the client network interface

Configuring DHCP options

- DHCP options:
  - Are values for common configuration data
  - Can be applied to the server, scope, class, and reservation level
- Common scope options include:
  - Router (Default gateway)
  - DNS domain name
  - DNS servers

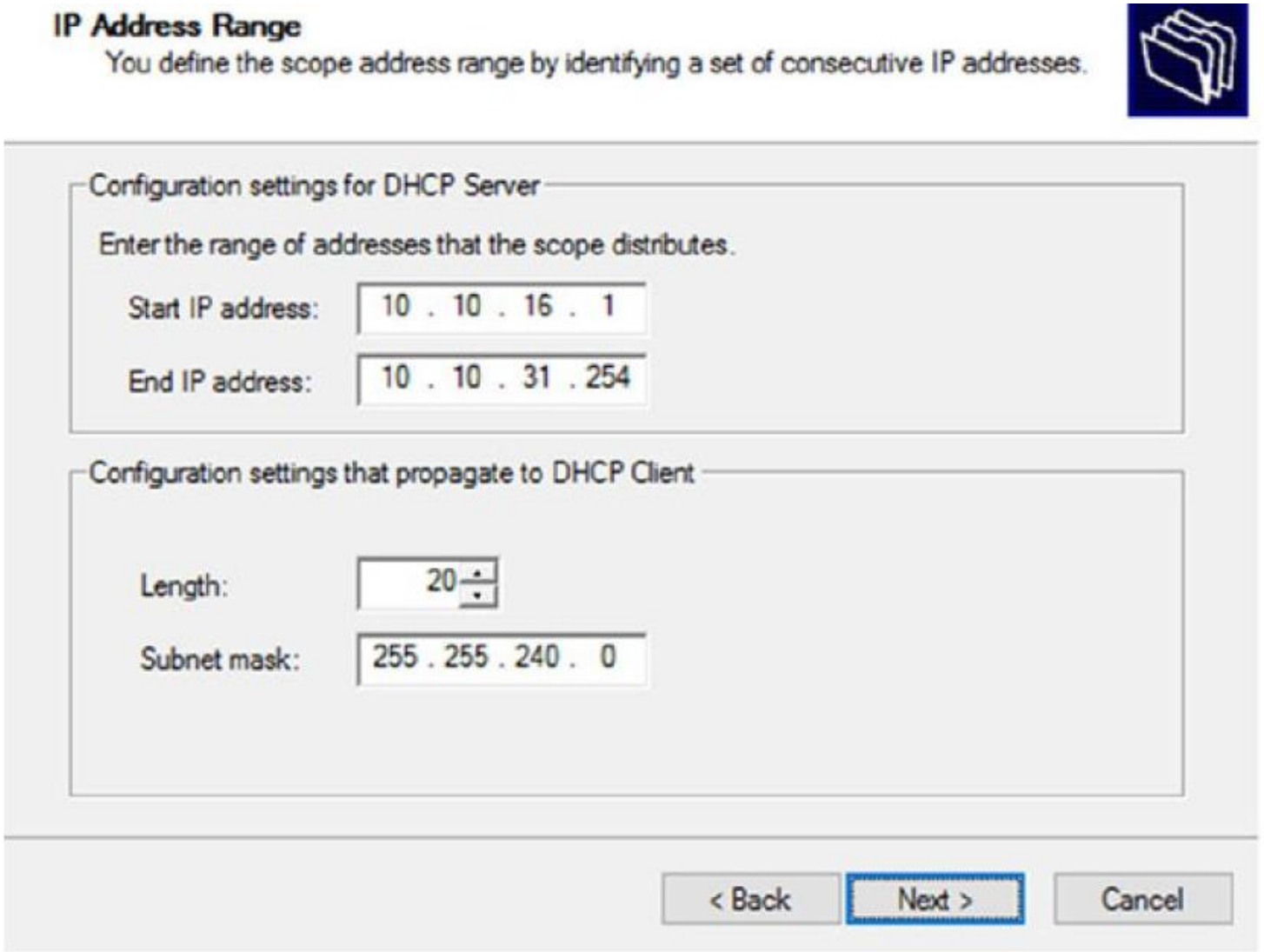
Demonstration: Configure a DHCP server

In this demonstration you will learn how to:

