Chapter 4

DHCP and DNS

Tran Thanh Dien, PhD

August, 2024

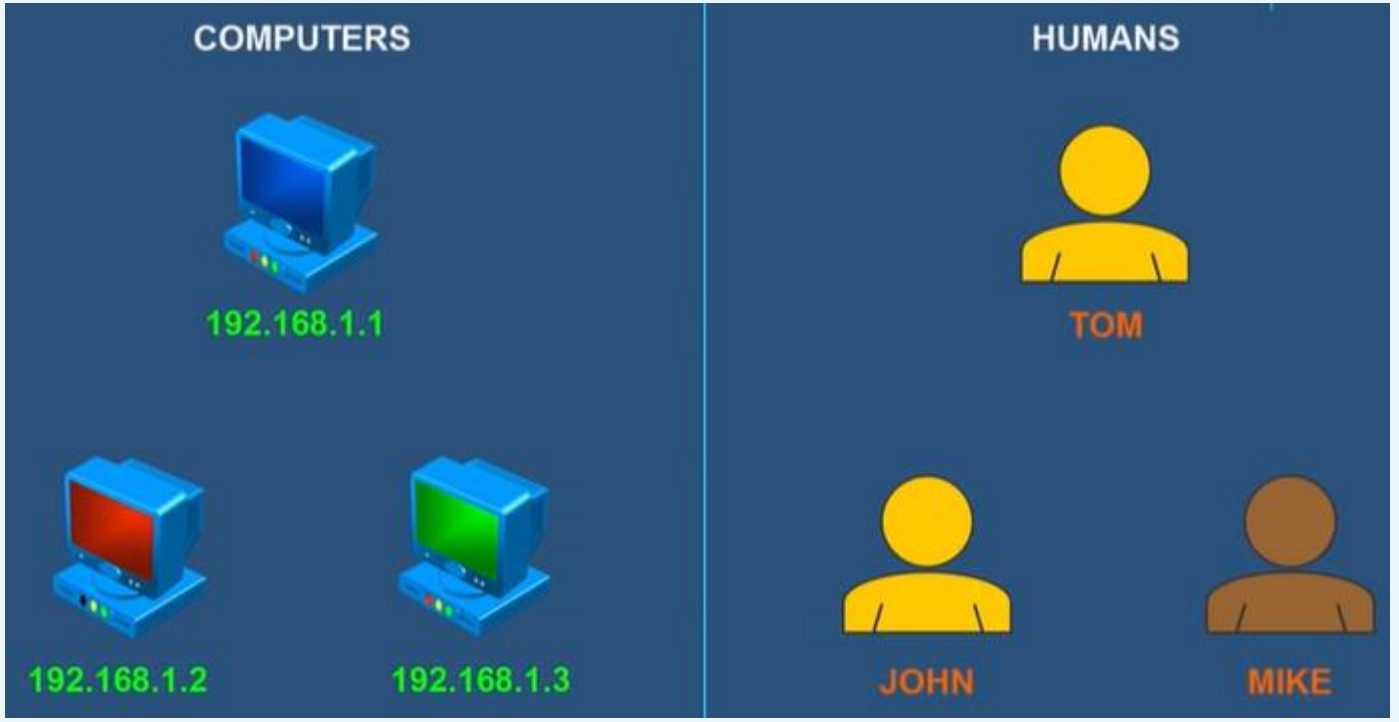
CANTHO UNIVERSITY

Content

- The purpose of DNS
- Types of DNS zones
- Types of DNS records
- DHCP
- Creating a DHCP scope

The purpose of DNS

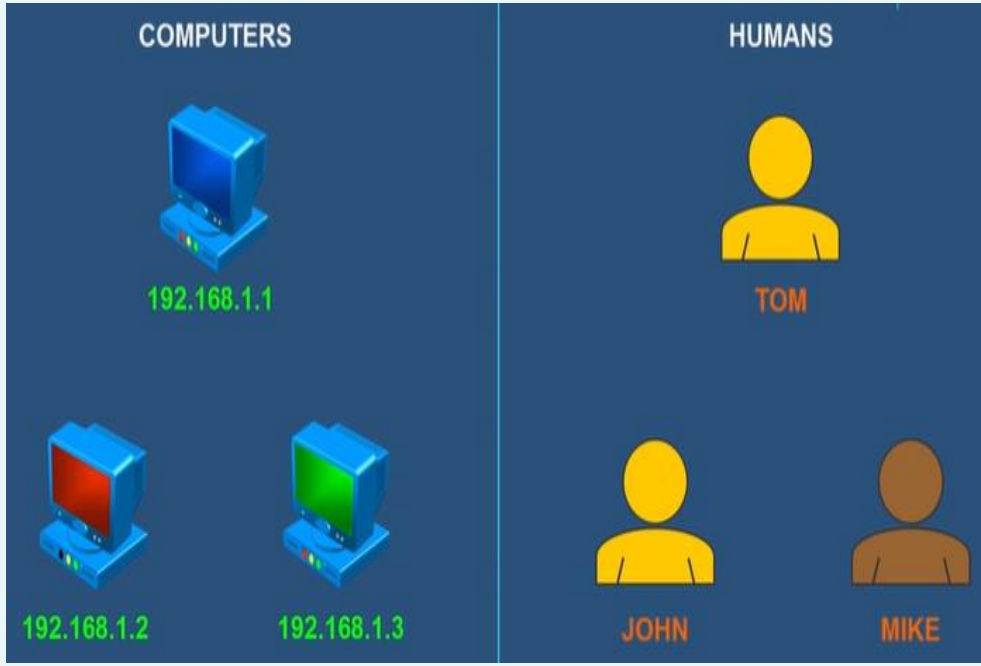
- In the world of networking, computers and devices identify and talk each other over a network using numbers (e.g., IP address)
- On the other hand, Humans are accustomed to using names



The purpose of DNS

- To bridge the gap to make the communication a lot easier, DNS developed
- DNS resolves names to numbers, i.e., domain names to IP addresses

- Basically, DNS works like a phone book:
  - When you find a number, you don't look up the number first.
  - You look up the name first then it will give you the number



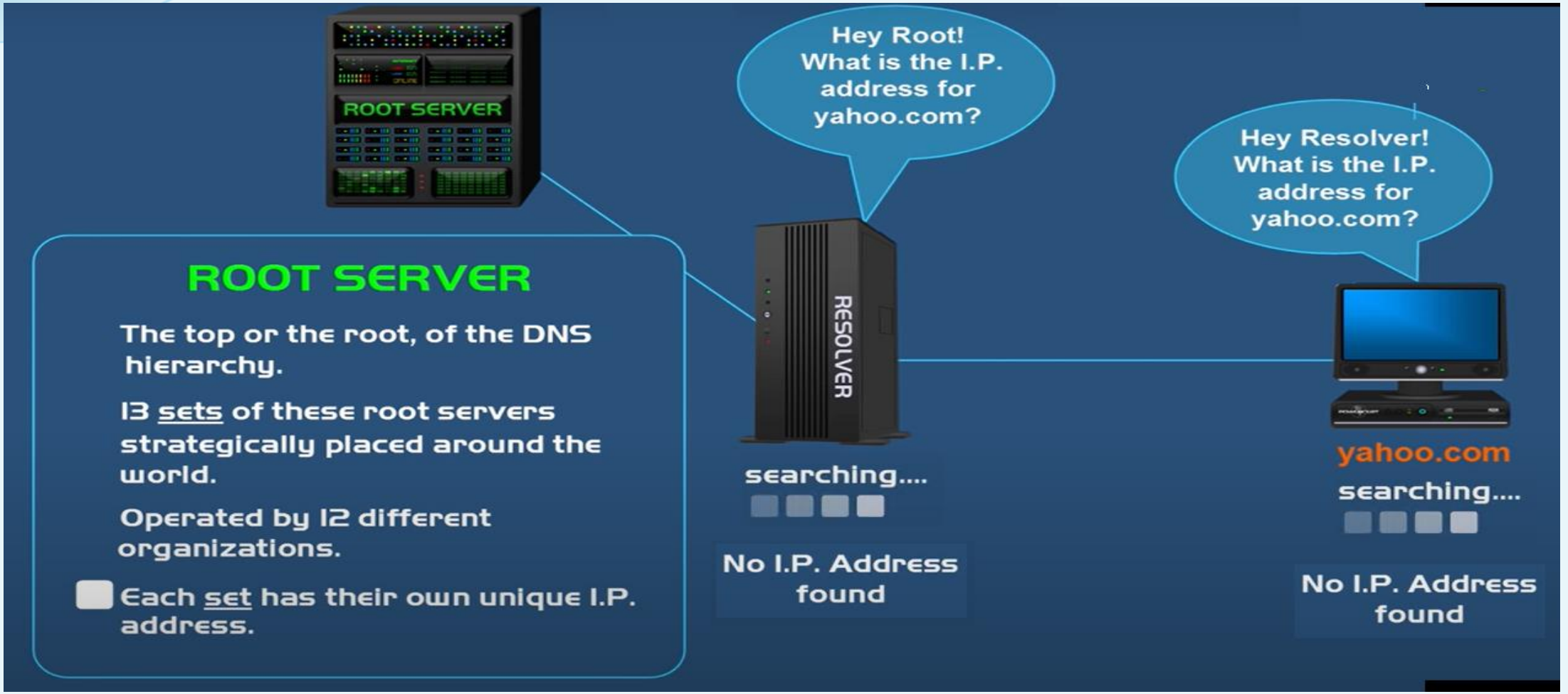
DNS

How DNS works

- Example

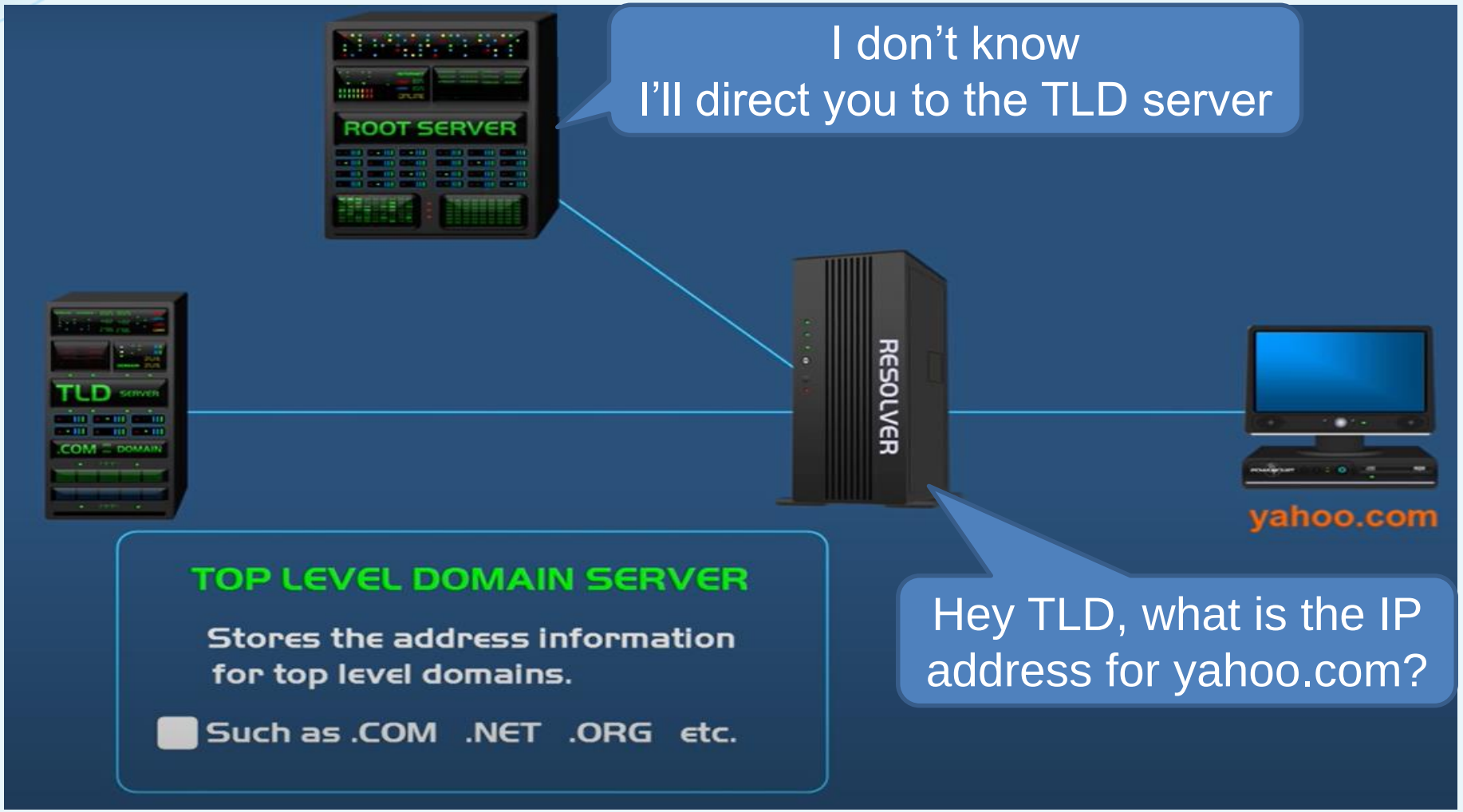
DNS

How DNS works



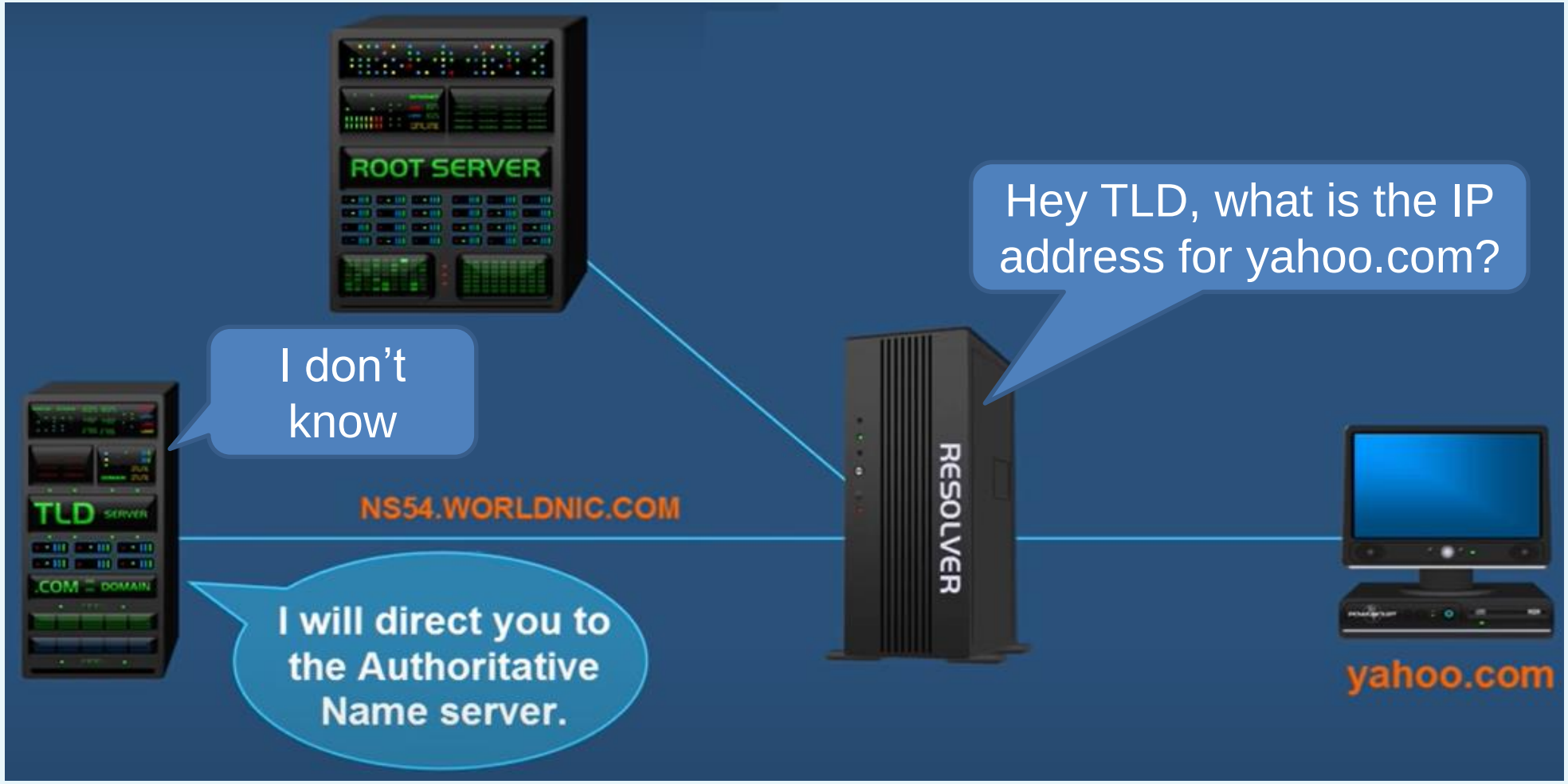
DNS

How DNS works



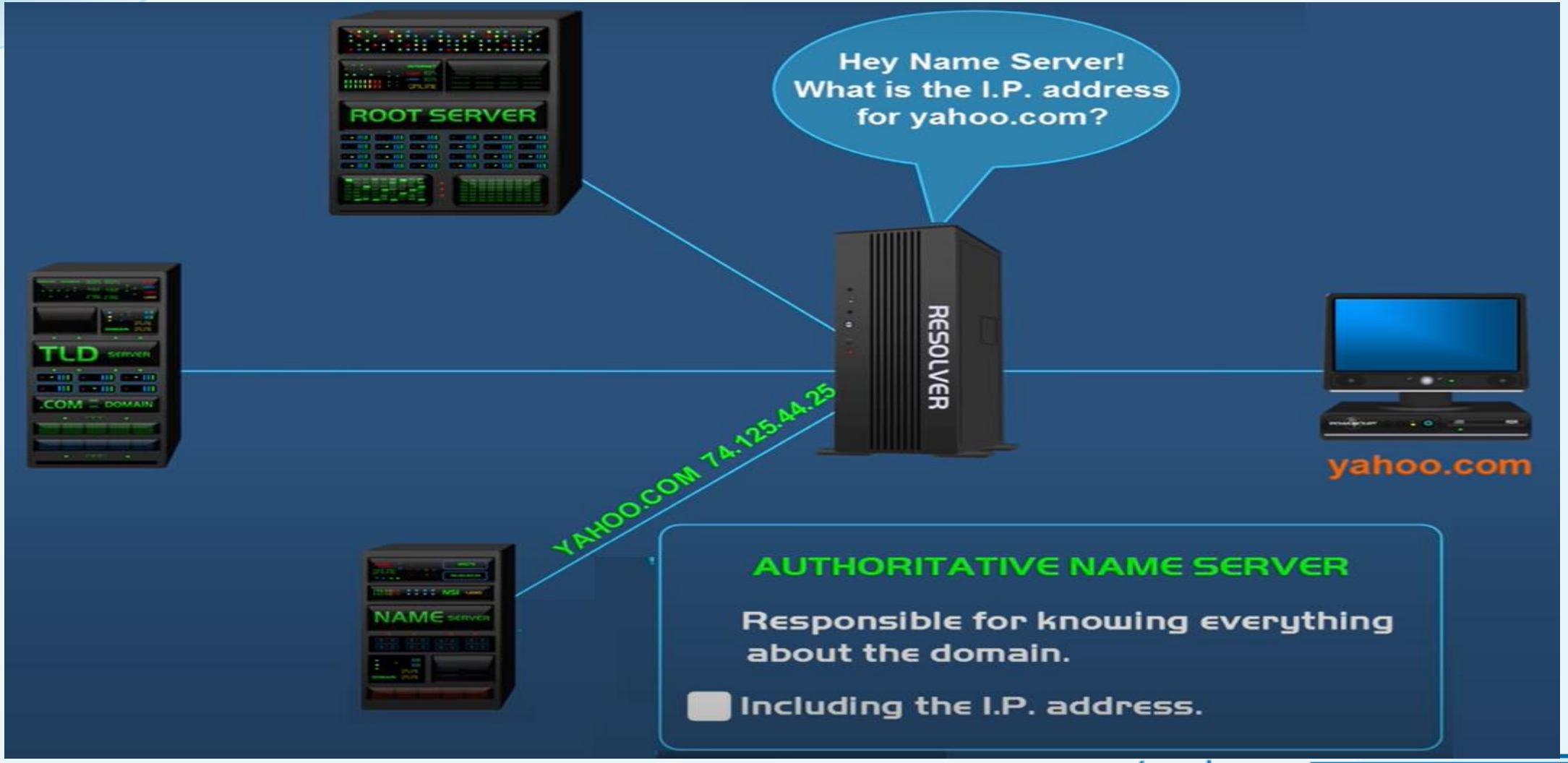
DNS

How DNS works



DNS

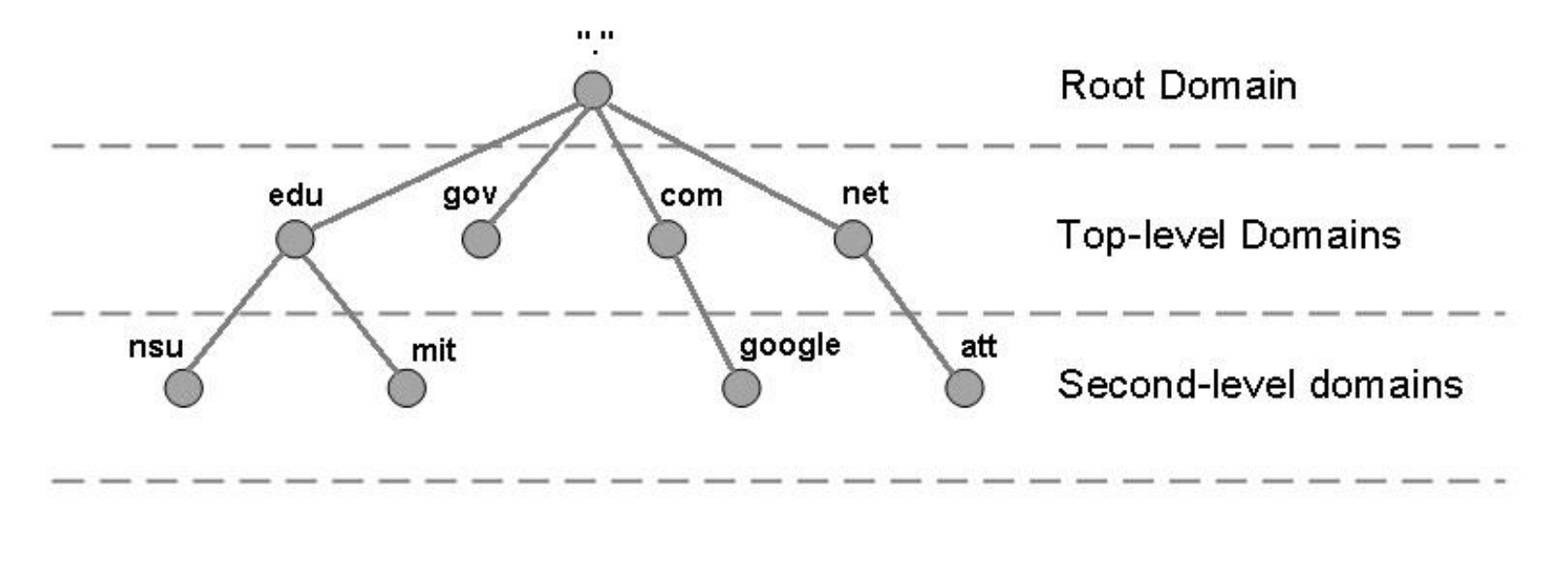
How DNS works



DNS

A hierarchically distributed database

- DNS – a hierarchically distributed database:
  - Its layers are arranged in a definite order
  - And its data is distributed across a wide range of machines
- Establishes an inverted logical tree structure called the domain namespace

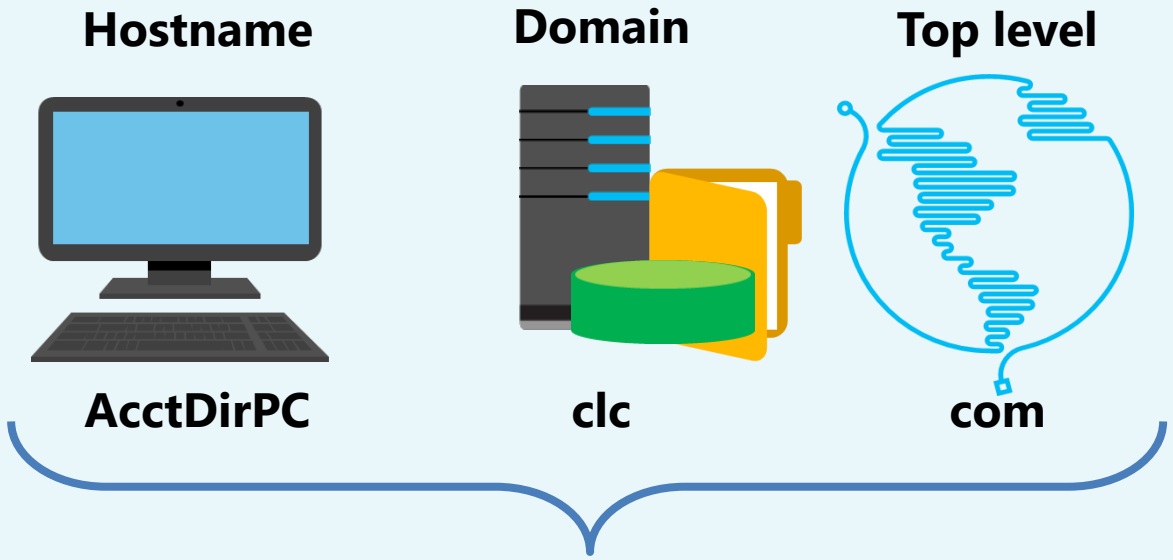


Each node, or domain, in that space has a unique name.

DNS

Fully qualified domain name

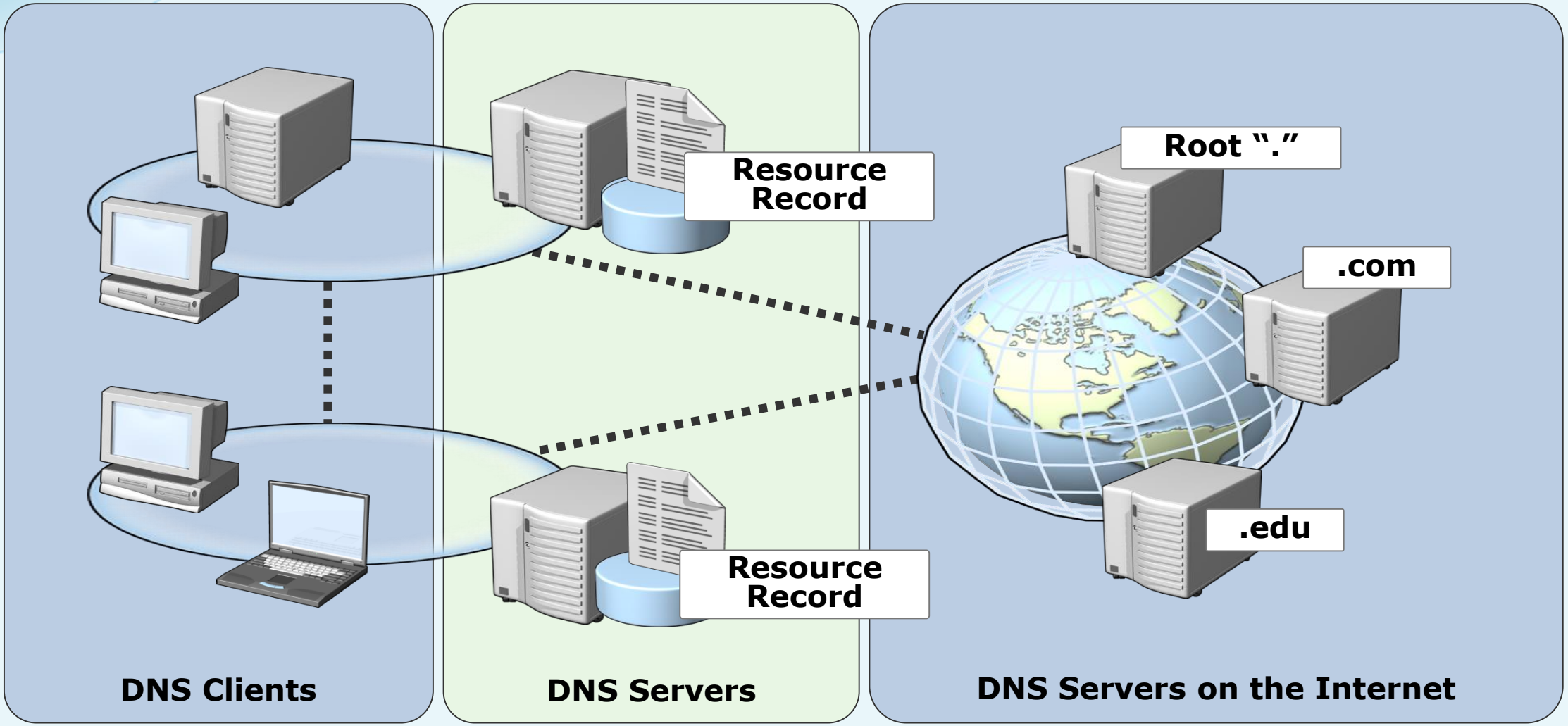
- If someone wanted to contact that host, they would use the Fully Qualified Domain Name (FQDN)
- A computer name added to a domain name and top level domain to make a FQDN



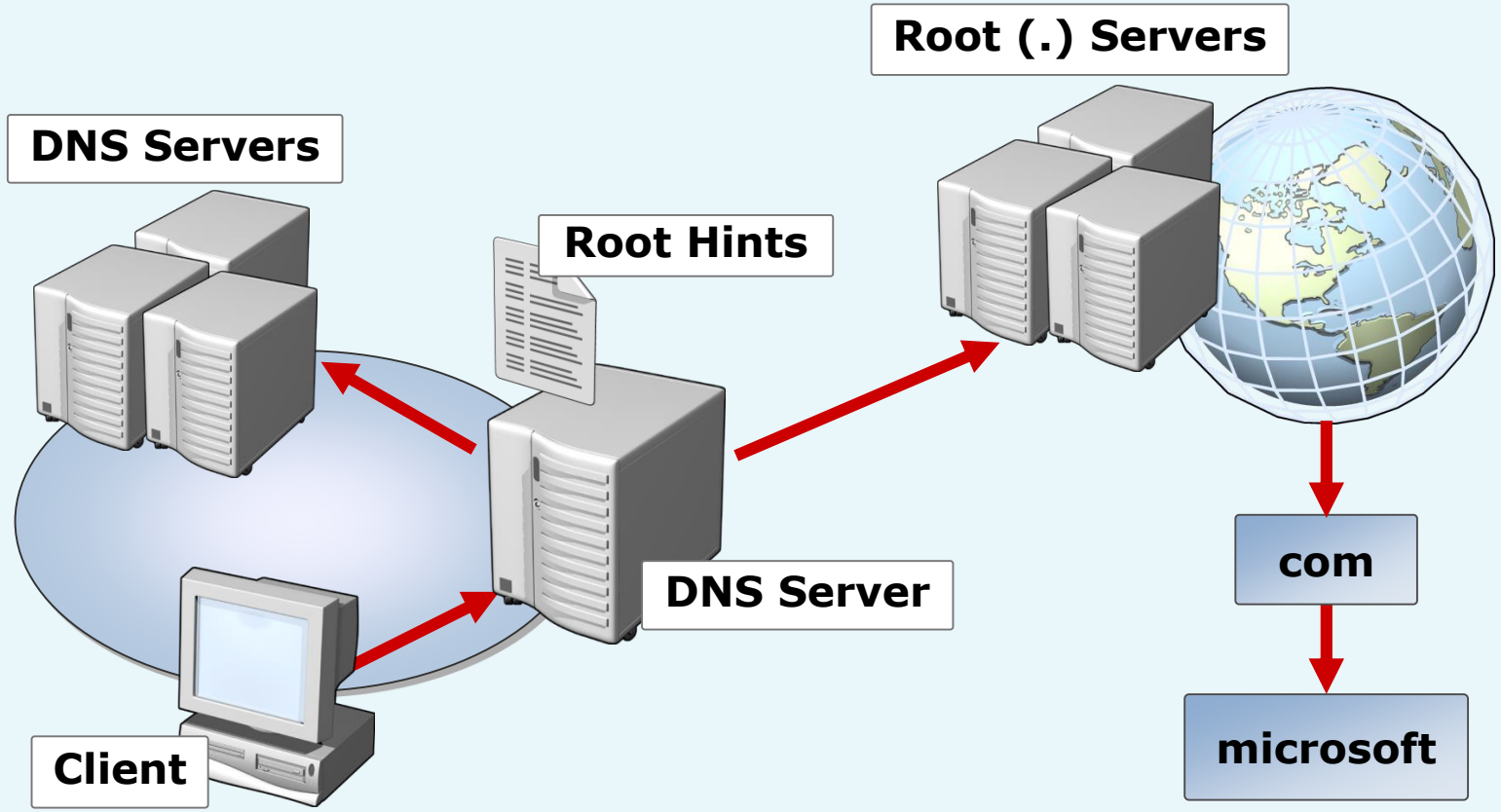
Fully qualified domain name = AcctDirPC.clc.com

DNS

DNS Architecture



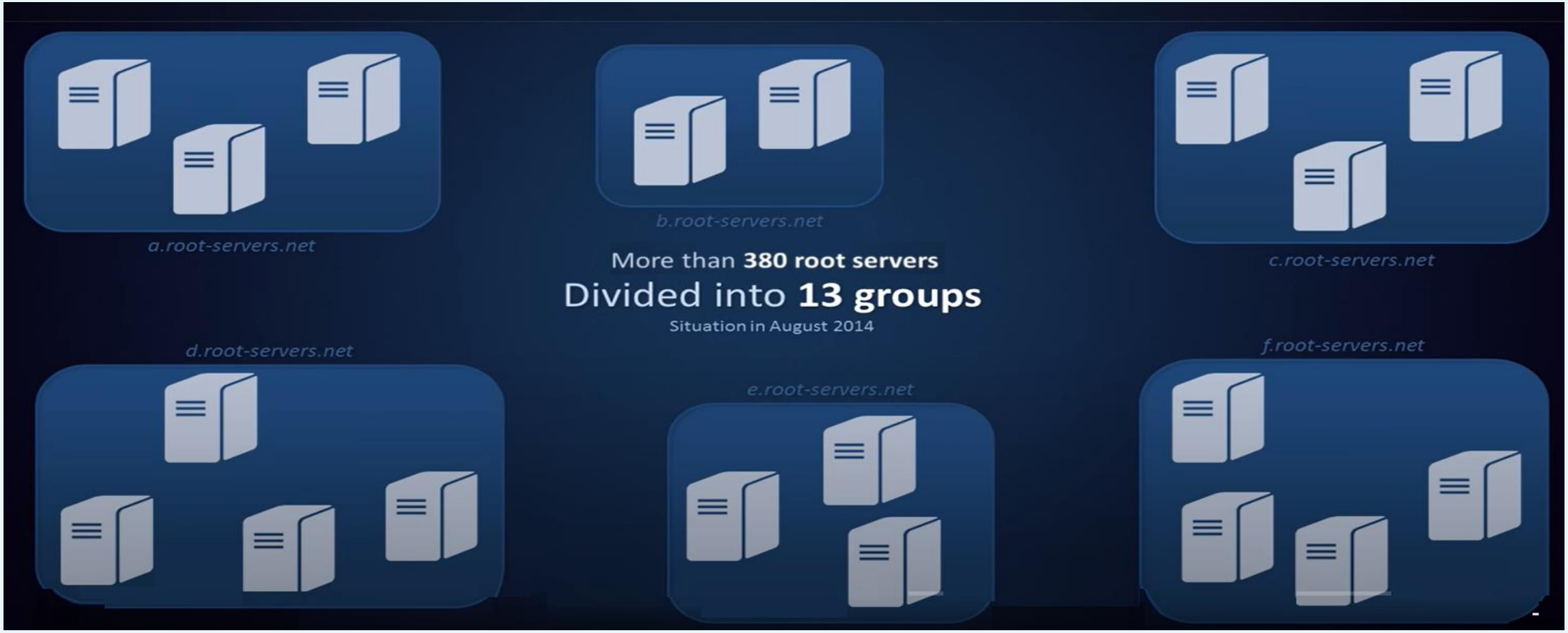
Root hints contains IP of root servers



DNS

The root name servers

The root name servers know other TLD servers



DNS

The TLD servers

The rightmost part of every domain name

DNS

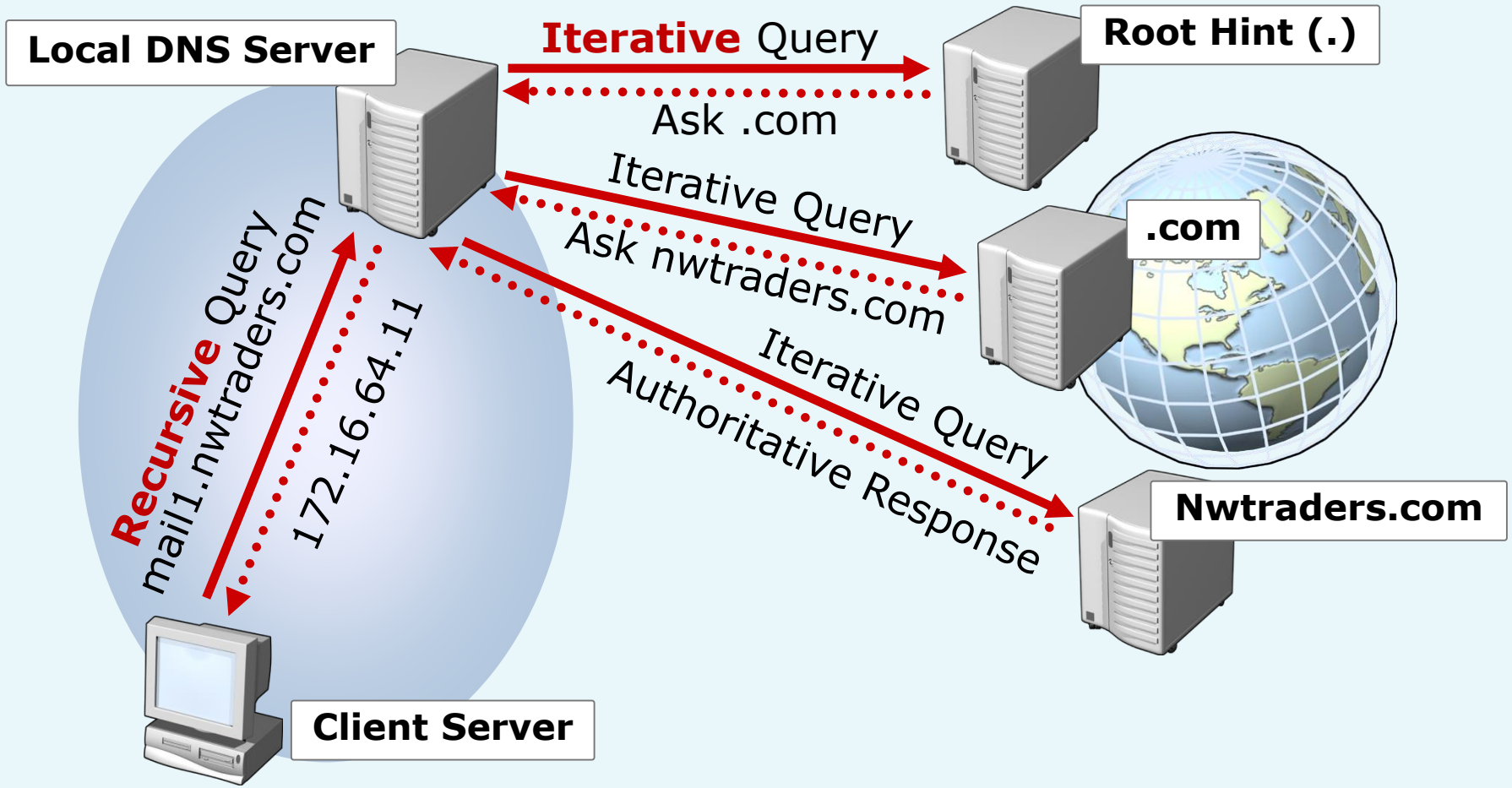
Authority Name servers

- Name server giving answers in response to questions asked about names in a zone

Google.com yahoo.com ctu.edu.vn

DNS

DNS queries



DNS

Infrastructure components

- DNS is a standard set of protocols that defines the following:
  - A mechanism for querying and updating address information in the database
  - A mechanism for replicating the information in the database among servers
  - A schema of the database
- DNS infrastructure components include**: DNS server**; **DNS zone**; **DNS resolvers**; **Resource records**

DNS

Infrastructure components: DNS server

- DNS server is responsible for:
  - storing and resolving all of the names on the network
  - turning FQDN into something else in order to get the traffic to the correct destination
- DNS servers work together to resolve hierarchical names
  - If a server already has information about a name, it simply fulfills the query for the client.
  - Otherwise, it queries other DNS servers for the appropriate information.

DNS

Infrastructure components: DNS Database zones

- A DNS zone is a specific portion of DNS namespace over which a specific DNS server has authority
- DNS zone contains ***resource records*** defining the hosts and other types of information that make up the database for the zone.
- **Zone types**:
  - Primary zones
  - Secondary zones
  - Stub Zones

Primary zones

- Responsible for maintaining all of the records for the DNS zone
- It contains the primary copy of the DNS database
- All record updates occur on the primary zone
- Two types of primary zones:
  - Primary zone: Local database (stored locally in a file on the server)
  - Primary zone with Active Directory Integration (Active Directory DNS)
    - The DNS database is stored in Active Directory.
    - All Active Directory DNS servers can have access to the same data
    - It has to reside on a domain controller

Secondary zones

- Noneditable copies of the DNS database
- Used for load balancing
- Gets its database from a primary zone
- It can be used to resolve DNS requests

Stub zones

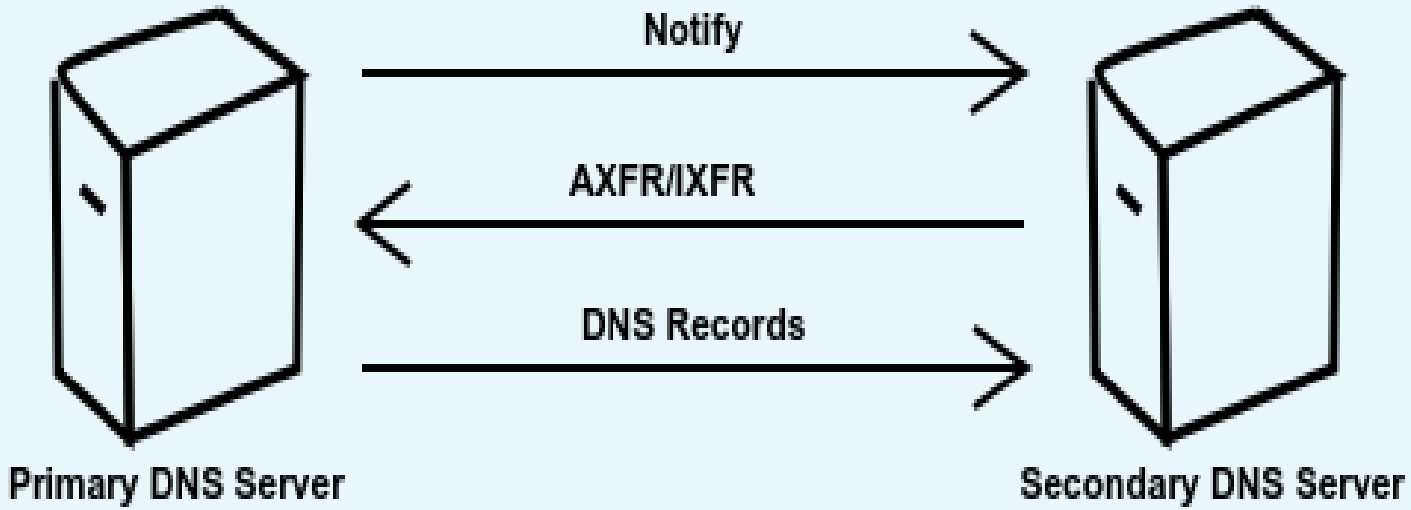
- The database is a noneditable copy of a primary zone
- Contains only the information necessary to identify the authoritative DNS servers for a zone
- Contain only three record types:
  - name server (NS)
  - start of authority (SOA)
  - glue host (A).

DNS

Infrastructure components: zone transfers and replication

- How to keep primary and secondary DNS service in synchronized?
- Secondary DNS servers receive their zone databases through zone transfers
- Configure a secondary server: specify the primary server that is authoritative for the zone and will send the zone transfer.
- The primary server must also permit the secondary server to request the zone transfer.
- Zone transfers occur in one of two ways:
  - full zone transfers (AXFR)
  - and incremental zone transfers (IXFR)

- The DNS system provides the Notify feature.
  - A primary DNS provider can notify the secondary providers that the records have changed.
  - After receiving the Notify message, secondary servers can use AXFR or IXFR query type to fetch the zone records.