- Create a DHCP scope
- Configure DHCP options
- Create a DHCP reservation

Demonstration: Configure a DHCP server

- Create a DHCP scope



Demonstration: Configure a DHCP server

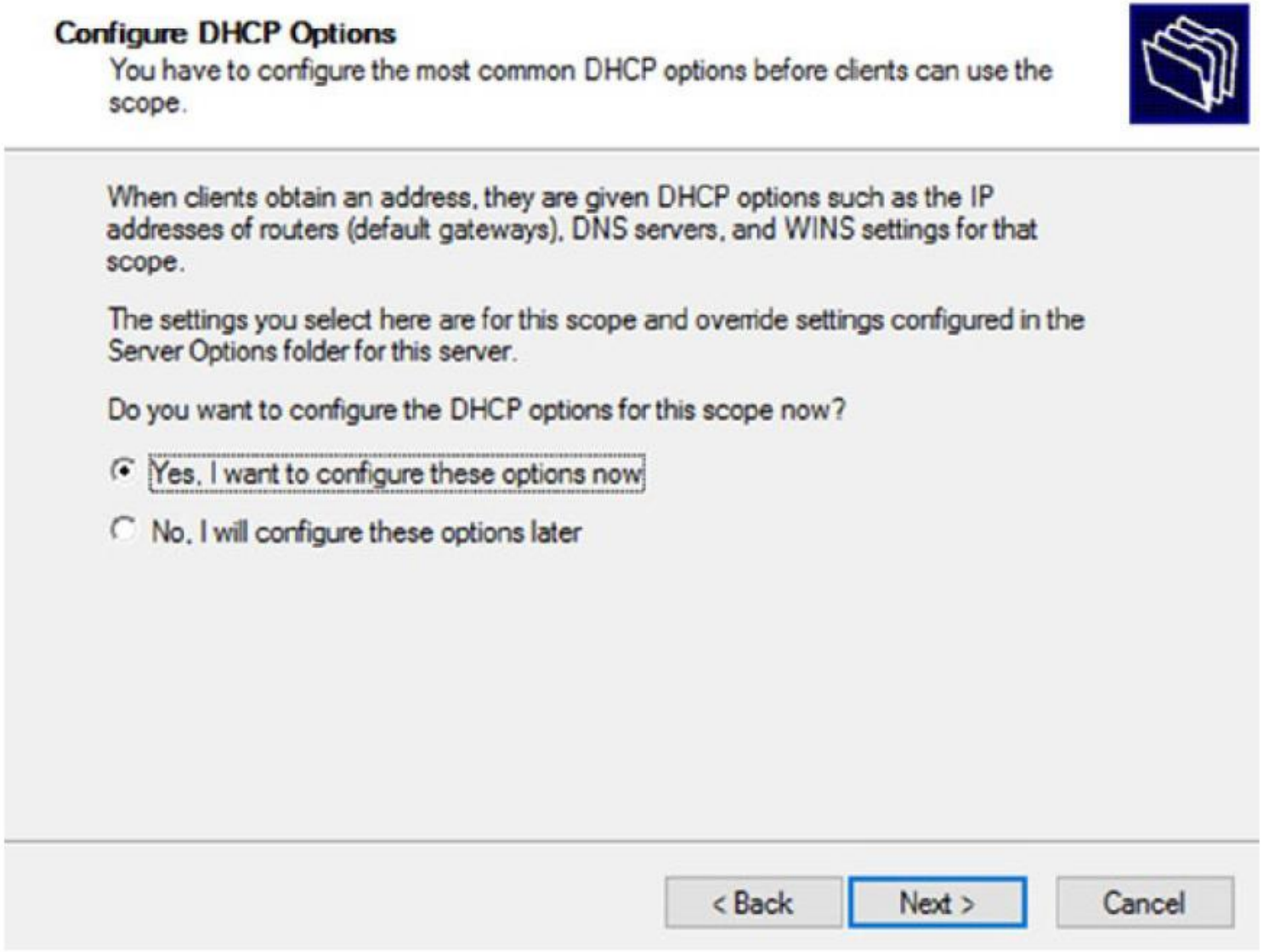
- Create a DHCP scope

You can perform the following management tasks on DHCP scopes:

- Create a scope
- Configure scope properties
- Configure reservations and exclusions
- Set scope options
- Activate and deactivate scopes
- Create a superscope
- Create a multicast scope
- Integrate Dynamic DNS and DHCP

Demonstration: Configure a DHCP server

- Configure DHCP options



Demonstration: Configure a DHCP server

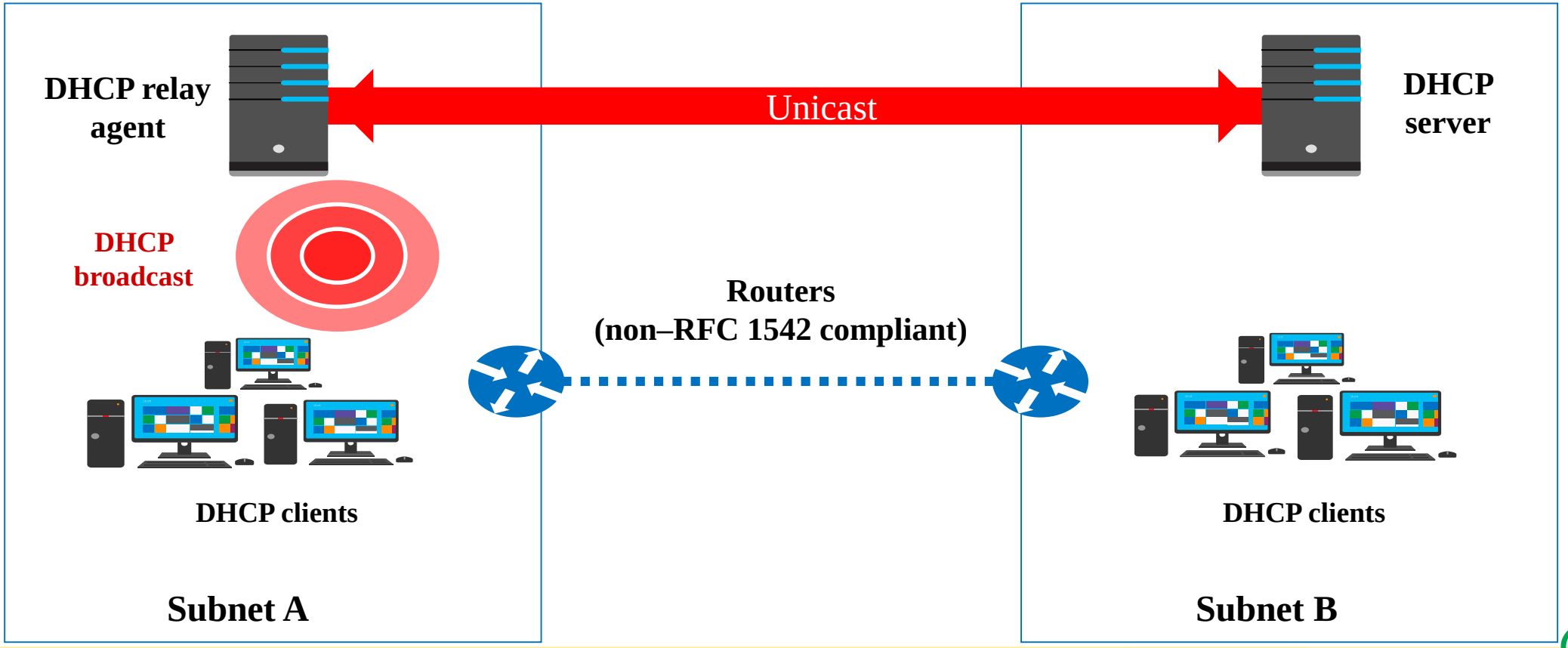
- Create a DHCP reservation

Adding a reservation is simple as long as you have the MAC address of the device for which you want to create a reservation. To add a reservation, perform the following tasks:

1. Right-click the scope and select New Reservation.
2. Enter the IP address and MAC address or ID for the reservation.
3. If you want, you can also enter a name and description.
4. For IPv4, in the Supported Types section, choose whether the reservation will be made by DHCP only, BOOTP only (useful for remote-access devices), or both.

What is a DHCP relay agent?