Message flow between DNS Servers

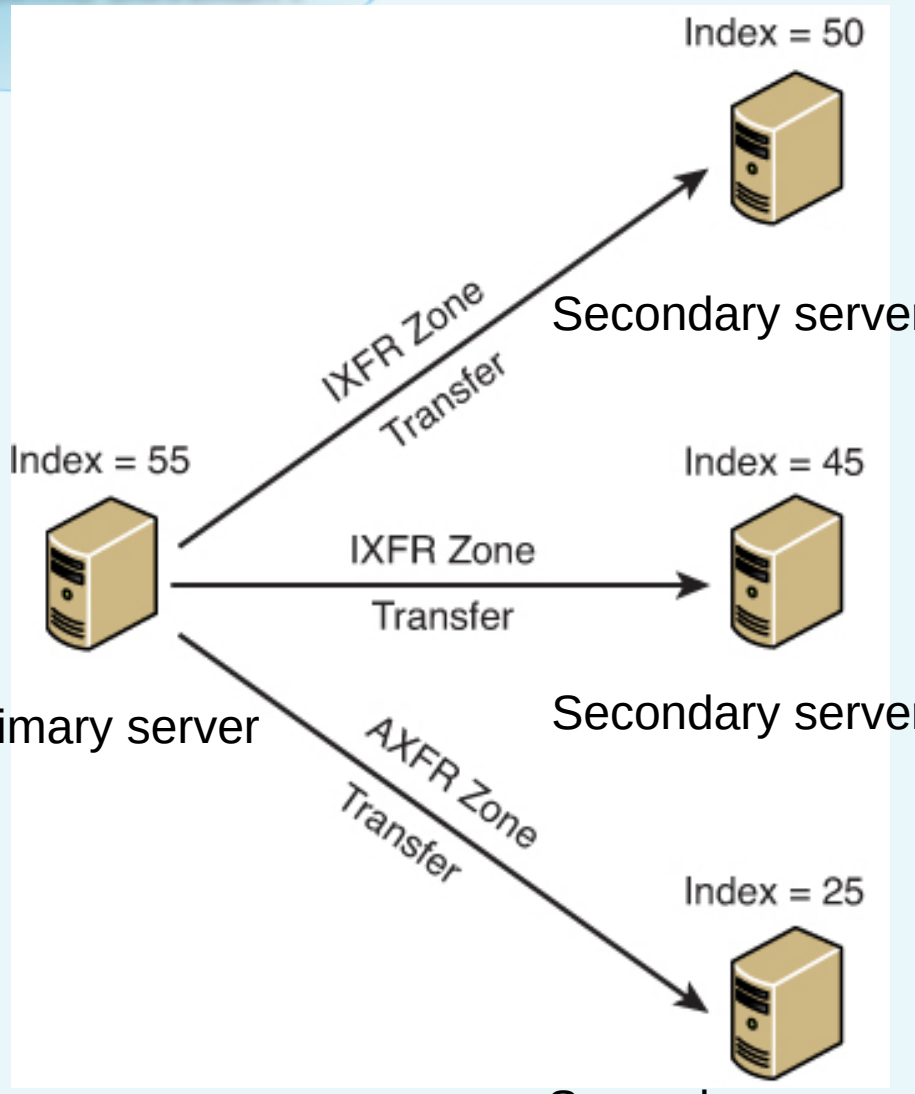
DNS

Infrastructure components: zone transfers and replication

- When configured for the first time, a new secondary server receives a full zone transfer from the primary DNS server
- After the secondary receives its first full zone transfer, subsequent zone transfers are incremental.
  - Based on the difference of the zone version number between two servers, and the primary sends only the changes that have been made in the interim
- The secondary server typically initiates zone transfers when:
  - The refresh interval time for the zone expires
  - The secondary or stub server boots.
  - The primary notifies the secondary whenever any changes to the zone database occur

DNS

Infrastructure components: zone transfers and replication



A zone transfer for all changes from index 50 to 55 is initiated from the Primary to Secondary

A zone transfer for all changes from index 45 to 55 is initiated from the Primary to Secondary

Because the difference between index number is great, a full AXFR zone transfer is initiated from the Primary to Secondary

DNS

Active Directory Integrated zones

- Not a zone type, but an option can be selected when create some types of DNS zone
- A checkbox that states **Store the zone in Active Directory**
- The new zone stored inside Active Directory
- Capable of being replicated automatically to all DC servers in your domain

DNS

Forward Lookup Zones and Reverse Lookup Zones

- Forward Lookup Zones:
  - Traditional DNS zones
  - Take an incoming DNS request and turn that DNS name request into an IP address
- Reverse Lookup Zones
  - opposite of forward
  - Mapping IP addresses backward into names

DNS

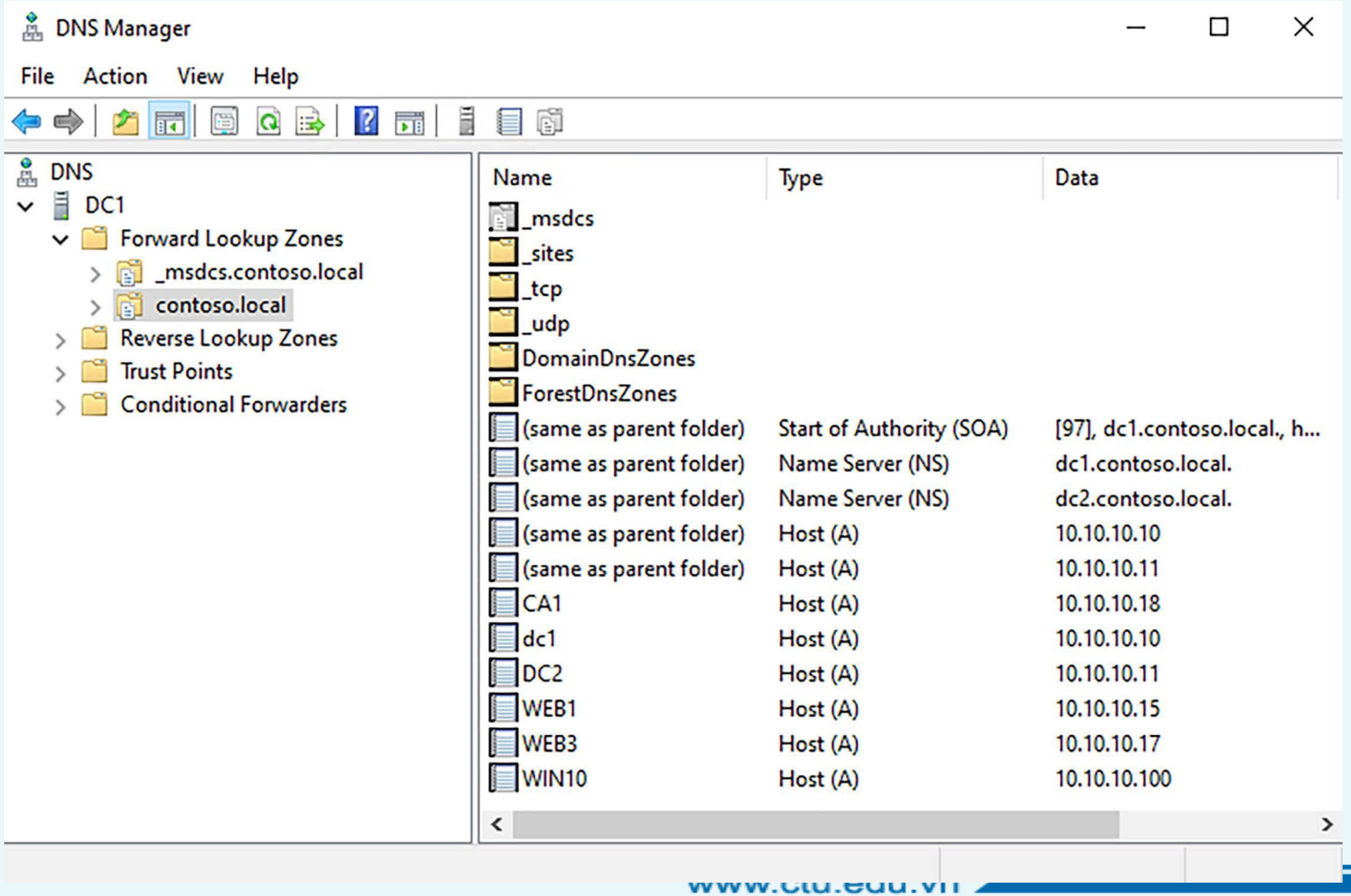
Types of DNS records

- DNS database zone files consist of a number of resource records.
- DNS records used to resolve names to their corresponding IP addresses
- Resource records in forward lookup zones include: A, MX, SRV, NS, SOA, and CNAME
- Resource records in reverse lookup zones include: PTR

DNS

Types of DNS records

DNS Manager console



DNS

Types of DNS records: Host record (A or AAAA)

- Used to associate a host's name to its IP addresses
- **A** records are for IPv4 addresses; **AAAA** (pronounced Quad A) records serve for IPv6 addresses
- The most common kind of DNS records
- Format

  host_name optional_TTL IN A IP_Address

- Example:

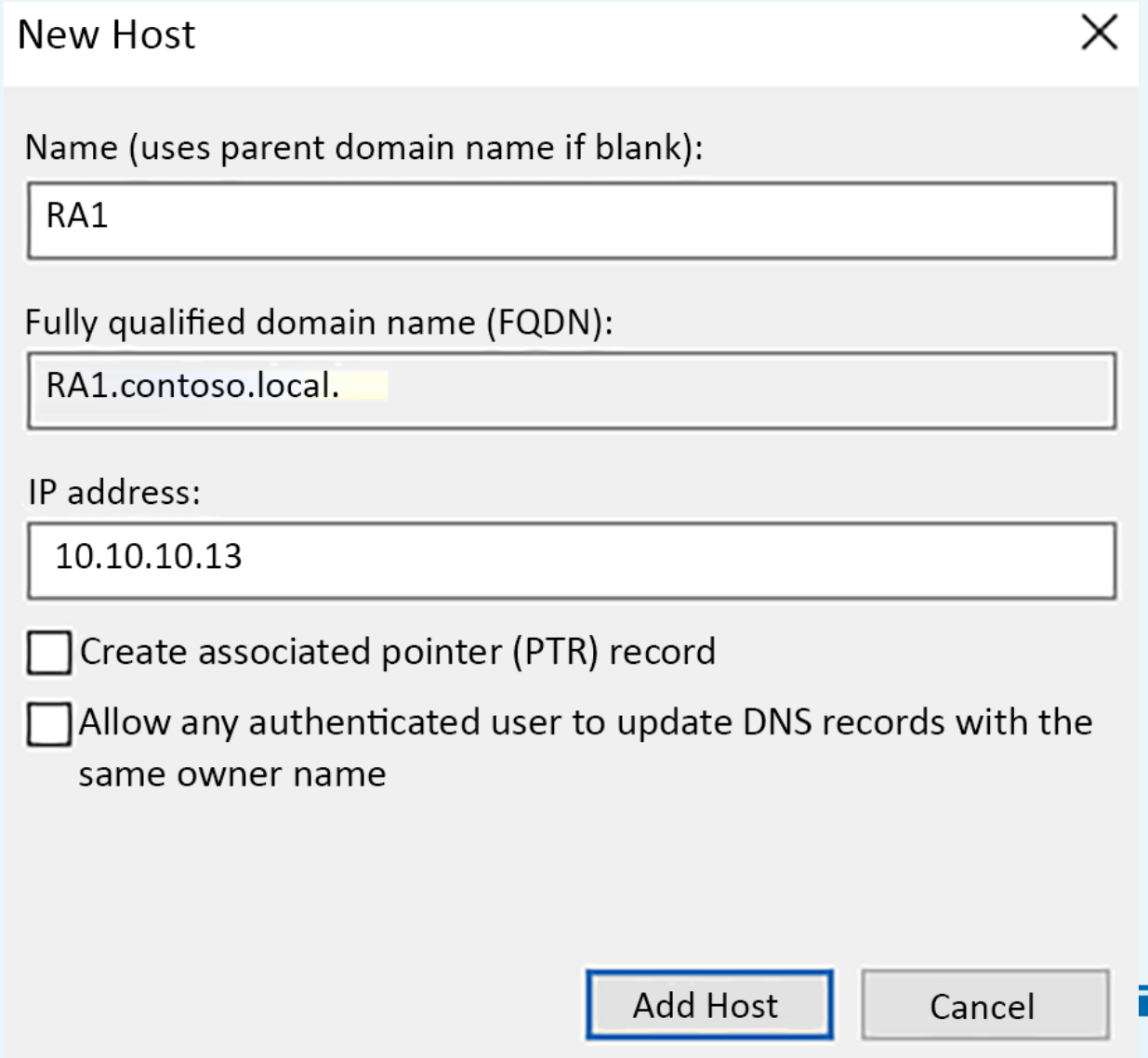
  www IN A 192.168.0.204

CANTHO UNIVERSITY

DNS

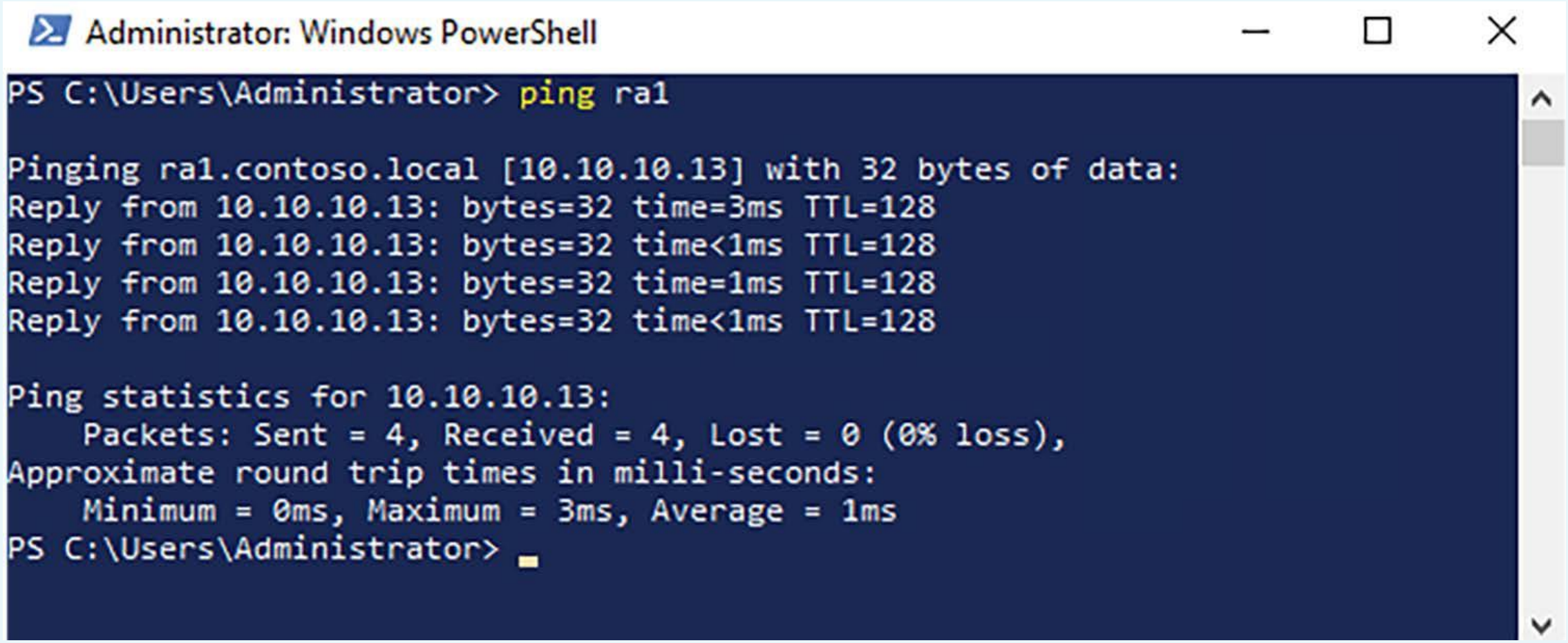
Types of DNS records:Host record (A or AAAA)

1. Open DNS Manager console
2. Right-click on the name of your domain listed under the Forward Lookup Zones folder, and then choose New Host (A or AAAA)



DNS

Types of DNS records: Host record (A or AAAA)



DNS

Types of DNS records: Alias record – CNAME

- Take a name and points it at another name.
- Format: ***alias optional_TTL IN CNAME hostname***
- It still needs to resolve the final name to an IP address to get the traffic where it needs to go
- CNAME is useful in many scenarios, including:
  - create some additional administrative flexibility;
  - Need to replace a web server;
  - Need to add another web server;
  - creates a very simple form of load balancing

DNS

Types of DNS records: Mail Exchanger (MX) record

- Used to specify which servers accept mail for this domain
- When resolving Domain name follows the "@" in your e-mail address, the DNS servers look up an MX record
- Format:

domain IN MX preference mailserver_host

Example:

example.com.	IN	MX	0	mail.example.com.
example.com.	IN	MX	10	backupmail.example.com.

- The preference value specifies which server should be used if more than one MX record is present (The lower the number, the more preferred the server)

DNS

Types of DNS records: Name Server (NS)

- List the name servers for a domain
- Identify which DNS servers are authoritative for the domain your are calling for
- Format: Name Class Type Name server

Field	Meaning
Name	The domain that will be serviced by this name server
Class	Internet (IN)
Record Type	Name server (NS)
Name Server	The FQDN of the server responsible for the domain

DNS

Record Types: Service Record (SRV)

- Windows client query DNS servers for the location of a domain controller
- Service (SRV) records tie together the location of a service (like a domain controller)
- Format: *domain TTL Class Record-Type Priority weight port-number target*

Example:

ldap.tcp.example.com. 86400 IN SRV 10 100 389 hsv.example.com

ldap.tcp.example.com. 86400 IN SRV 20 100 389 msy.example.com

- Priority: Specifies a preference, SRV record with the lowest priority is used first (10).
- Weight: Service records with equal priority are chosen according to their weight (100)
- Port number: The port where the server is listening for this service (389).
- Target: The FQDN of the host computer

DNS

Record Types: Pointer Record (PTR)

- Mapping an IP address to a hostname through the use of the in-addr.arpa zone
- Format:

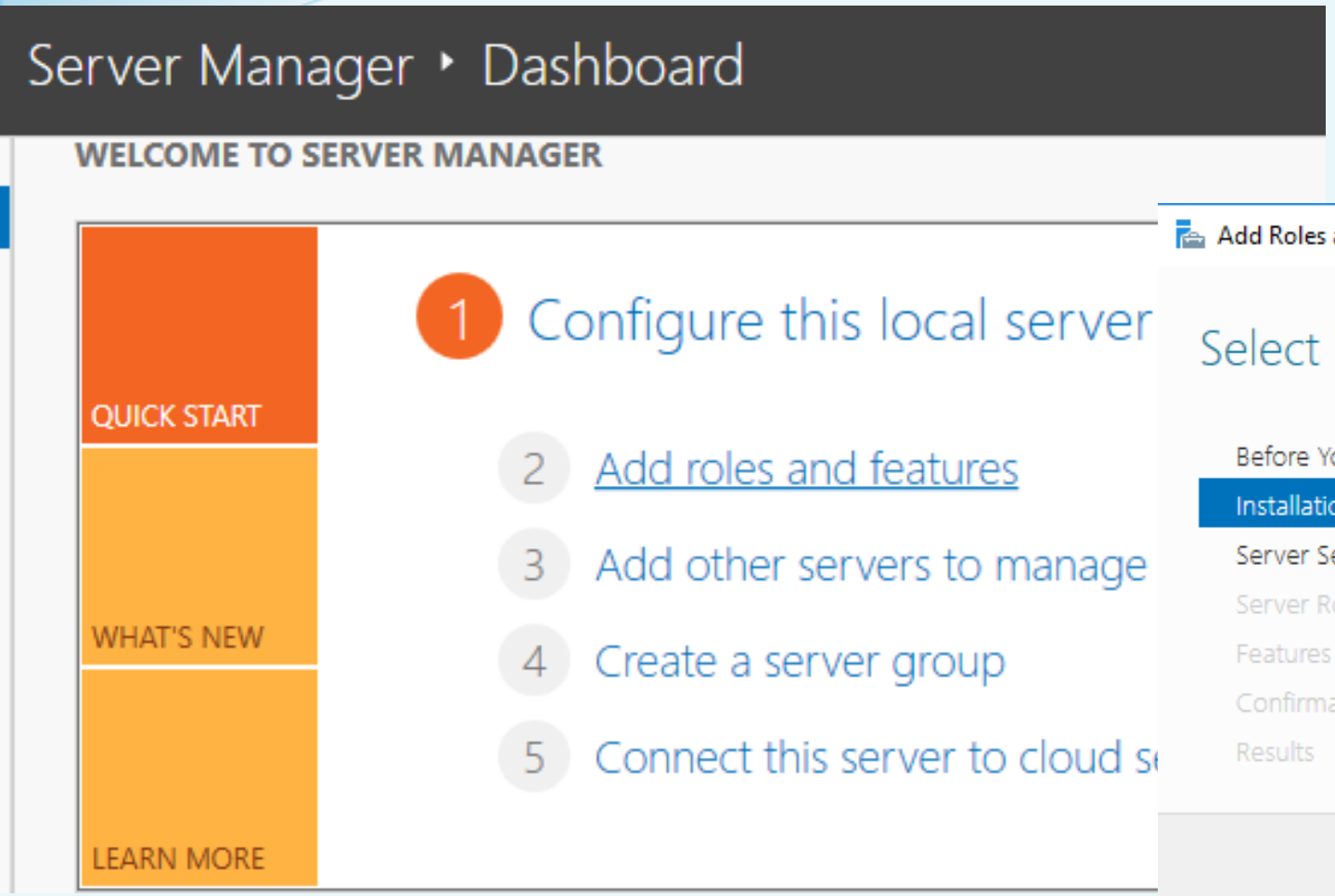
reversed_address.in-addr.arpa. optional_TTL IN PTR targeted_domain_name

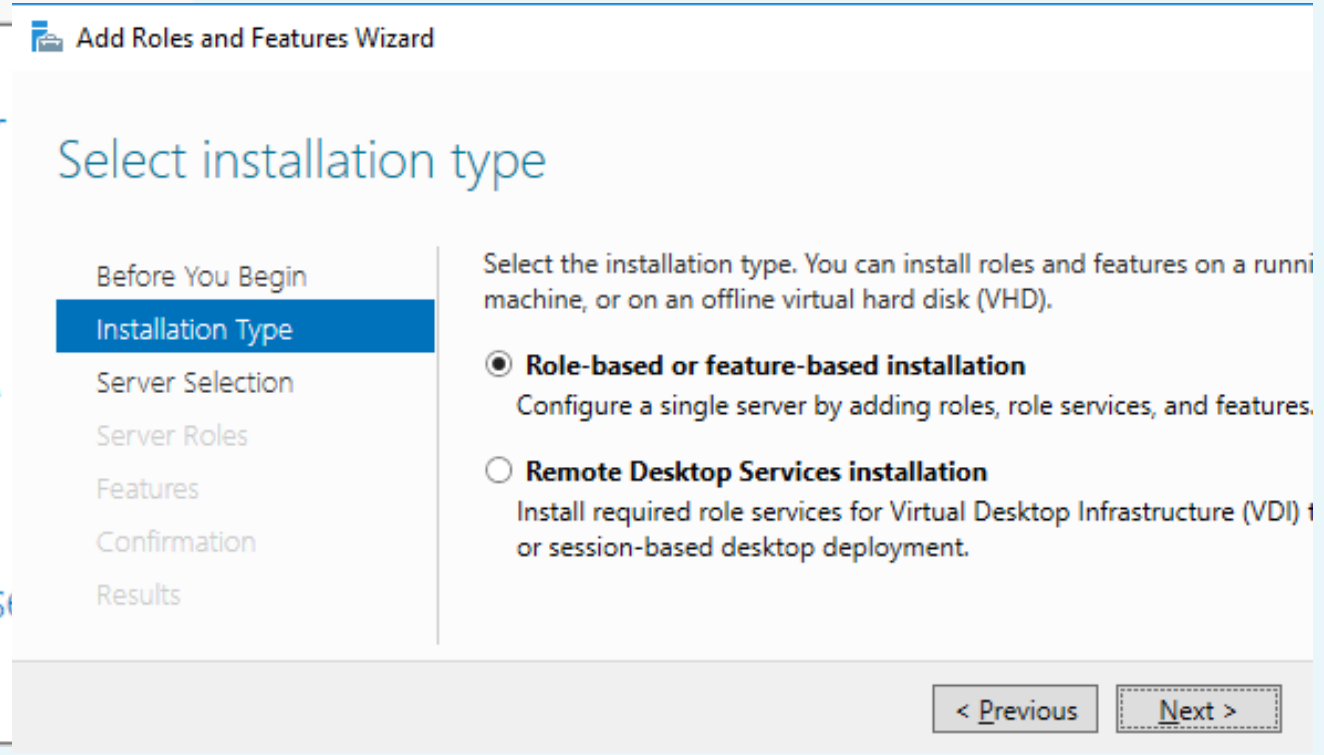
- *Example:*

10.1.168.192.in-addr.arpa. IN PTR www.example.com.