A DHCP relay agent listens for DHCP broadcasts from DHCP clients, and then relays them to DHCP servers in different subnets



Managing and troubleshooting DHCP

- What are DHCP security options?
- Advanced options for configuring DHCP
- Configuring superscopes and multicast scopes
- High availability options for DHCP
- What is DHCP failover?
- Demonstration: Configure DHCP failover
- Maintaining the DHCP database
- Migrating the DHCP server
- Discussion: Troubleshooting DHCP

What are DHCP security options?

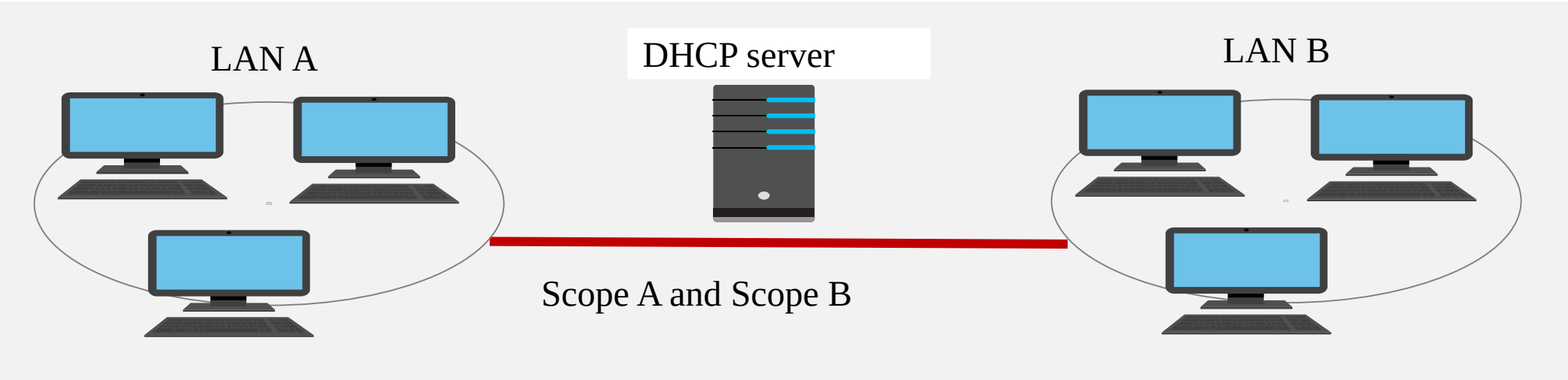
- Limit physical access to the network by:
  - Disconnecting unused LAN drops
  - Require authenticated layer 2 connections
- Enable DHCP auditing to track DHCP usage
- DHCP name protection:
  - Prevents Windows operating systems from having their DNS name registration overwritten by non-Windows operating systems using the same name
  - Uses a DHCID resource record to track the devices that originally requested the DNS name registration