Configuring DNS

Installing DNS





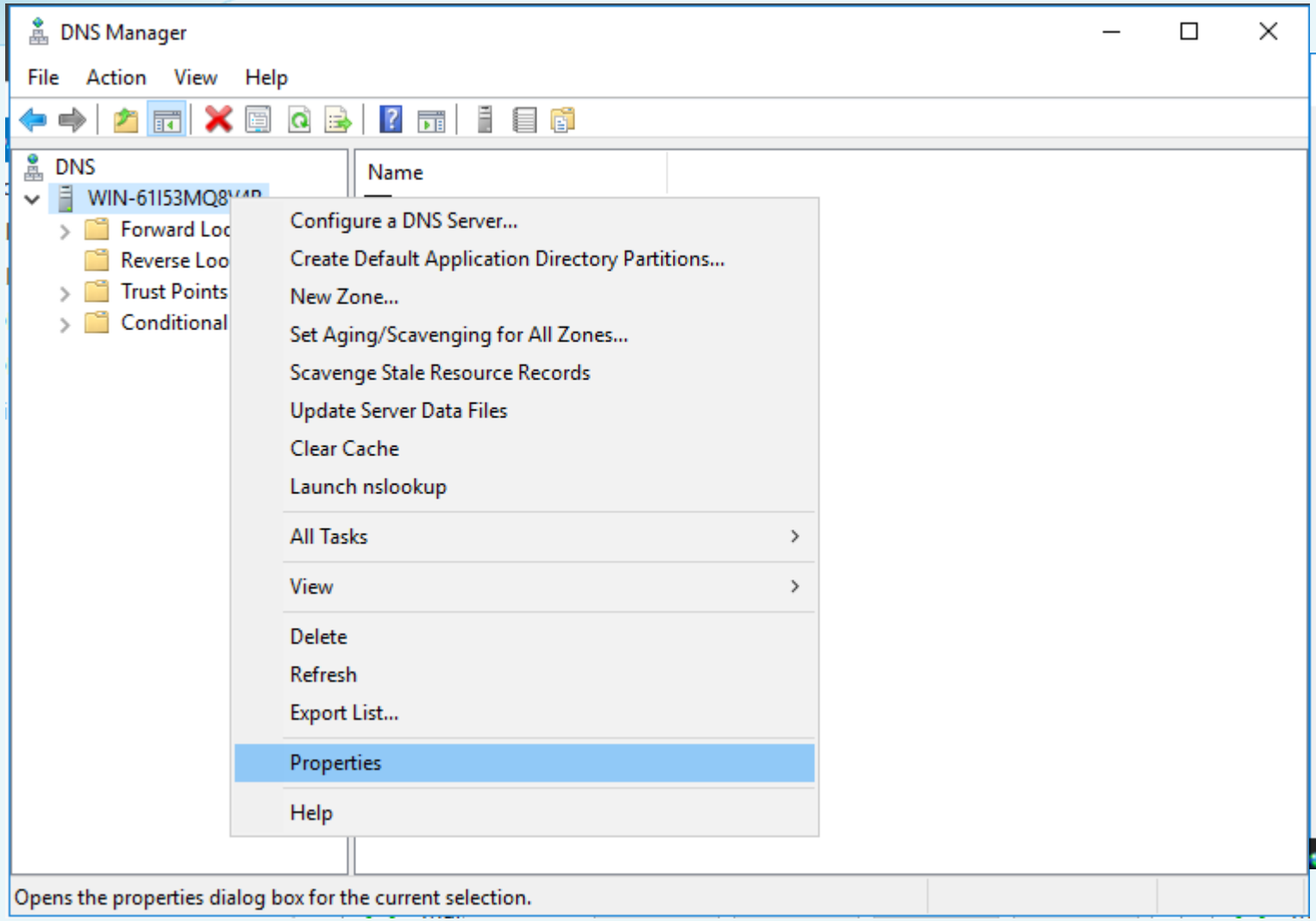
DNS

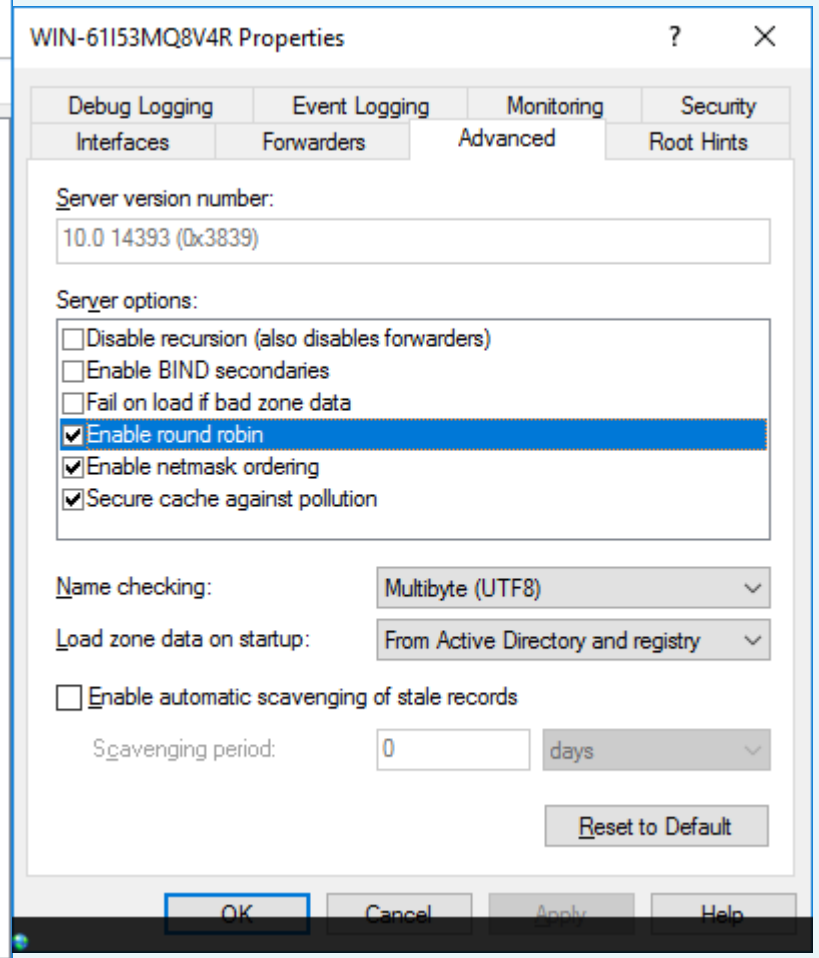
Configuration: Load Balancing with Round Robin

- Implementation of DNS supports load balancing
- Distribute the network load among multiple network hosts if they are available
- Round-robin load balancing: creating multiple resource records with the same hostname but different IP addresses for multiple computers
- If round robin is enabled:
  - When a client requests name resolution, the first address entered in the database is returned to the resolver and is then sent to the end of the list.
  - The next time a client attempts to resolve the name, the DNS server returns the second name in the database (which is now the first name) and then sends it to the end of the list, and so on.
- Round robin is enabled by default.

DNS

Configuration: Load Balancing with Round Robin



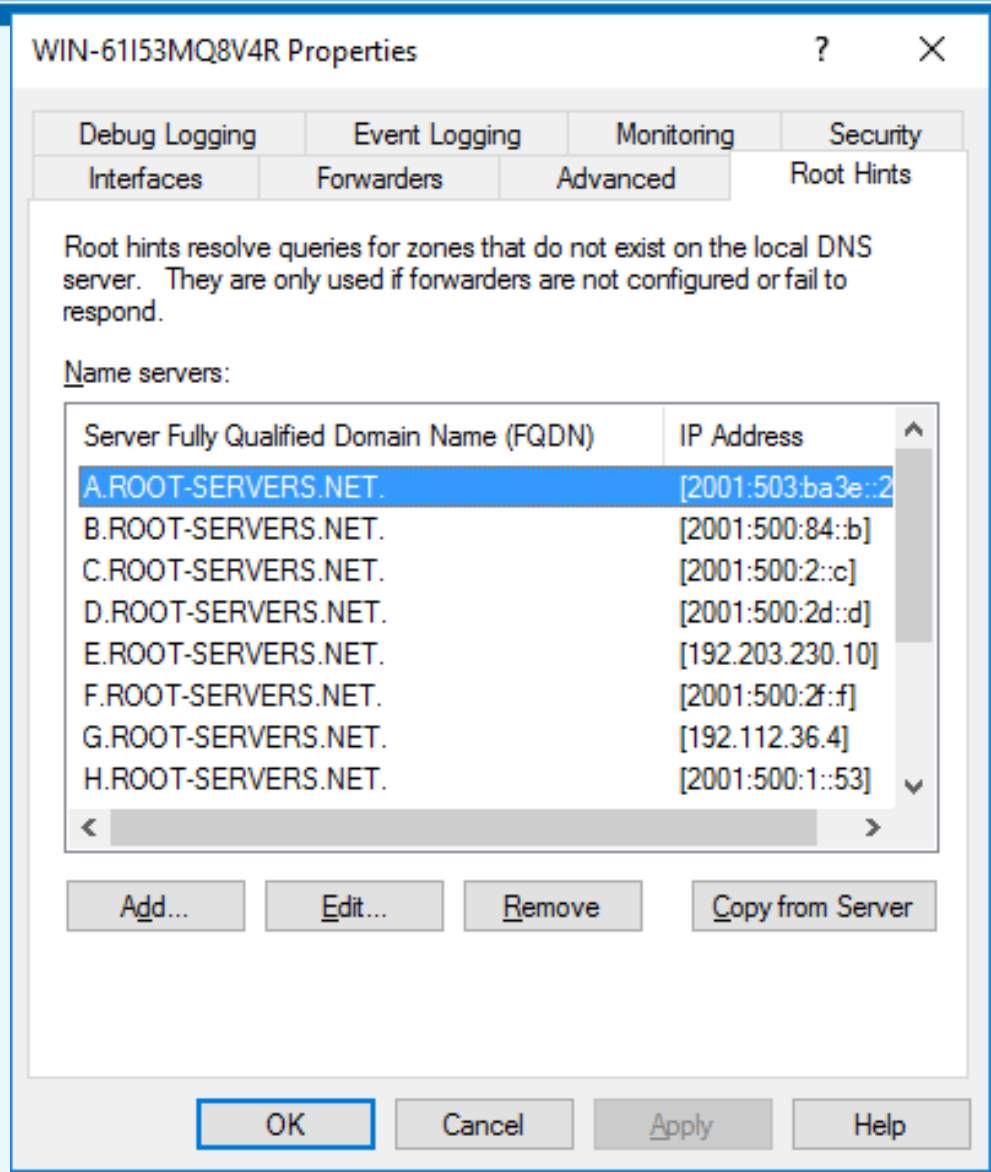


CANTHO UNIVERSITY

DNS

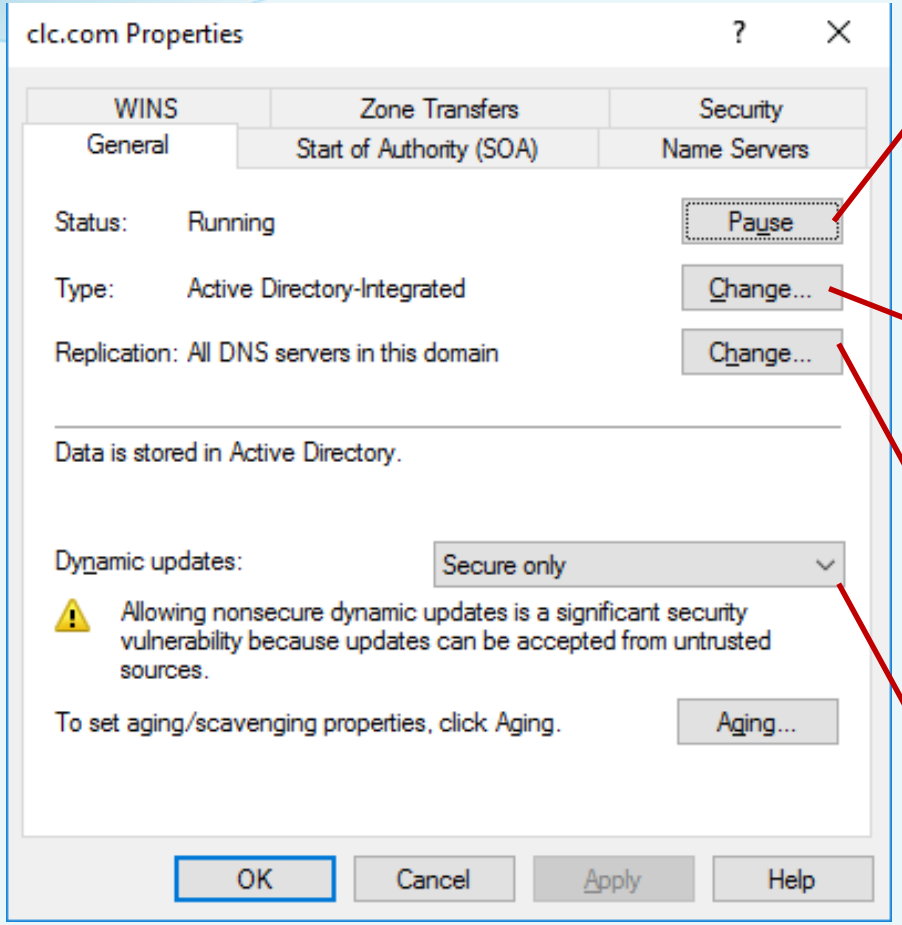
Configuration: Caching-Only Server

- Only perform queries, cache the answers, and return the results
- Not authoritative for any domains
- Do not have any zone files, and don't participate in zone transfers
- Easy to configure: After installing the DNS service, simply make sure the root hints are configured properly



DNS

Configuration: Setting Zone Properties



See and control whether this zone can be used to answer queries

Allow to select the zone type.

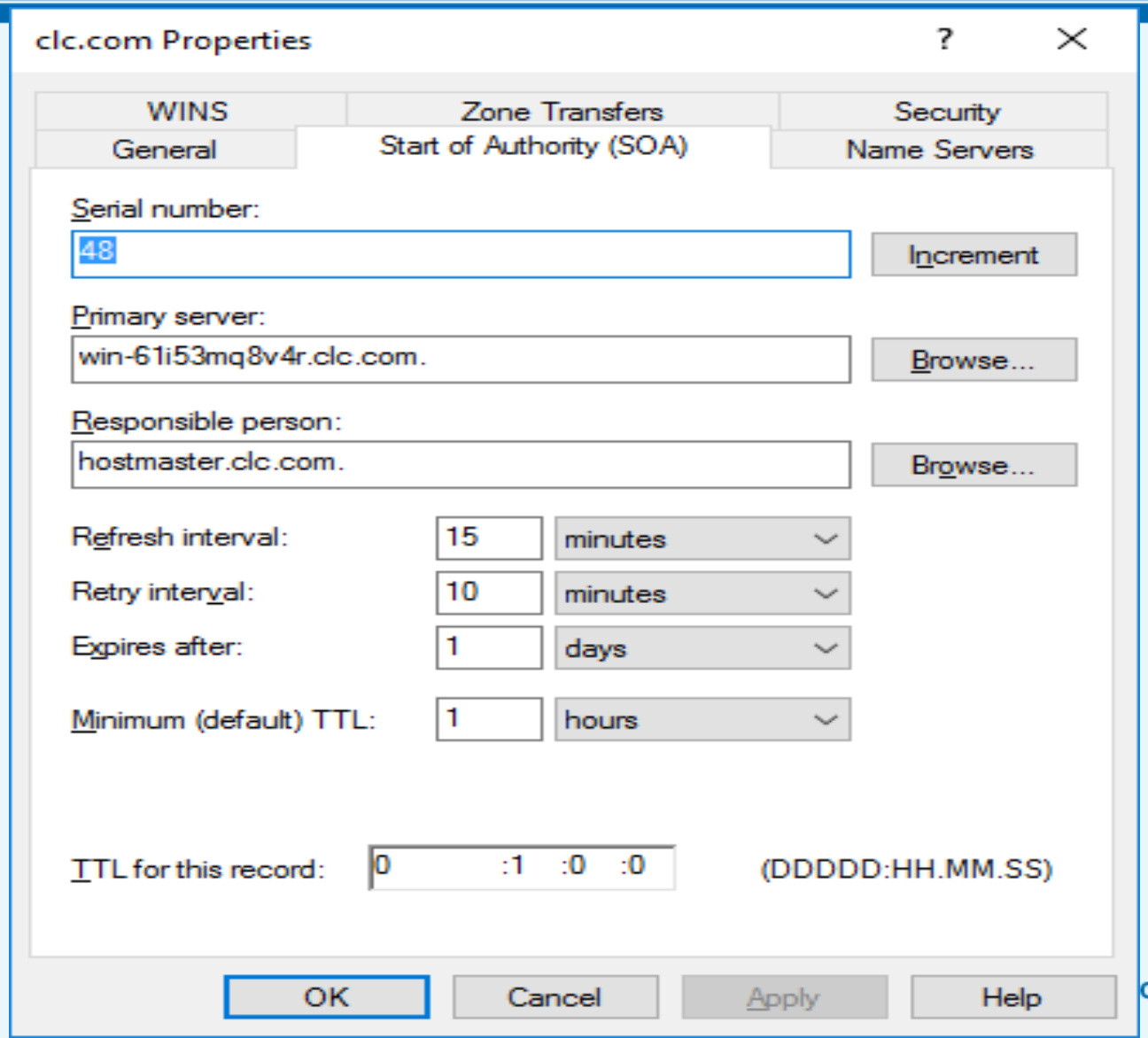
Allow to change the replication scope if the zone is stored in Active Directory.

Specify whether to support Dynamic DNS updates from compatible DHCP servers.

DNS

Configuration: Setting Zone Properties

Start Of Authority (SOA) record

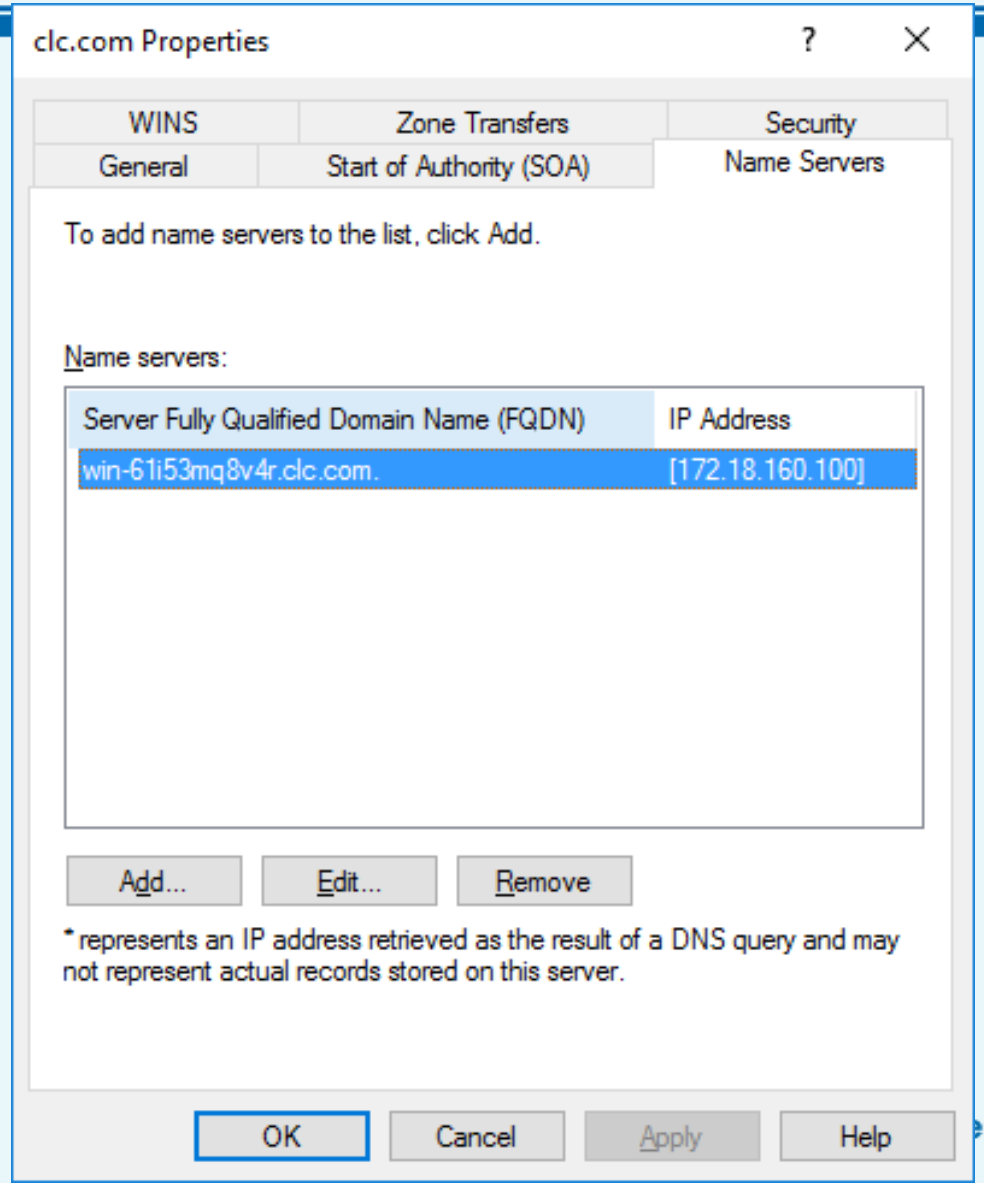


CANTHO UNIVERSITY

DNS

Configuration: Setting Zone Properties

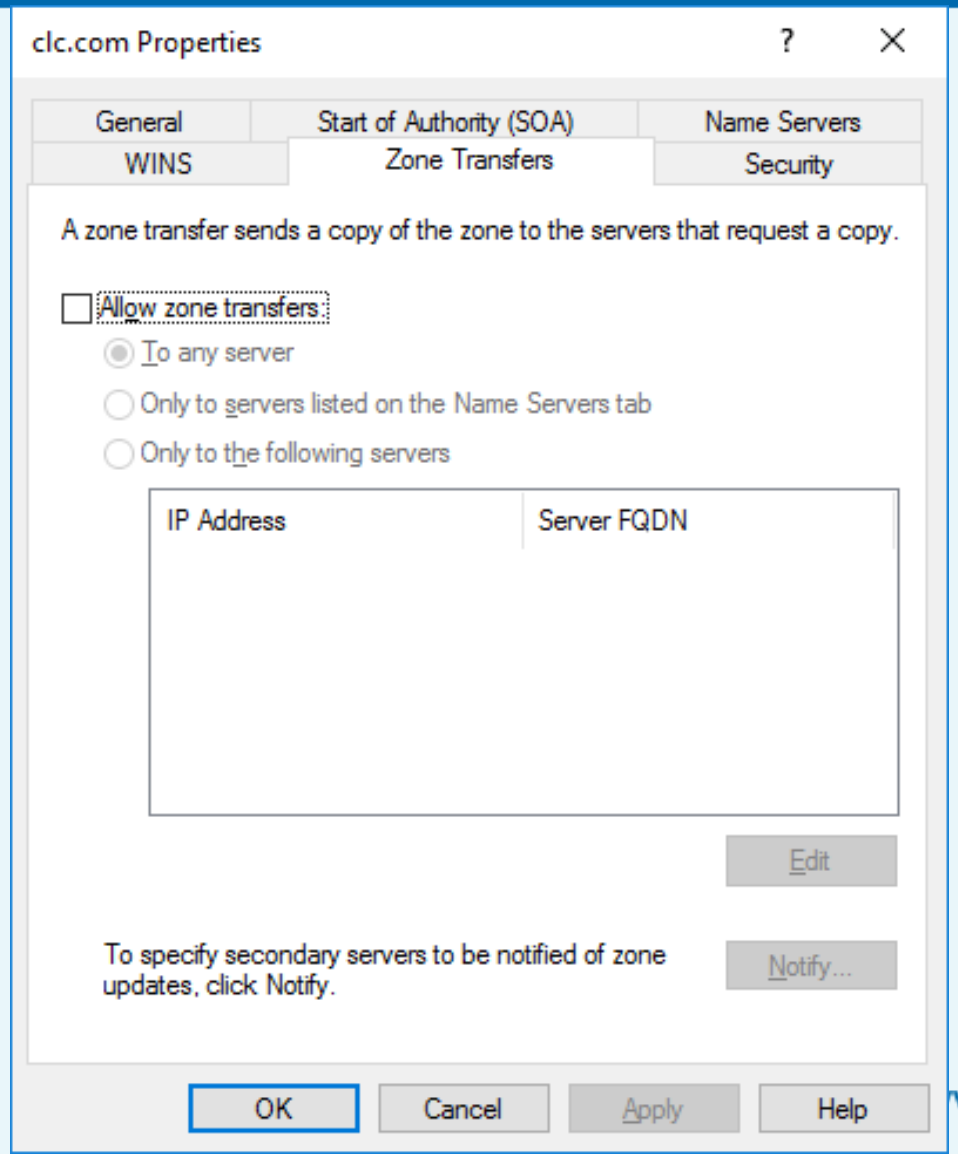
Indicate which name servers are authoritative for the zone.



DNS

Configuration: Setting Zone Properties

Specify whether the servers allow zone transfers and, if so, to whom.



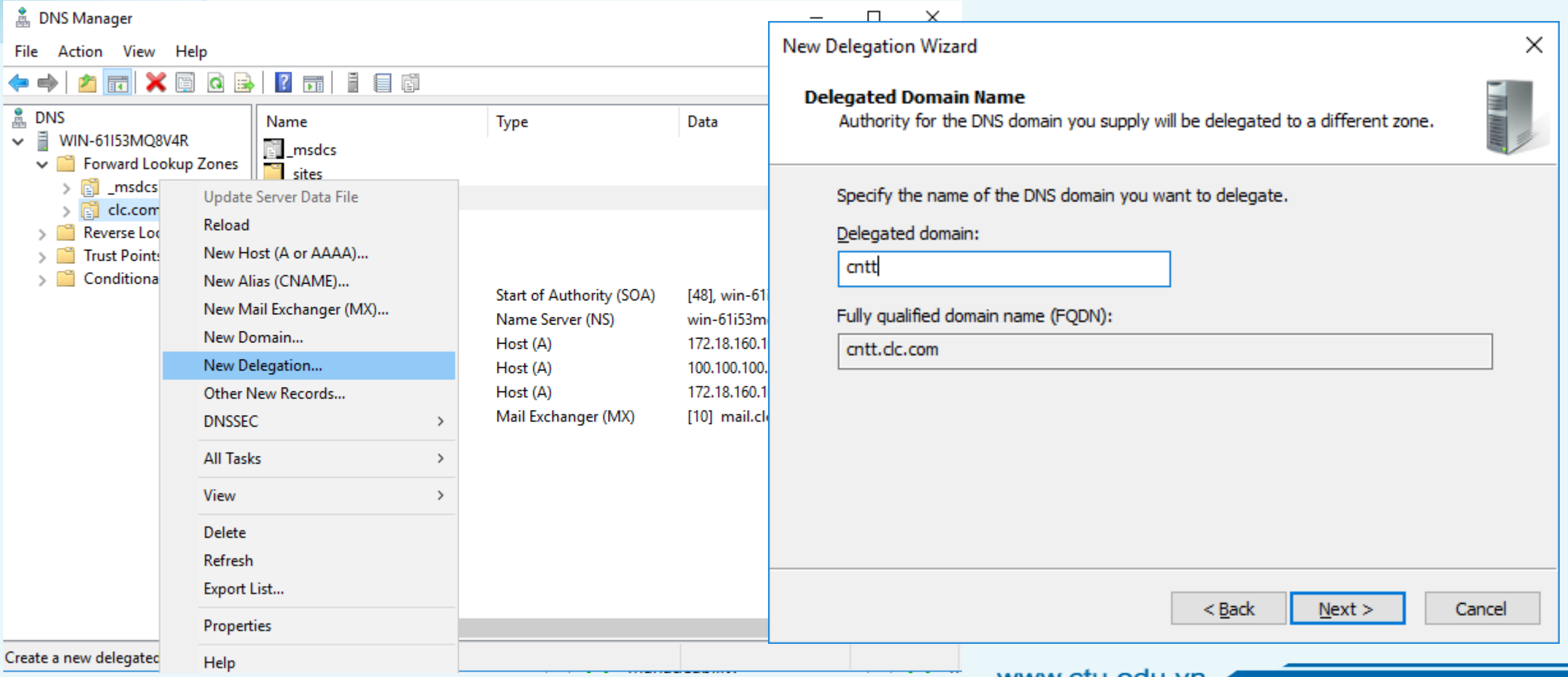
DNS

Configuration: Delegating Zones for DNS

- DNS provides the ability to divide the namespace into one or more Zones
- A need to delegate management of part of the DNS namespace to another location or department within the organization
- Each newly delegated zone requires a primary DNS server just as a regular DNS zone does

DNS

Configuration: Delegating Zones for DNS



DNS

Configuration: Delegating Zones for DNS

New Delegation Wizard

Name Servers

You can select one or more name servers to host the delegated zone.

Specify the names and IP addresses of the DNS servers you want to have host the delegated zone.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address

Add... Edit... Remove

< Back Next > Cancel

Edit Name Server Record

Enter the name of a DNS server that is authoritative for this zone.

Server fully qualified domain name (FQDN):

ns.cntt.dc.com. Resolve

IP Addresses of this NS record:

IP Address	Validated
<Click here to add an IP Address>	
172.18.161.100	Validating...

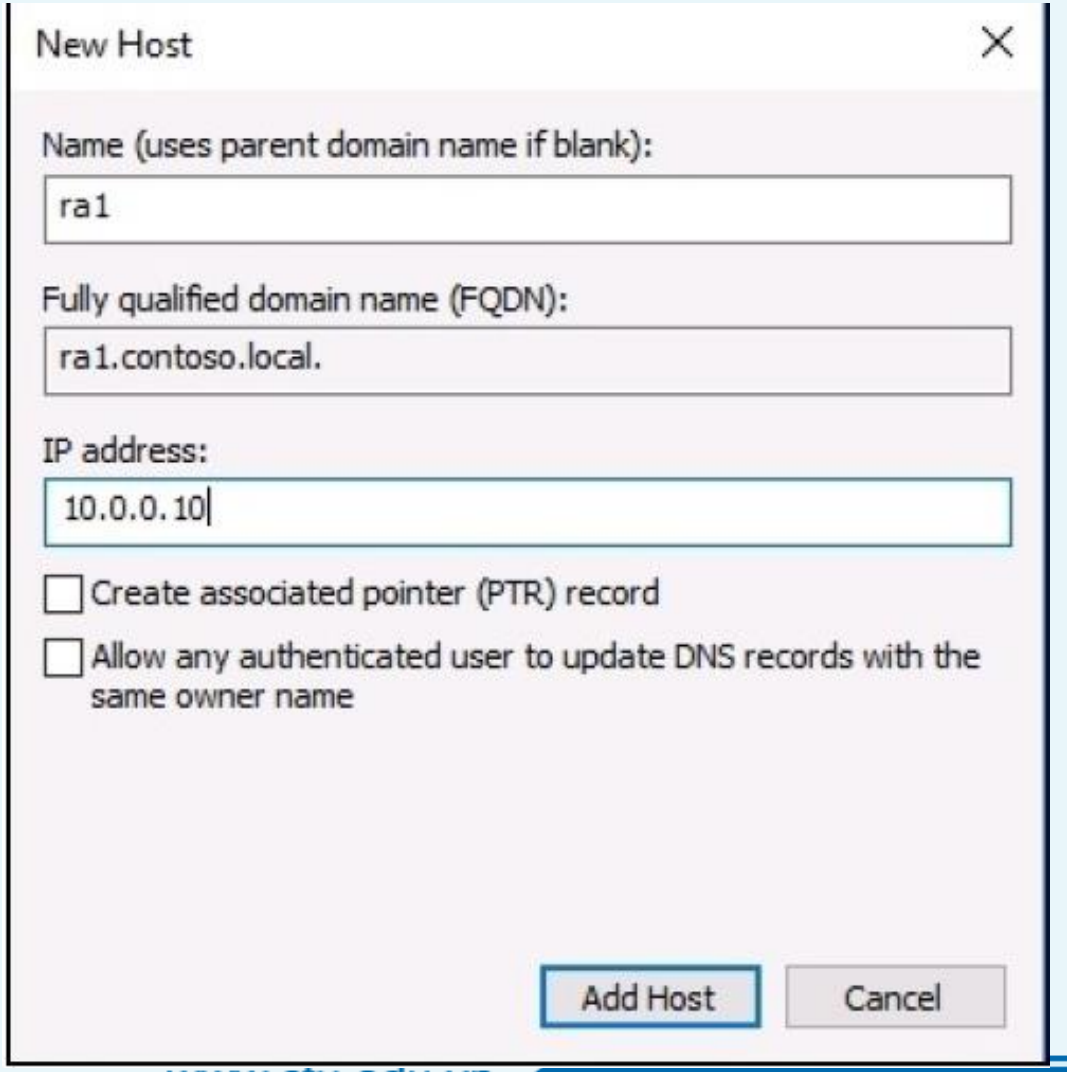
Delete Up Down

OK Cancel

DNS

Creating Records: Host record

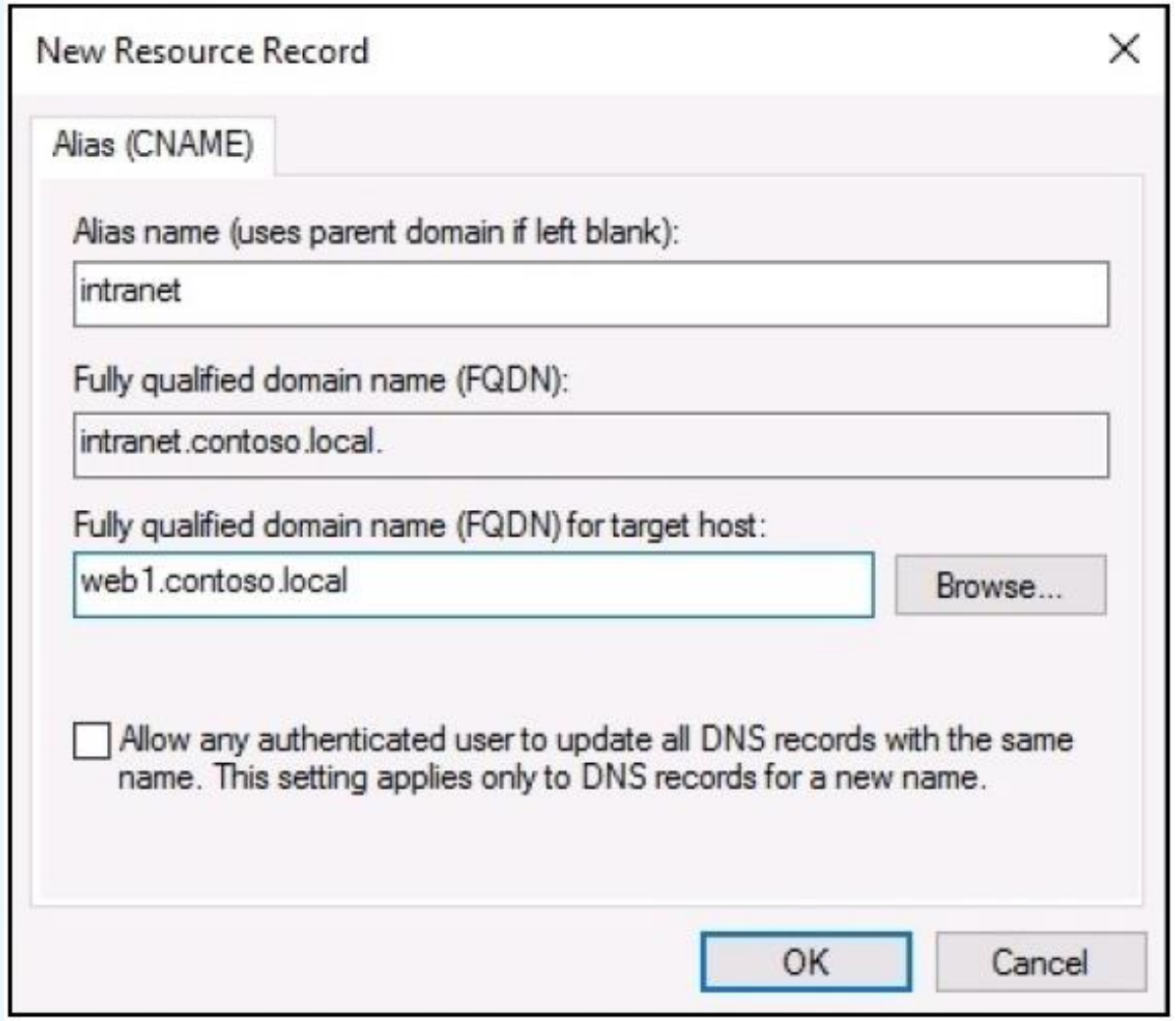
1. Open DNS Manager
2. Right-click on the name of domain listed under the Forward Lookup Zones folder, and then choose New Host (A or AAAA)
3. Enter the name of theserver, and the IP address configured on its network interface.



DNS

Creating Records: Alias record – CNAME

1. Open DNS Manager
2. Right-click on the name of domain listed under the **Forward Lookup Zones** folder, and then choose **New Alias (CNAME)**
3. Enter Alias for host name

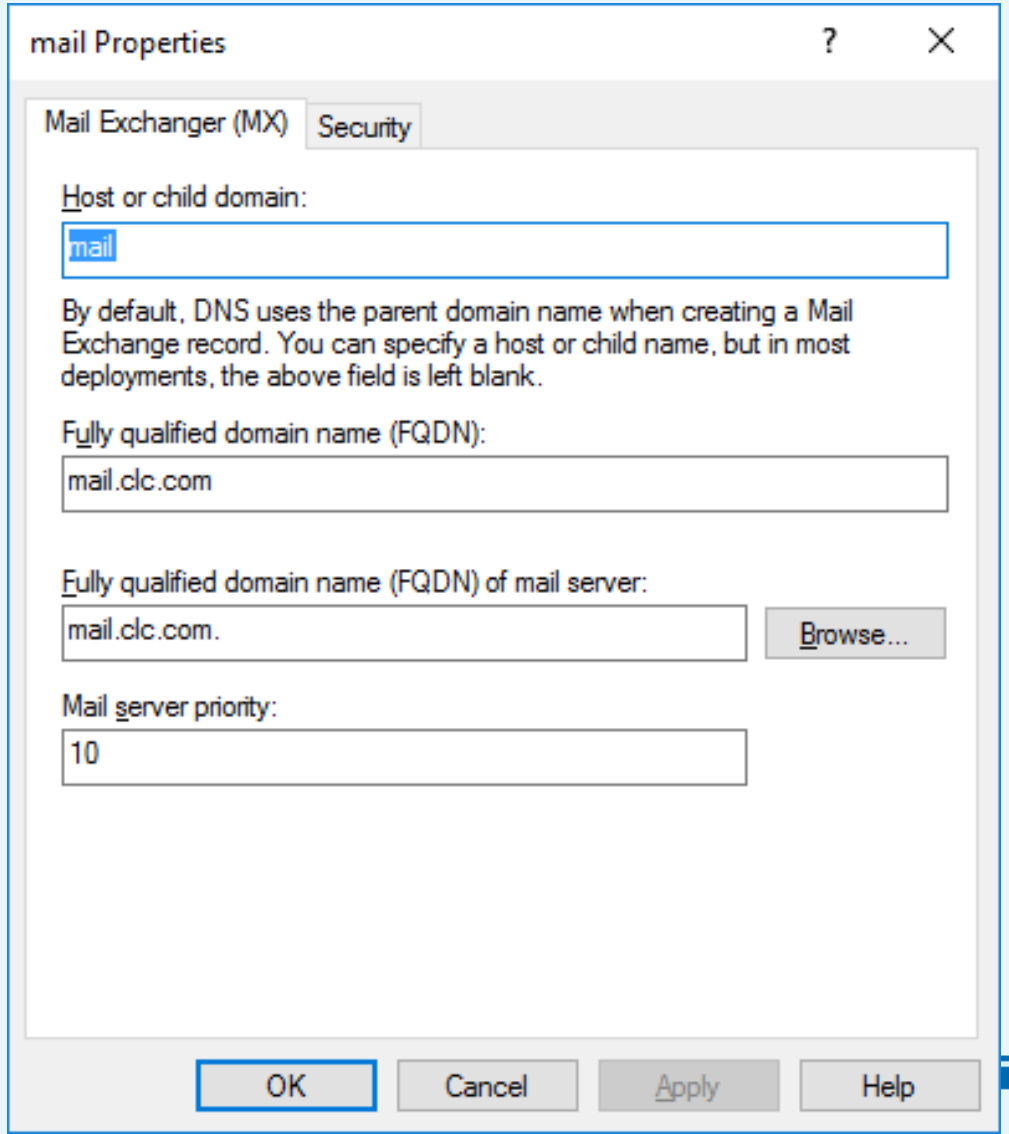


CANTHO UNIVERSITY

DNS

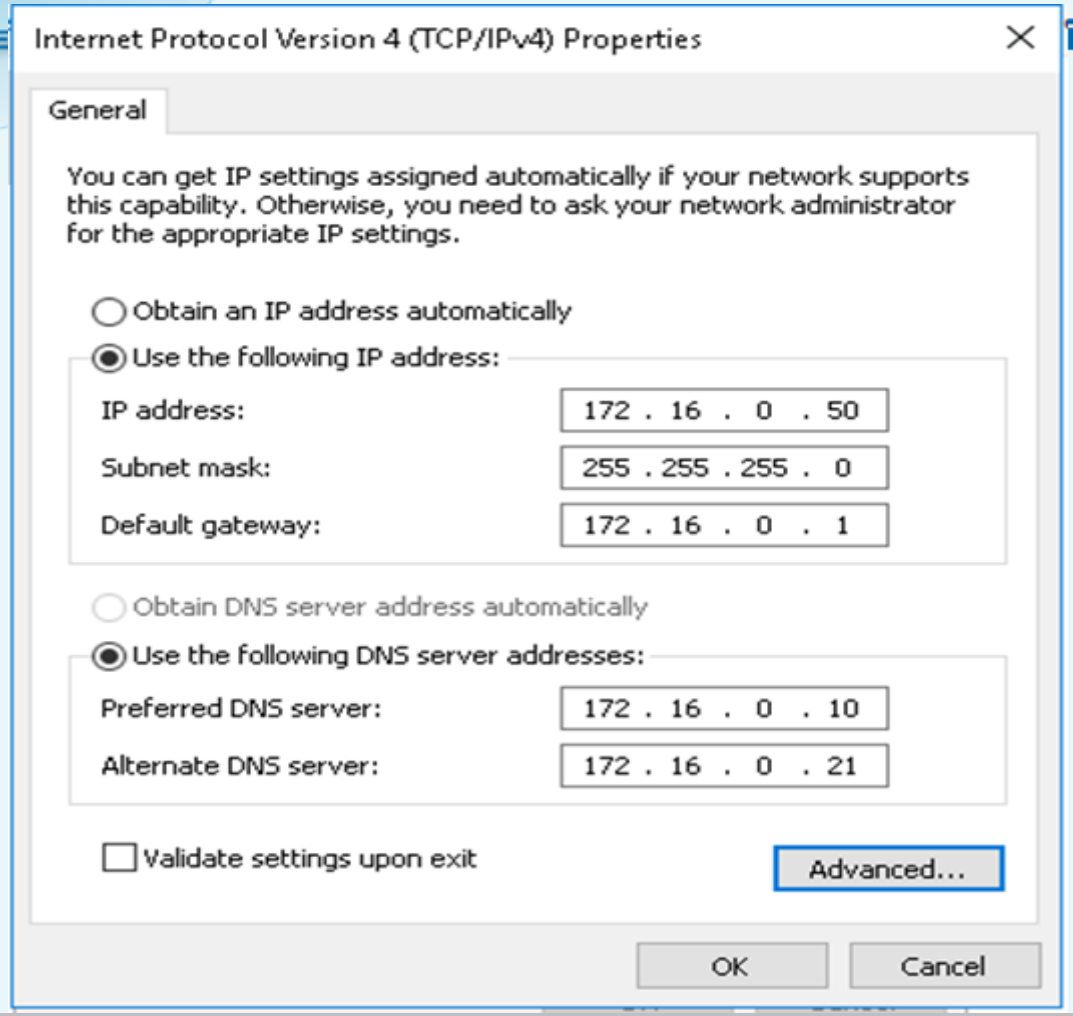
Creating Records: Mail Exchange (MX) record

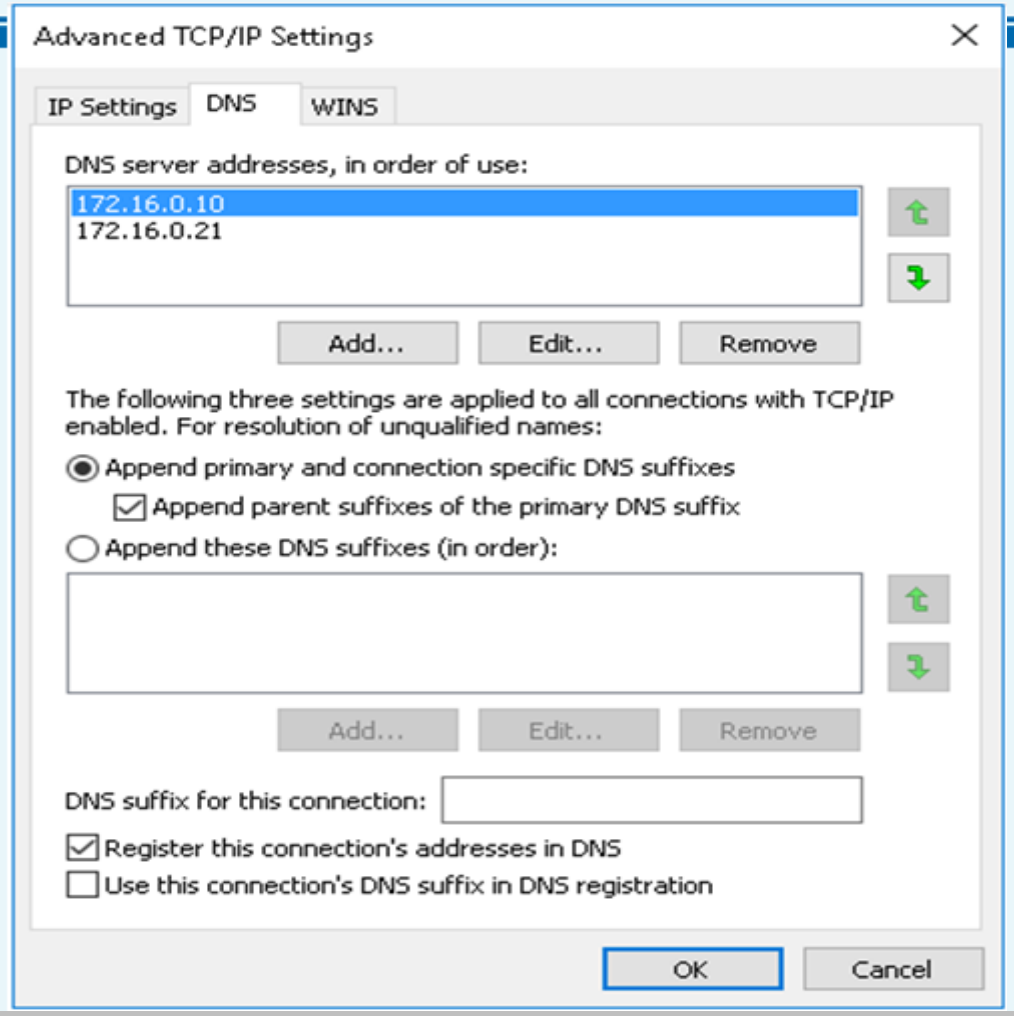
1. Open DNS Manager
2. Right-click on the name of domain listed under the **Forward Lookup Zones** folder, and then choose **New Mail Exchange (MX)…**
3. Enter Host or child domain and FQDN of mail server