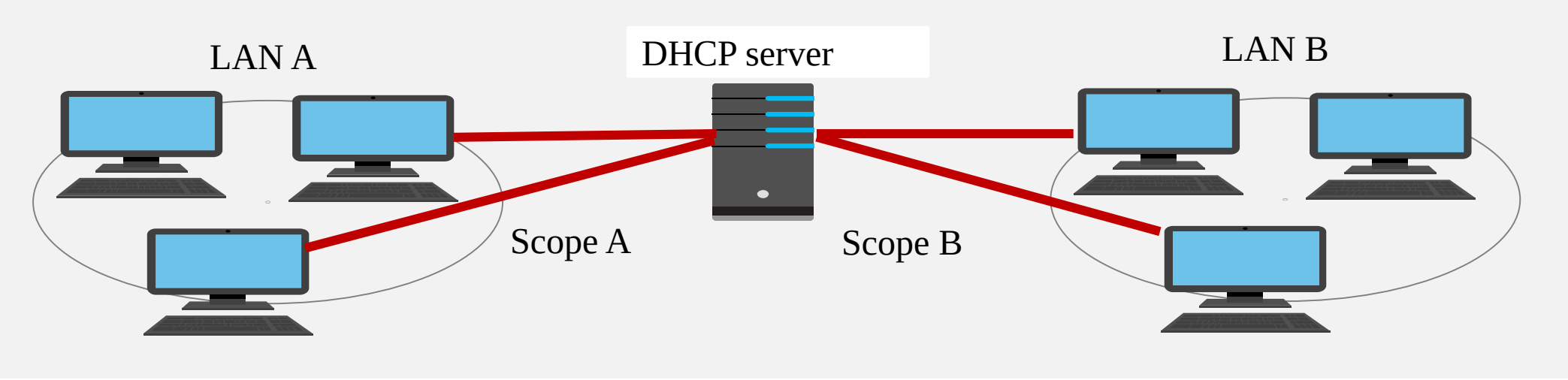
Advanced options for configuring DHCP

Policy-based assignments allow you to base IP assignment on the following criteria:

- Vendor class (defined by hardware vendors)
- User class (defined by Administrators)
- MAC address
- FQDN
- Relay agent information

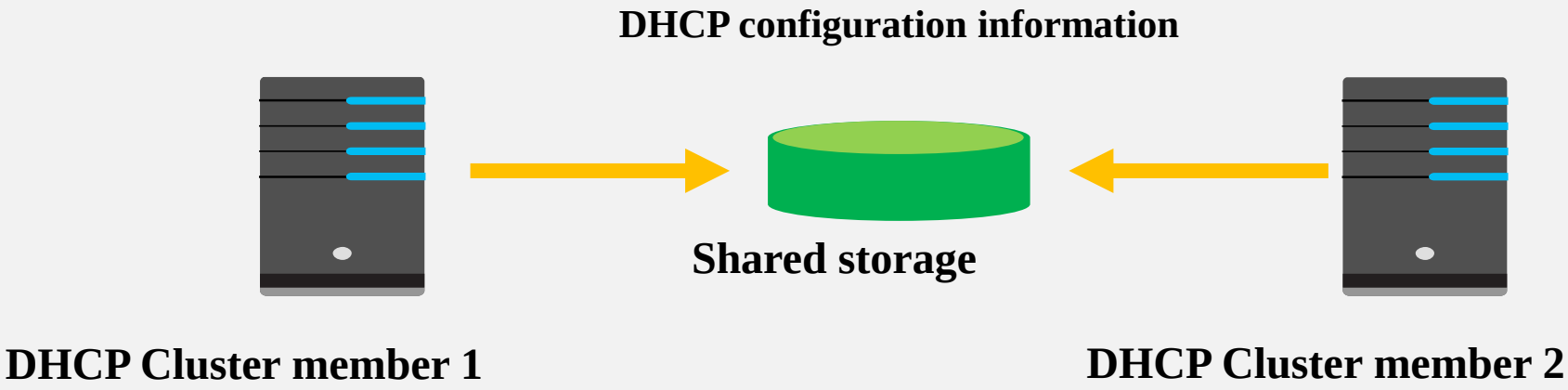
Configuring superscopes and multicast scopes



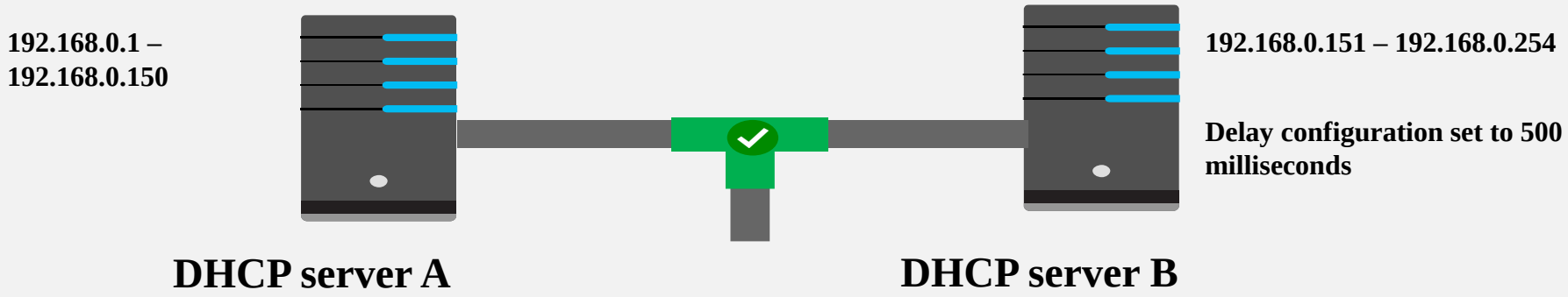


High availability options for DHCP

DHCP cluster



DHCP split scope



What is DHCP failover?