DNS

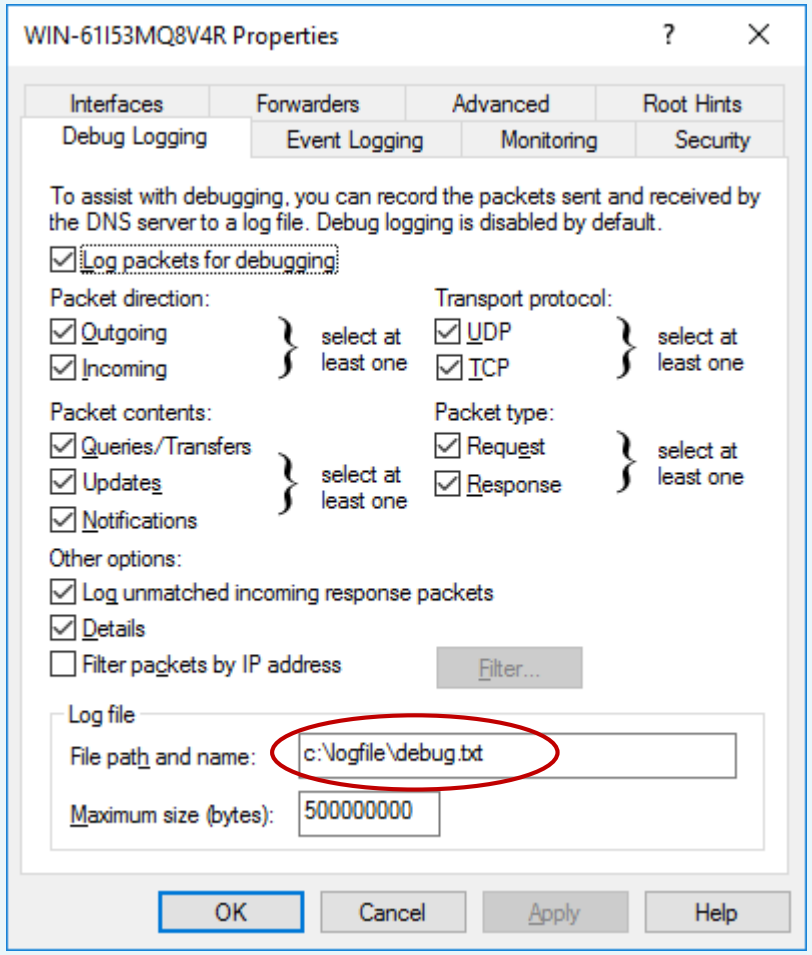
Configuring clients

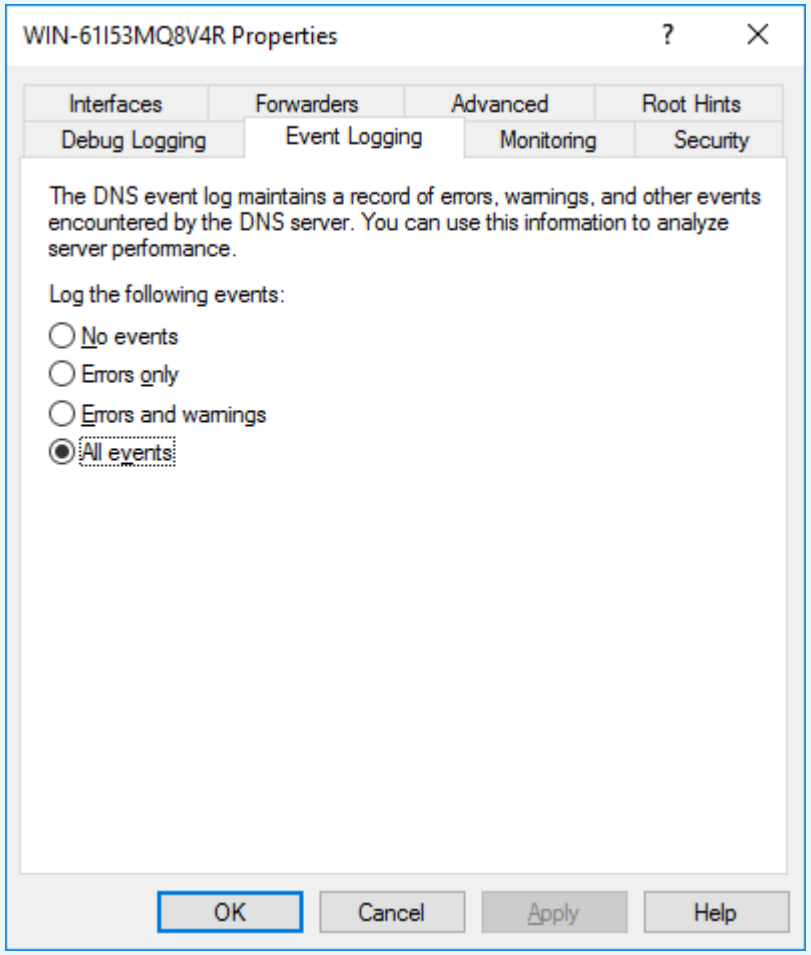


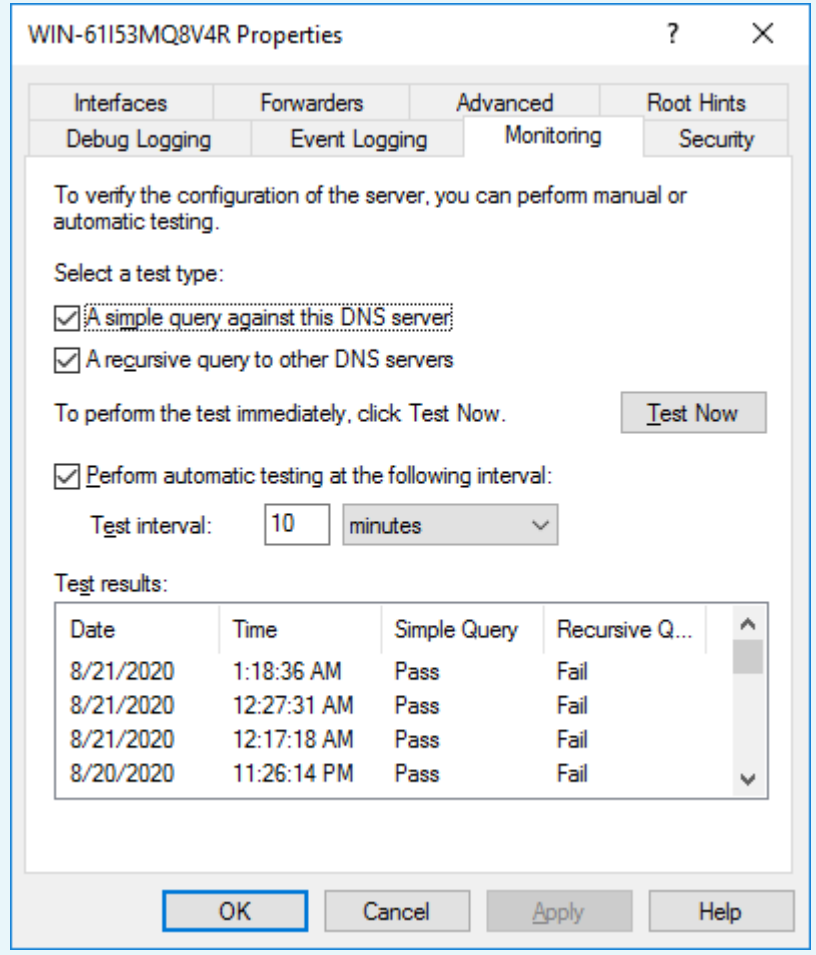


Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses ("172.16.0.10","172.16.0.21")

- To monitor and set logging options







DNS

Monitoring and Troubleshooting: DNS Snap-In

debug - Notepad

File Edit Format View Help

```
DNS Server log file creation at 8/20/2020 11:14:21 PM
Log file wrap at 8/20/2020 11:14:21 PM

Message logging key (for packets - other items use a subset of these fields):
        Field #  Information         Values
        -------  -----------         ------
           1     Date
           2     Time
           3     Thread ID
           4     Context
           5     Internal packet identifier
           6     UDP/TCP indicator
           7     Send/Receive indicator
           8     Remote IP
           9     Xid (hex)
          10     Query/Response      R = Response
                                     blank = Query
          11     Opcode              Q = Standard Query
                                     N = Notify
                                     U = Update
                                     ? = Unknown
          12     [ Flags (hex)
          13     Flags (char codes)  A = Authoritative Answer
                                     T = Truncated Response
                                     D = Recursion Desired
                                     R = Recursion Available
          14     ResponseCode ]
```

- To confirm that DNS server is resolving and replying to client DNS requests.
- When troubleshooting DNS problems, ask yourself the following basic questions:
  - What application is failing? What works? What doesn't work?
  - Is the problem basic IP connectivity, or is it name resolution?
  - Have the things that don't work ever worked on this computer or network? If so, what has changed since they last worked?

- 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

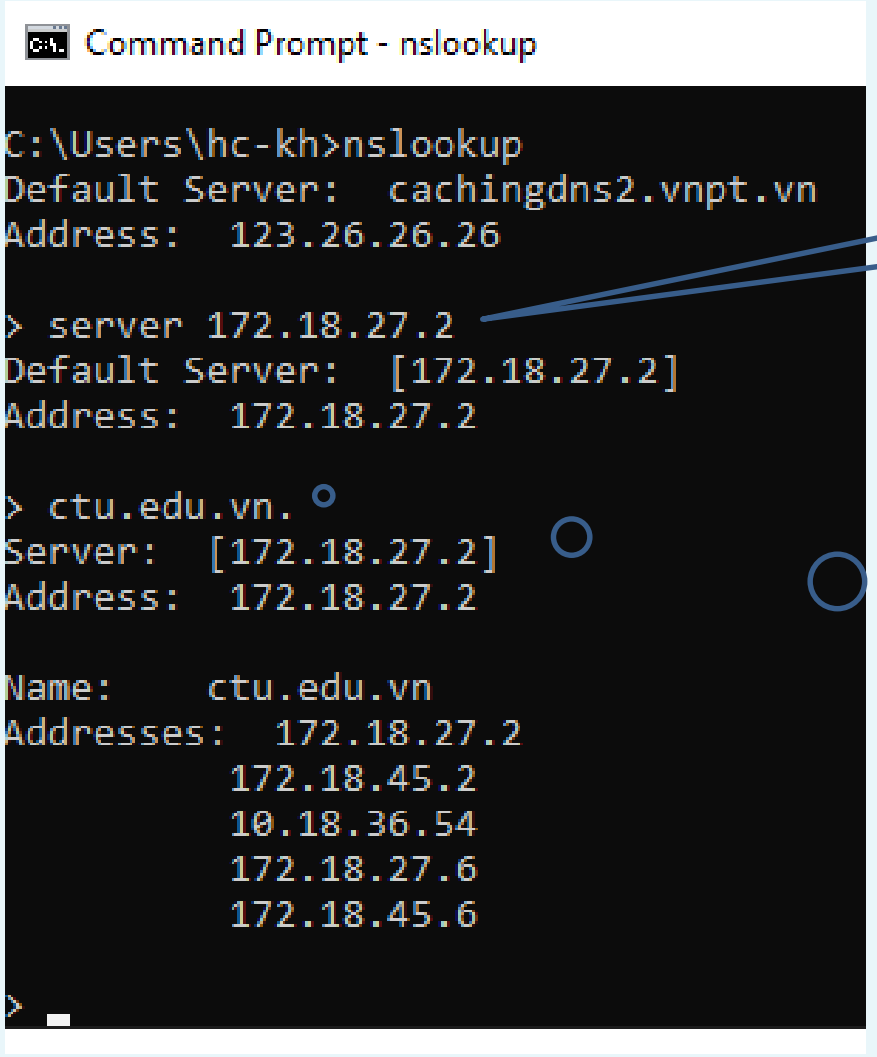
DNS

Troubleshooting DNS: Nslookup

- Used to perform DNS queries and to examine the contents of zone files on local and remote servers
- Offer the ability to perform query testing of DNS servers and to obtain detailed responses at the command prompt.
- Useful for:
  - diagnosing and solving name resolution Problems
  - verifying that resource records are added or updated correctly in a zone,
  - debugging other server-related problems

DNS

Troubleshooting DNS: Nslookup

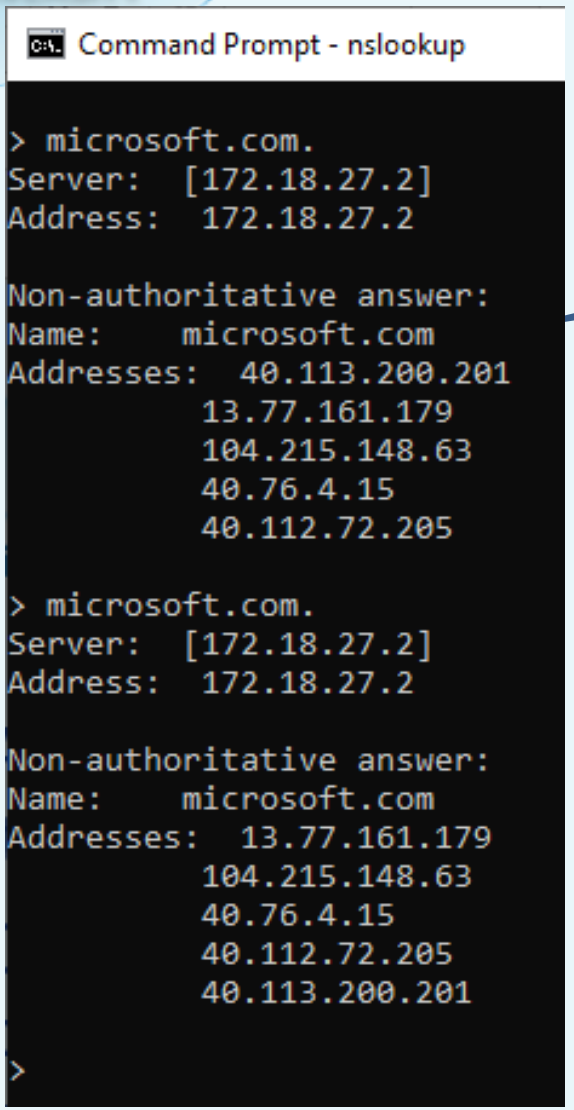


Change the DNS server

Look up a name

DNS

Troubleshooting DNS: Nslookup



Non-authoritative???

Round-robin

DNS

Troubleshooting DNS: Nslookup

Command Prompt - nslookup

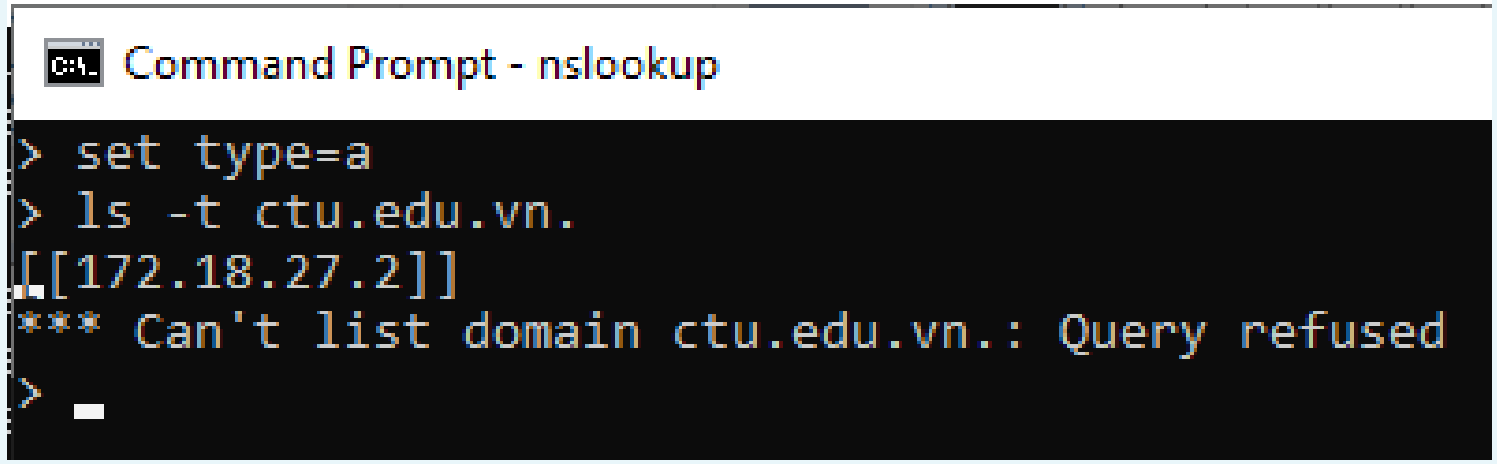
```
> set type=MX
> ctu.edu.vn.
Server:  [172.18.27.2]
Address:  172.18.27.2

ctu.edu.vn      MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
ctu.edu.vn      MX preference = 10, mail exchanger = alt3.aspmx.l.google.com
ctu.edu.vn      MX preference = 10, mail exchanger = alt4.aspmx.l.google.com
ctu.edu.vn      MX preference = 30, mail exchanger = aspmx4.googlemail.com
ctu.edu.vn      MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
ctu.edu.vn      MX preference = 1, mail exchanger = aspmx.l.google.com
ctu.edu.vn      MX preference = 30, mail exchanger = aspmx5.googlemail.com
alt2.aspmx.l.google.com internet address = 74.125.127.26
alt2.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4003:c11::1a
alt3.aspmx.l.google.com internet address = 209.85.234.26
alt3.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4001:c17::1b
alt4.aspmx.l.google.com internet address = 173.194.209.26
alt4.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4024:c02::1a
aspmx4.googlemail.com   internet address = 209.85.234.26
aspmx4.googlemail.com   AAAA IPv6 address = 2607:f8b0:4001:c17::1b
alt1.aspmx.l.google.com internet address = 74.125.28.26
alt1.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:400e:c04::1a
aspmx.l.google.com      internet address = 172.217.194.26
aspmx.l.google.com      AAAA IPv6 address = 2404:6800:4003:c03::1b
aspmx5.googlemail.com   internet address = 173.194.209.26
aspmx5.googlemail.com   AAAA IPv6 address = 2607:f8b0:4024:c02::1a
>
```

Lookup mail servers for a domain

DNS

Troubleshooting DNS: Nslookup

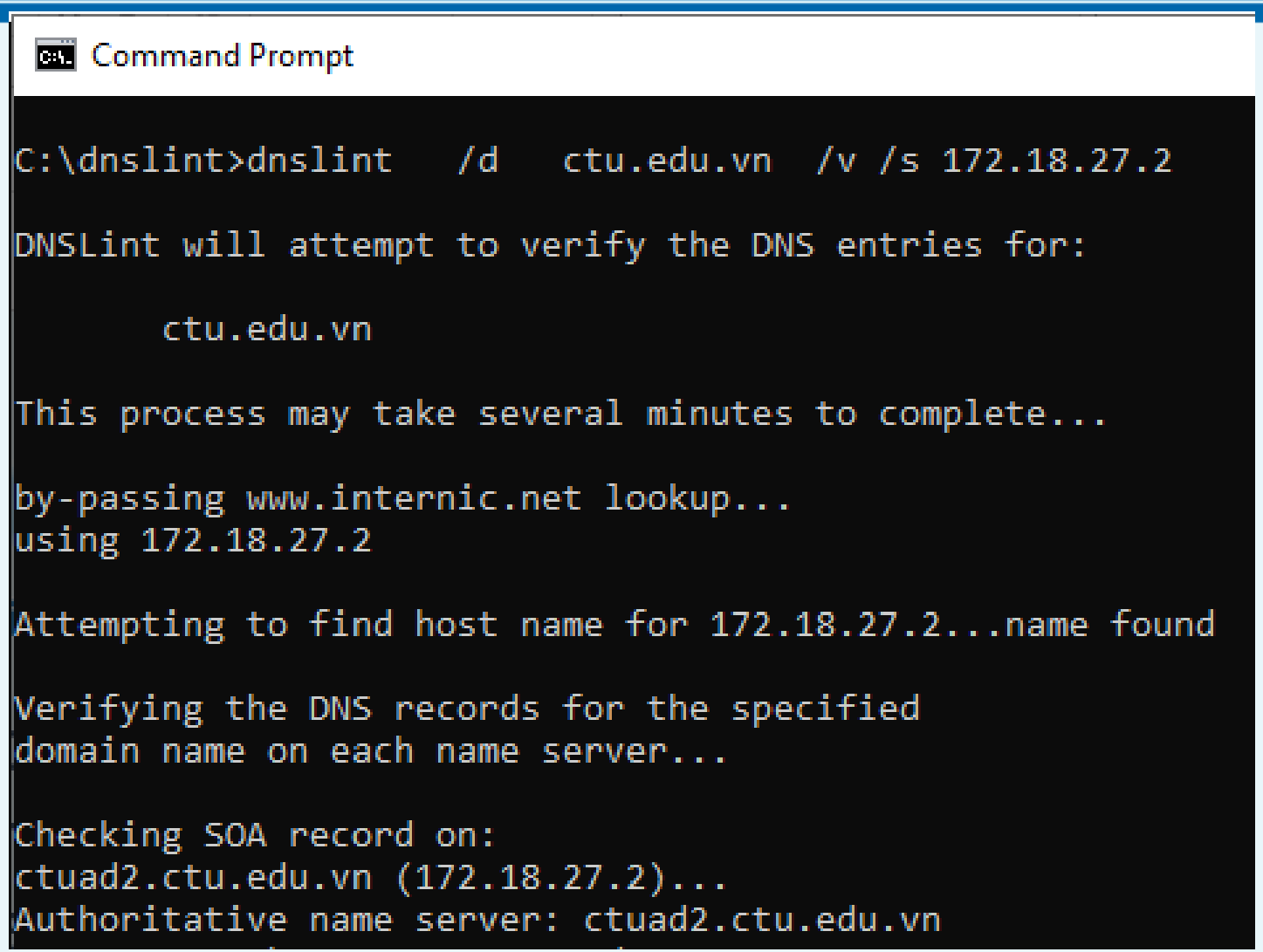
Listing the Contents of a Domain



DNS

Troubleshooting DNS: DNSLint

- utility to help diagnose:
  - some common DNS name-resolution issues
  - potential problems of incorrect delegation



DNS

Troubleshooting DNS: DNSLint

DNSLint Report

Tệp | C:/dnslint/dnslint.htm

DNSLint Report

System Date: Mon Aug 24 08:41:01 2020

Command run:

dnslint /d ctu.edu.vn /v /s 172.18.27.2

Domain name tested:

ctu.edu.vn

The following 4 DNS servers were identified as authoritative for the domain:

DNS server: ctuad2.ctu.edu.vn
IP Address: 172.18.27.2
UDP port 53 responding to queries: YES
TCP port 53 responding to queries: Not tested
Answering authoritatively for domain: YES

SOA record data from server:
Authoritative name server: ctuad2.ctu.edu.vn
Hostmaster: hostmaster.ctu.edu.vn
Zone serial number: 375045
Zone expires in: 0.13 day(s)
Refresh period: 900 seconds
Retry delay: 600 seconds
Default (minimum) TTL: 60 seconds

Additional authoritative (NS) records from server:
ctuad2.ctu.edu.vn 172.18.27.2
ctuad3.ctu.edu.vn 172.18.45.2
ctuad7.ctu.edu.vn 172.18.27.6
ctuad8.ctu.edu.vn 172.18.45.6

Host (A) records for domain from server:
172.18.27.2
172.18.45.2
10.18.36.54
172.18.27.6
172.18.45.6

Mail Exchange (MX) records from server (preference/name/IP address):
5 alt1.aspmx.l.google.com 74.125.28.27
1 aspmx.l.google.com 172.217.194.27
30 aspmx5.googlemail.com 173.194.209.27
5 alt2.aspmx.l.google.com 74.125.127.27
10 alt3.aspmx.l.google.com 209.85.234.27
10 alt4.aspmx.l.google.com 173.194.209.26
30 aspmx4.googlemail.com 209.85.234.26

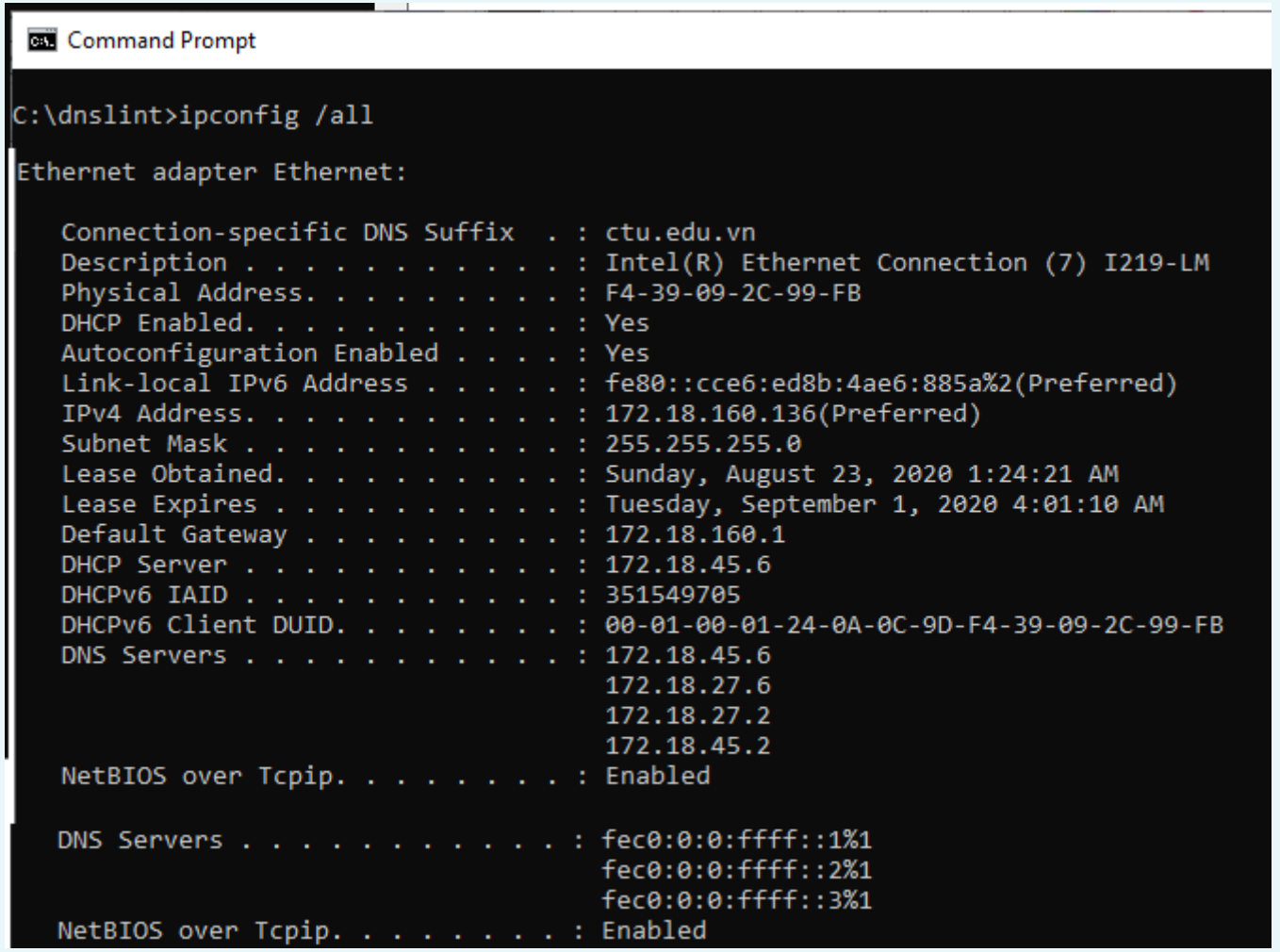
DNS server: ctuad7.ctu.edu.vn
IP Address: 172.18.27.6
UDP port 53 responding to queries: YES
TCP port 53 responding to queries: Not tested
Answering authoritatively for domain: YES

SOA record data from server:
Authoritative name server: ctuad7.ctu.edu.vn
Hostmaster: hostmaster.ctu.edu.vn
Zone serial number: 375045
Zone expires in: 0.13 day(s)
Refresh period: 900 seconds
Retry delay: 600 seconds
Default (minimum) TTL: 60 seconds

DNS

Ipconfig

- To view your DNS client settings
- To view and reset cached information used locally for resolving DNS name queries
- To register the resource records for a dynamic update client.



DNS

Ipconfig /flushdns

- After created, a new DNS record needs to replicate itself around to all of the other DCs in your network
- Once the new record exists on all of DC servers, your clients may still take a little bit of time to utilize the new record
- If you immediately test out a new DNS record just created and it's not working, try to run the command ***ipconfig /flushdns*** on your client computer

Integrating Dynamic DNS and IPv4 DHCP

CANTHO UNIVERSITY

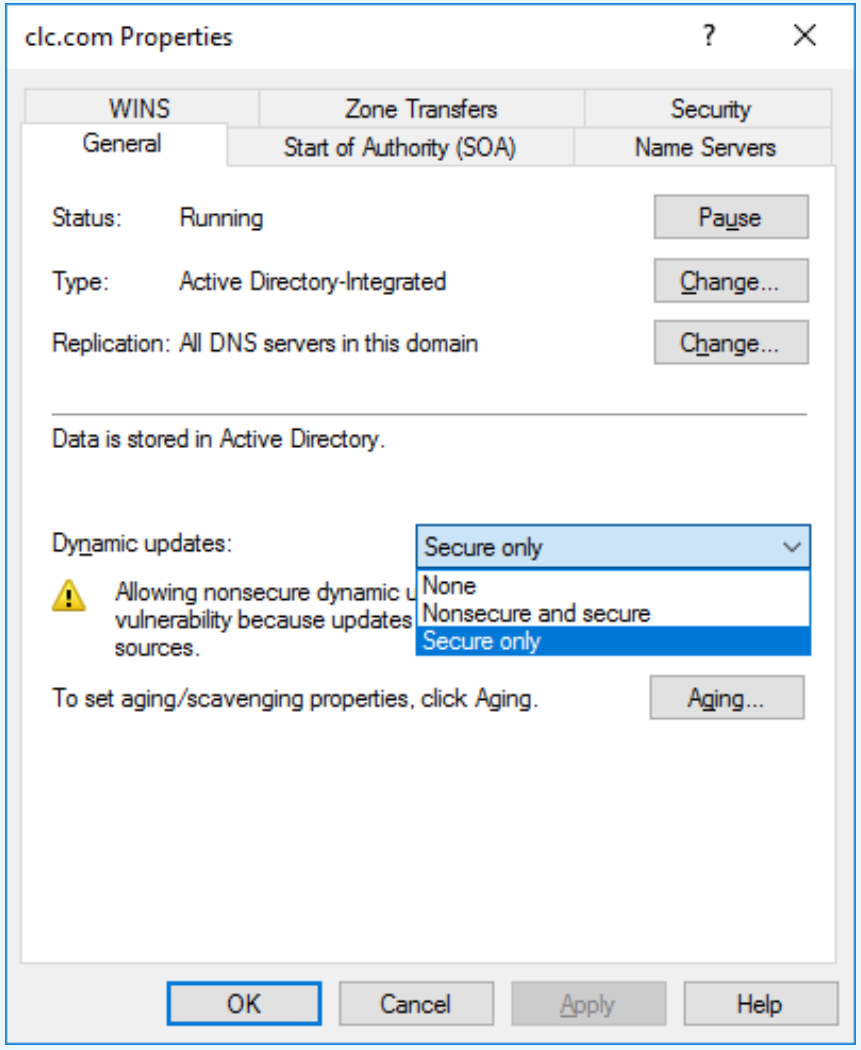
Integrating Dynamic DNS and IPv4 DHCP

- Dynamic DNS server can be updated in two ways:
  - DHCP client to tell the DNS server its address.
  - DHCP server tells the DNS server when it registers a new client
- Configuring DNS server to use Dynamic DNS at two level:
  - The scope level, it will apply only to the scope.
  - The server level, it will apply to all scopes and superscopes served by the server.

CANTHO UNIVERSITY

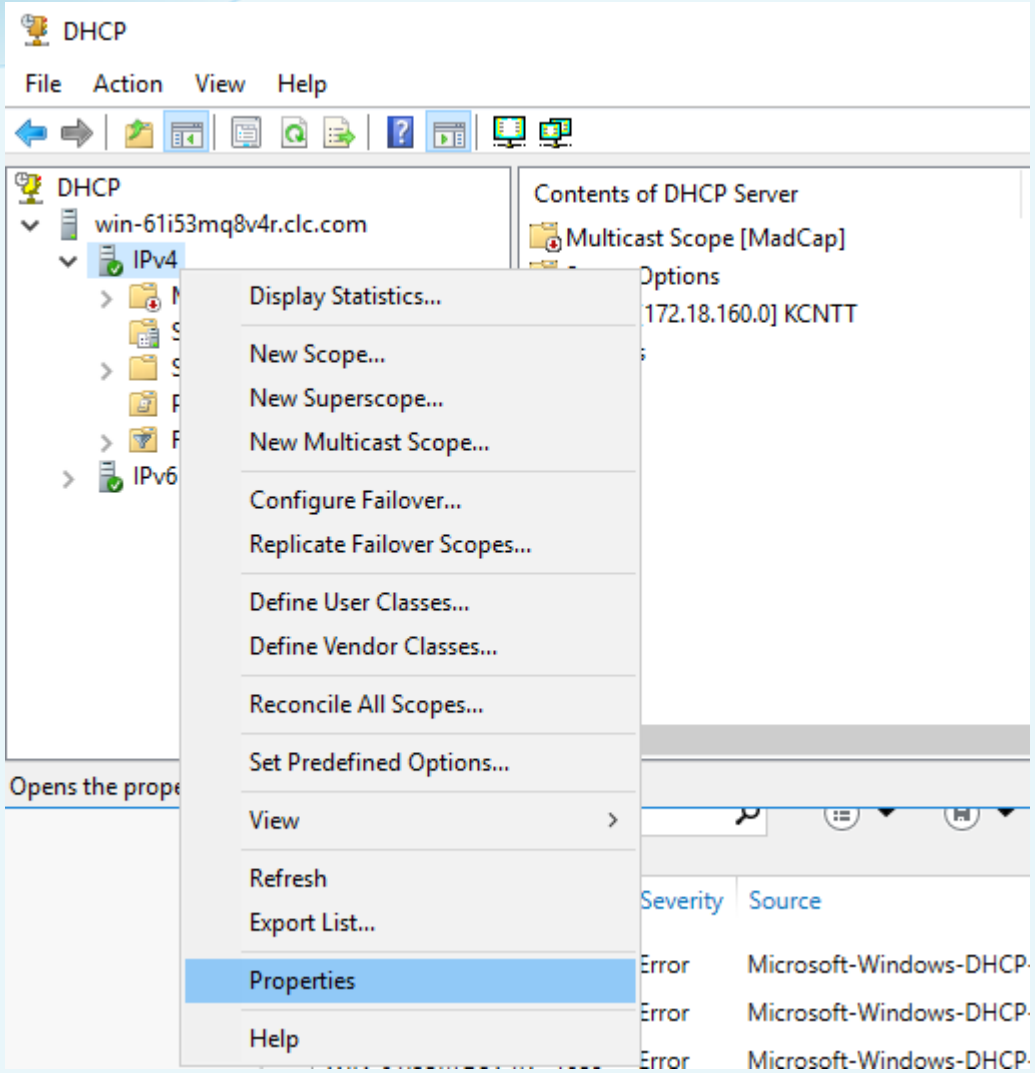
Integrating Dynamic DNS and IPv4 DHCP

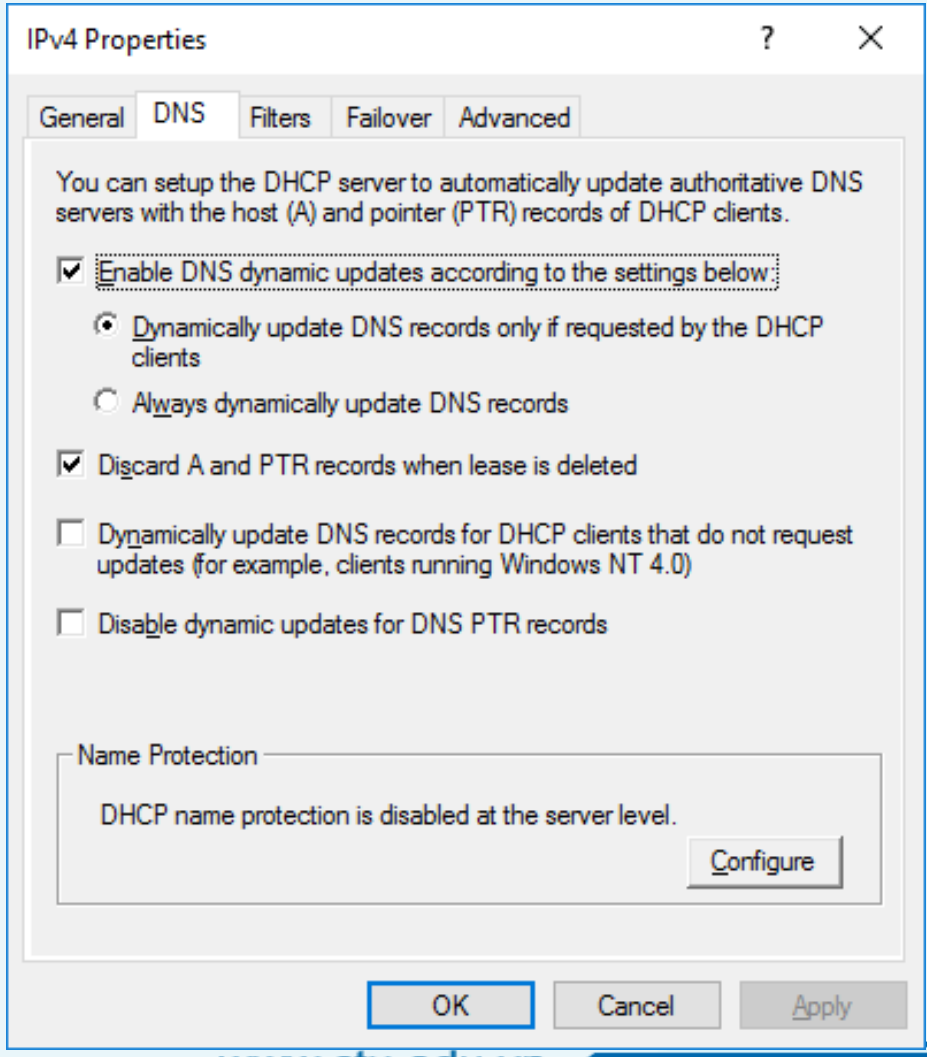
- Allow DNS clients to update information in the DNS database files
- Used with Dynamic IP address
- Allow to access devices in your home even if IP address changes



CANTHO UNIVERSITY

Integrating Dynamic DNS and IPv4 DHCP





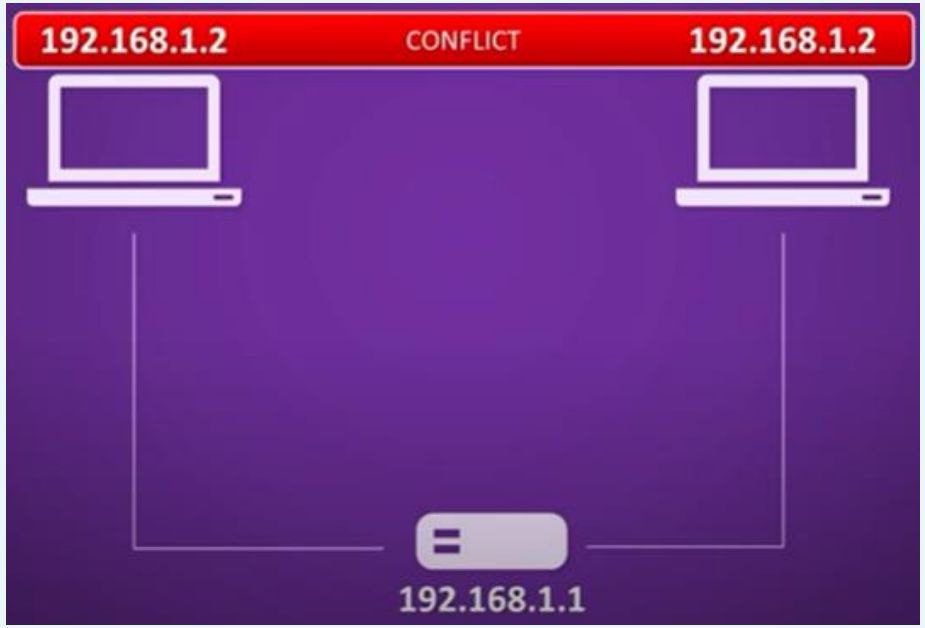
DHCP

Dynamic Host Configuration Protocol

DHCP

Static IP Address

- Manually assigned by administrator
- IP address not automatically change
- Must know the basic TCP/IP settings
  - Available IP address
  - Subnet mask
  - Default gateway
  - DNS servers
- Will not work if settings are invalid



DHCP

Static IP Address

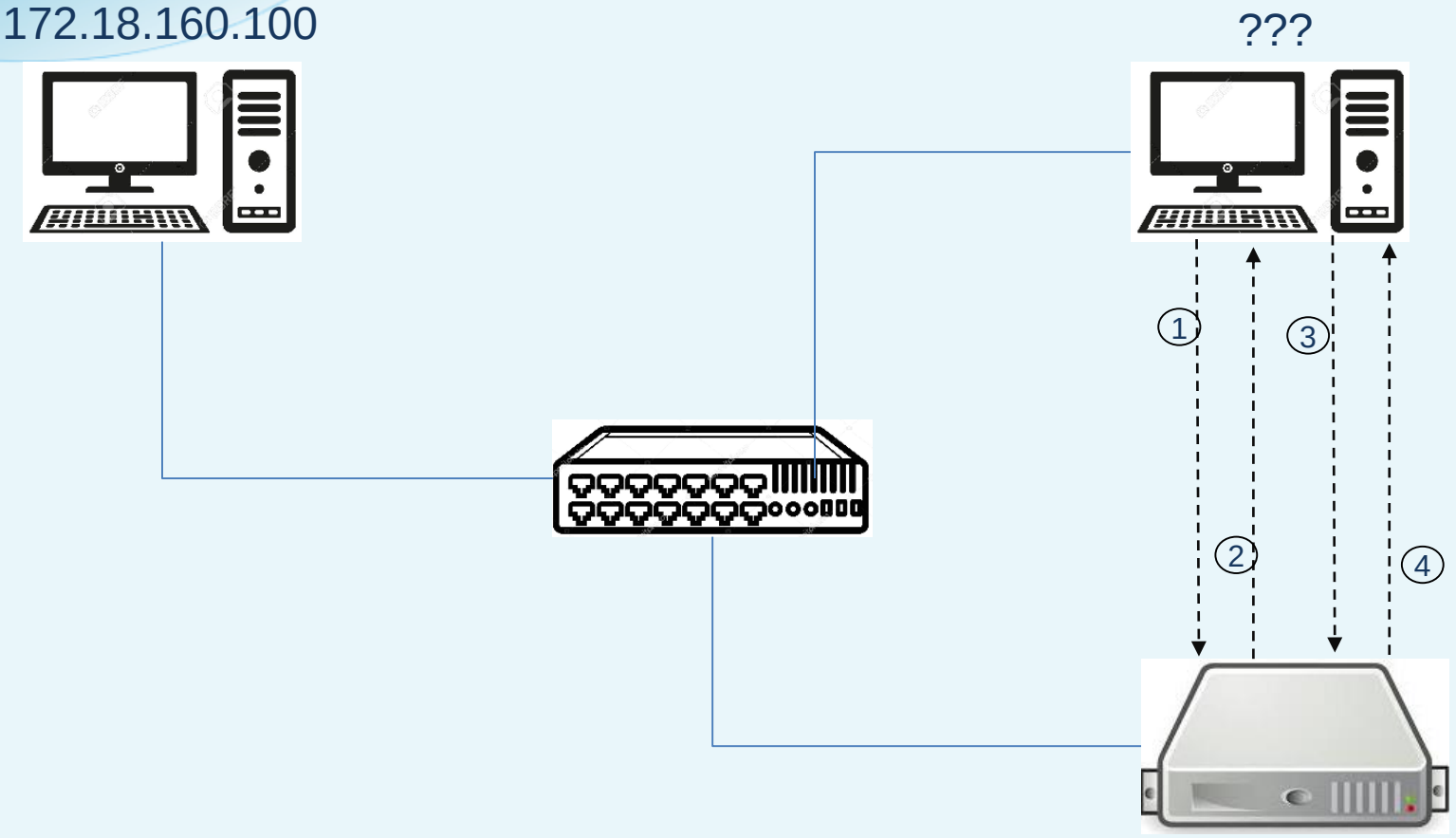
- Appropriate for servers, but what about on the client and device side?
- Are you willing to do static addressing if the company has 1000 devices?
- What happens if the company changes to new IP address (sub)net

DHCP
Overview

- Dynamic Host Configuration Protocol (DHCP)
- Solve static addressing problem by allowing DHCP server to automatically set IP configuration network for client computers
- Users uses DHCP every day without even realizing it
- DHCP can run on the router or on OS such as Windows.