- DHCP failover:
  - Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes
  - Requires failover relationships to have unique names
  - Supports the hot standby mode and the load sharing mode

What is DHCP failover?

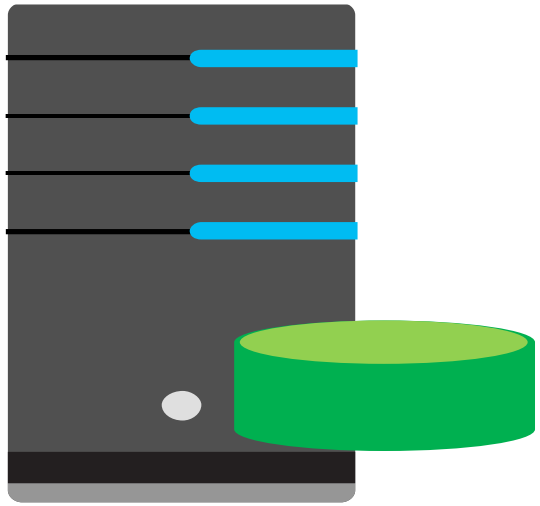
- When you use DHCP failover:
  - The MCLT determines when a failover partner assumes control of the subnet or scope
  - The auto state switchover interval determines when a failover partner is considered to be down
  - Message authentication can validate the failover messages
  - Firewall rules are auto-configured during DHCP installation

Maintaining the DHCP database

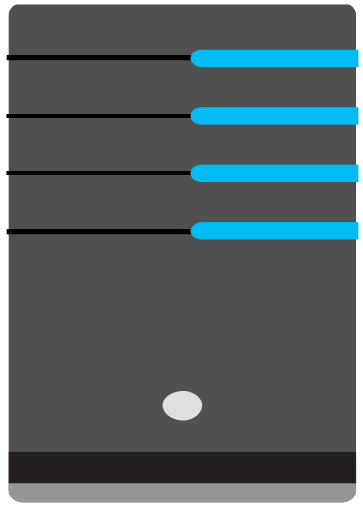
- The DHCP database (Dhcp.mdb) contains information relating to scopes, leases, reservations, and all other configuration information
- The default location of DHCP database files is **%systemroot%\system32\DHCP**
- The DHCP database is automatically backed up every 60 minutes, or can be backed up manually
- You can reconcile the DHCP database to repair inconsistencies
- You can move the DHCP database to a new DHCP server when the DHCP Server service is moved.

Migrating the DHCP server

- You can migrate the DHCP server by exporting the DHCP data from the old server and importing it to the new server
- You can use Windows PowerShell or NetShell commands



Export data from current server to a file

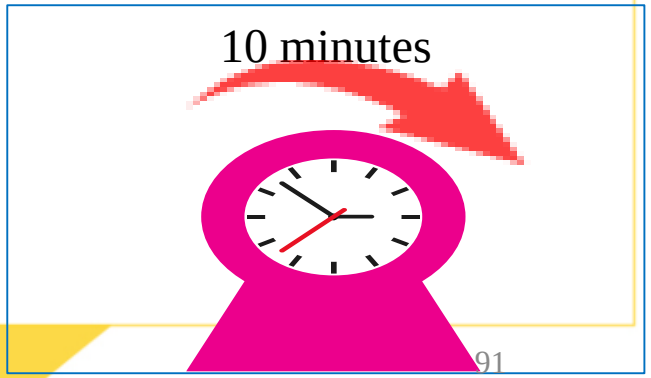


Import data to new server from the file

Discussion: Troubleshooting DHCP

How do you address the following issues that can occur when you do not configure DHCP properly?

- Address conflicts
- Failure to obtain a DHCP address
- Address obtained from an incorrect scope
- DHCP database suffered data corruption or loss
- DHCP server has exhausted its IP address pool



SUMMARY

- Understanding DNS
- Installing and configuring DNS
- Understanding DHCP
- Installing and configuring DHCP


Q&A