DHCP

Overview

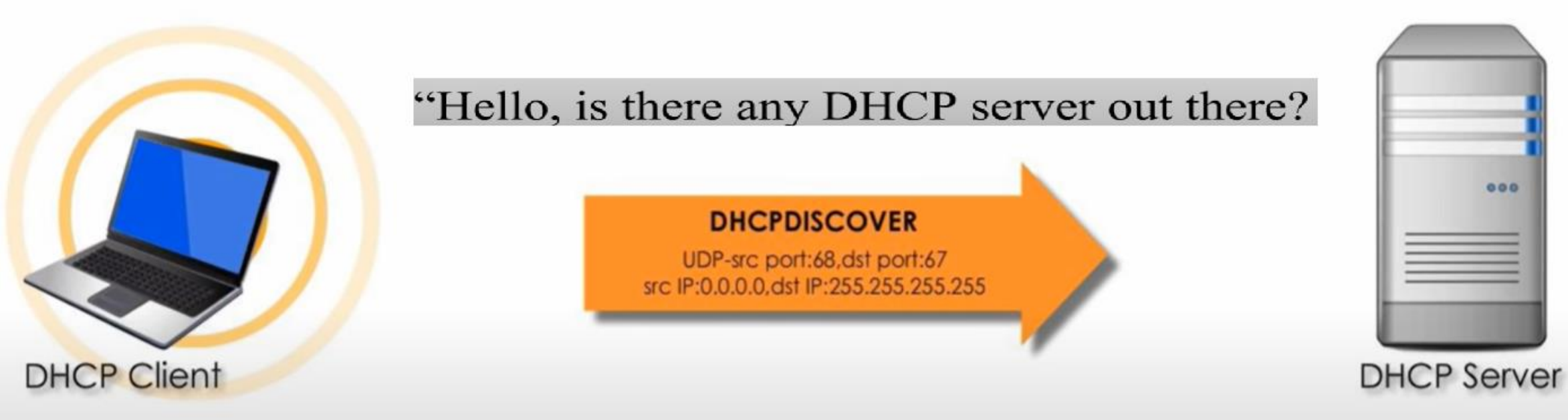


1. Address please!
2. Want 172.18.160.101
3. I'll take 172.18.160.101
4. Alright

DHCP

How DHCP works

Step 1: DHCP client searches for DHCP server



DHCP

How DHCP works

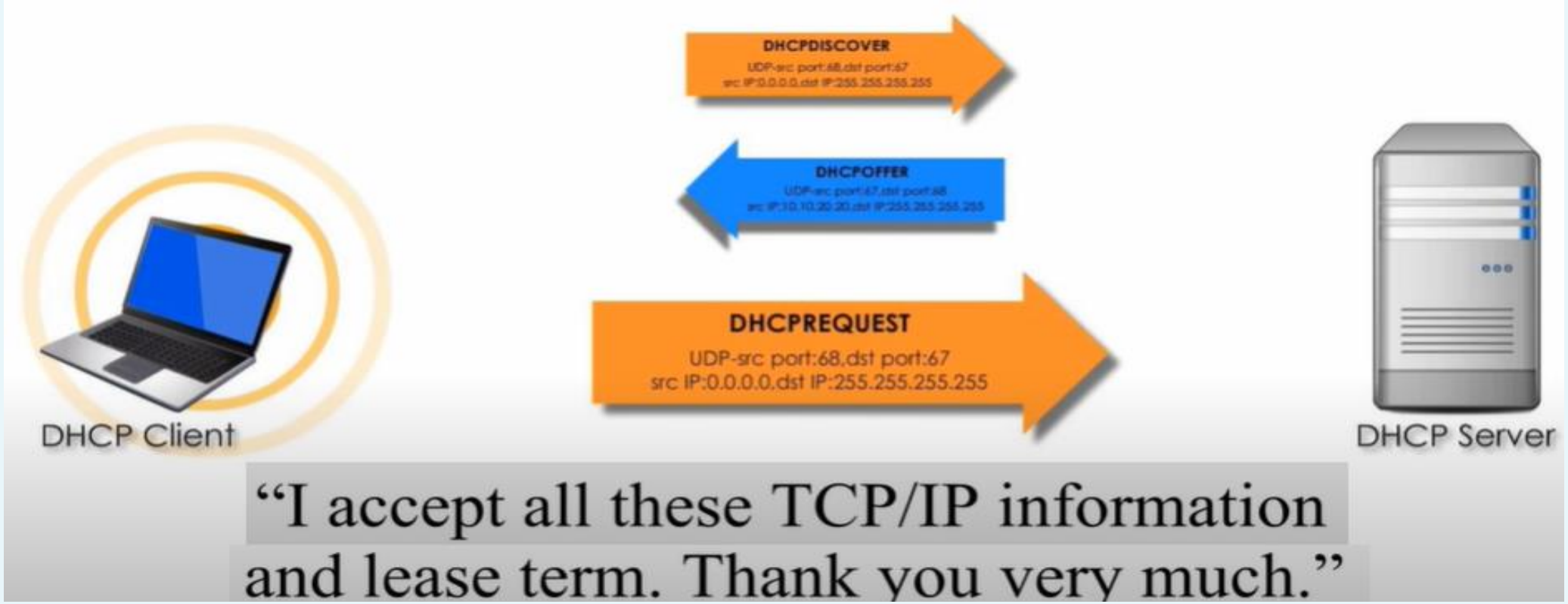
Step 2: DHCP servers make an offer

Subnet mask, Default gateway, DNS servers and lease duration

DHCP

How DHCP works

Step 3: Host chooses offer and requests address



DHCP

How DHCP works

Step 4: DHCP server confirms the address

OK, Let's do these. You go ahead use the network, and I register your MAC address and other IP information in my DHCP database!

DHCP

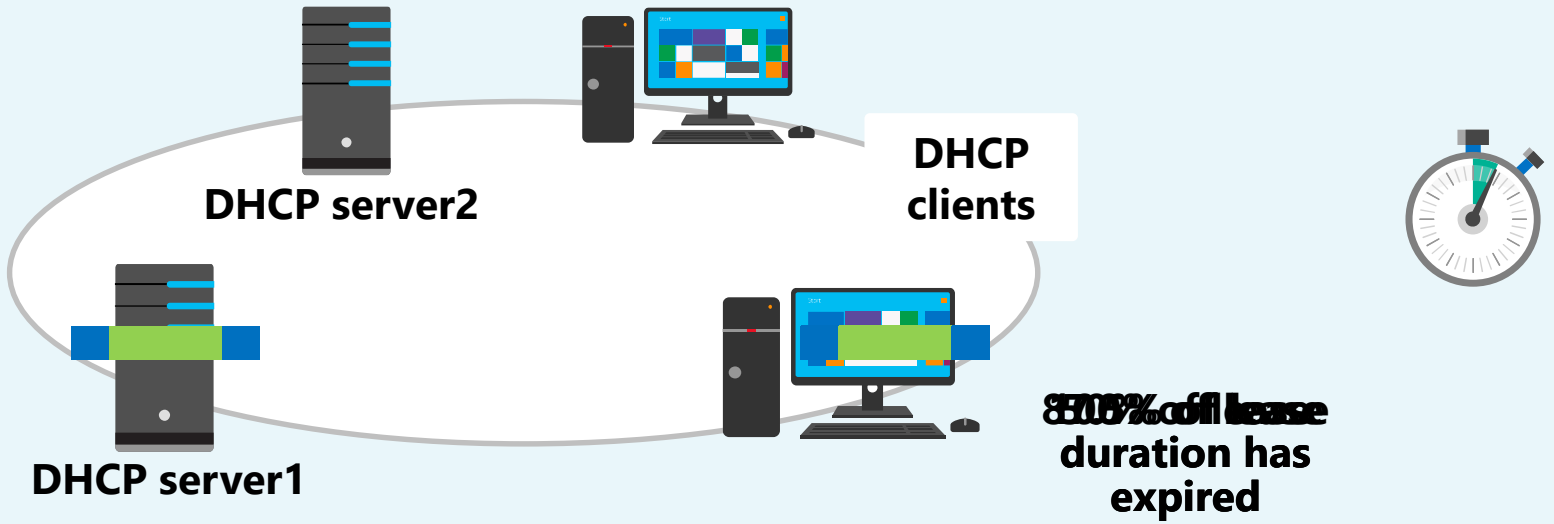
Benefits of using DHCP

- 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

DHCP

DHCP lease renewal



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

DHCP
Scope

- DHCP uses scopes as the basis for managing and assigning IP addressing information.
- Contiguous range of addresses
- There's usually one scope per physical subnet
- Each scope has a set of parameters, scope options, that can be configured
- Scope options control what data is delivered to DHCP clients

DHCP
Address Pool

- The range of IP addresses that the DHCP server can assign
- **For example**: let's say you set up a new DHCP scope covering the 192.168.1 subnet.
  - 255 IP addresses in the pool.
  - After adding an exclusion from 192.168.1.240 to 192.168.1.254
  - Having 241 (255 – 14) IP addresses left in the pool.
  - That means (in theory, at least) that you can service 241 unique clients at a time before you run out of IP addresses

DHCP
Superscope

- Enable the DHCP server to provide addresses from more than one scope to clients on the same physical subnet
- Helpful when clients within the same subnet have more than one IP network and thus need IPs from more than one address pool
- Must still configure other scope options individually for each child scope

DHCP

Exclusions and Reservations

- **Exclusions**
  - IP addresses within the range that you never want automatically assigned
  - Used to set aside addresses that you want to assign permanently to servers
- **Reservations**
  - IP addresses within the range for which you want a permanent DHCP lease
  - Essentially reserve a particular IP address for a particular device.
  - The device still goes through the DHCP process but it always obtains the same addressing information from the DHCP server.

- Installation process installs just the service and its associated snap-in
- At that point, it's not delivering any DHCP service

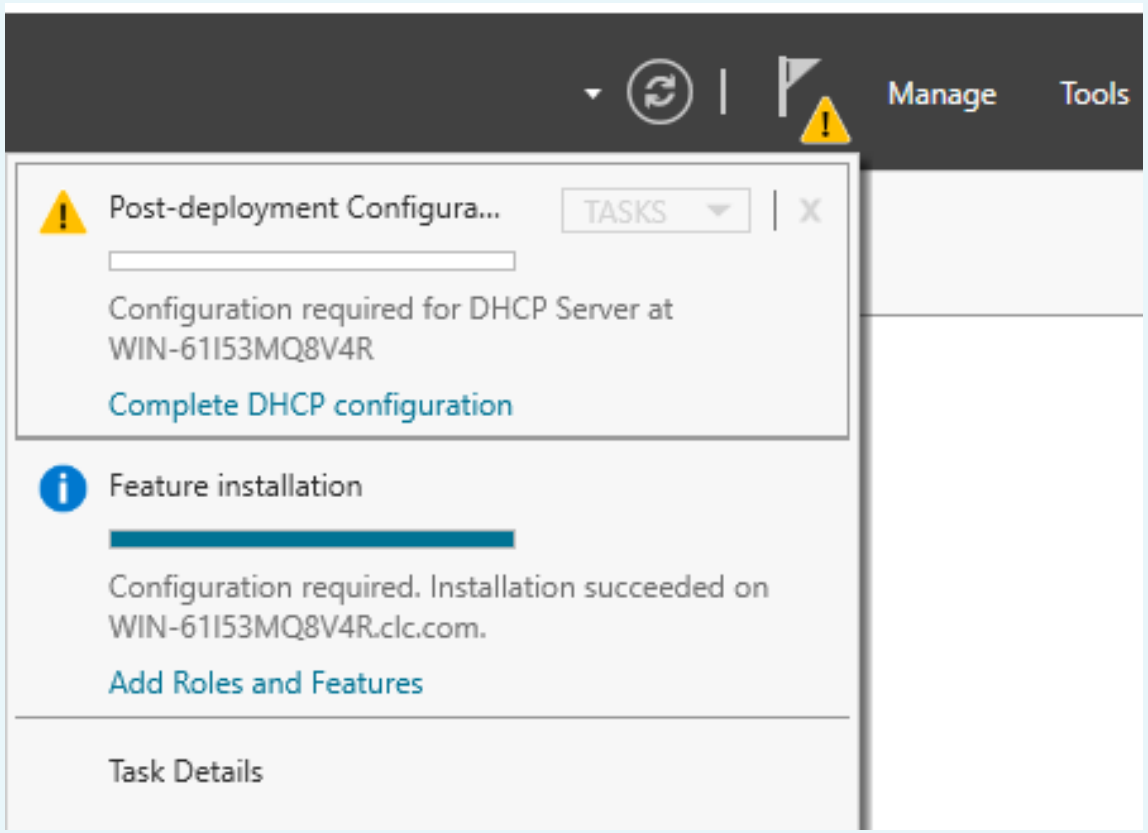
Installing the DHCP Service

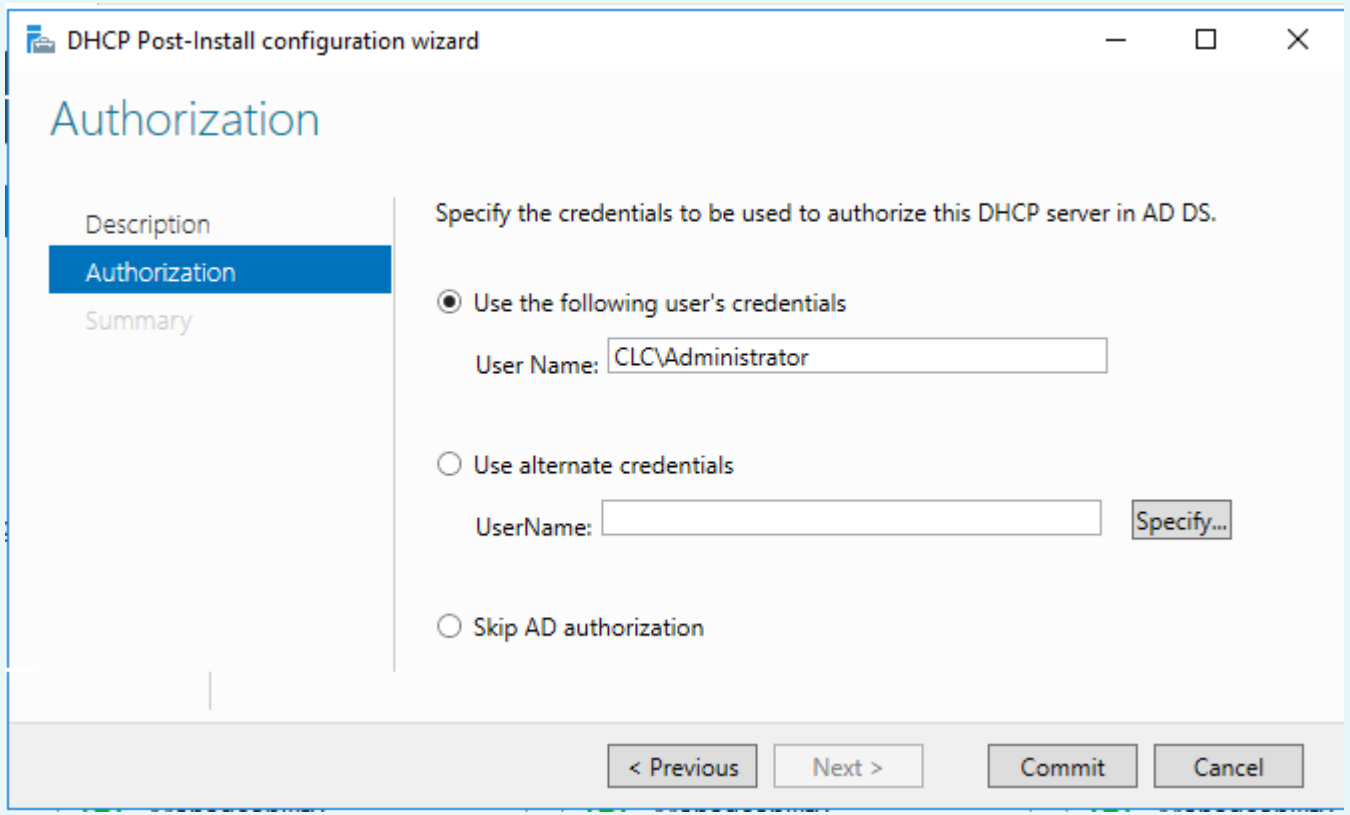
1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click **Add Roles And Features**.
3. Choose **role-based or feature-based installation** and click Next.
4. Choose your server and click Next.
5. Choose **DHCP Server**, the click **Add Features** and click Next.

DHCP

DHCP configuration

- After installing, we need to configure the DHCP server





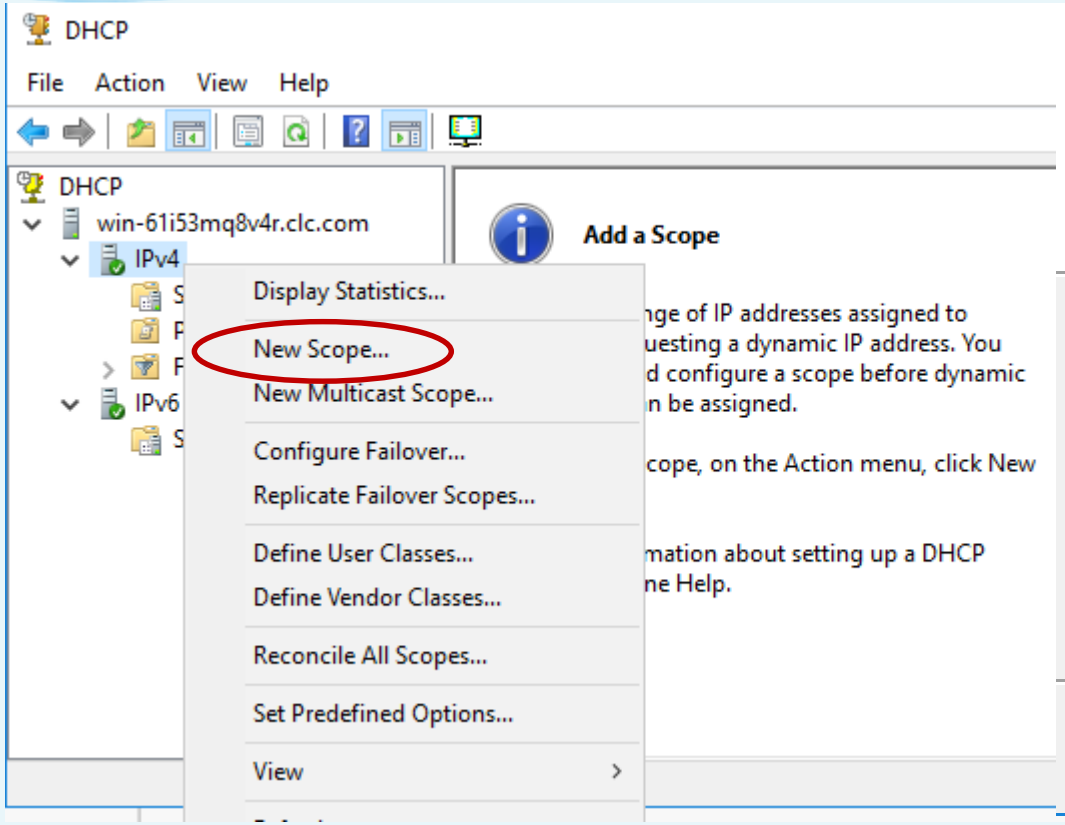
DHCP

Create a DHCP scope

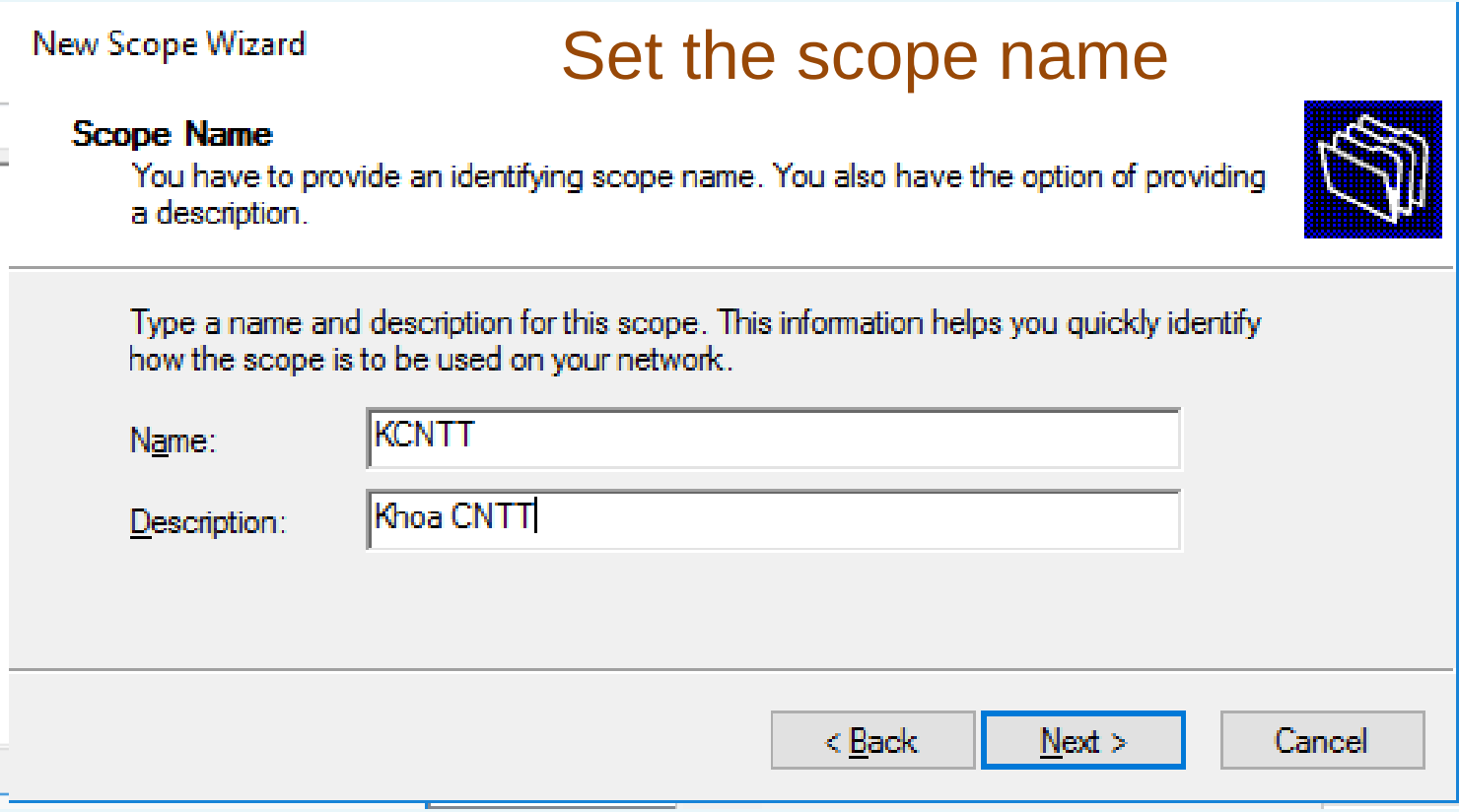
- Create scopes to define the network information distributed to clients
- Need the following information to define a scope:
  - A range of IP addresses and subnet mask;
  - A lease duration
  - IP addresses to exclude from the pool
  - IP Addresses to be reserved
- Values for DHCP options: Default gateway address; DNS server, suffix,..

DHCP

Create a DHCP scope



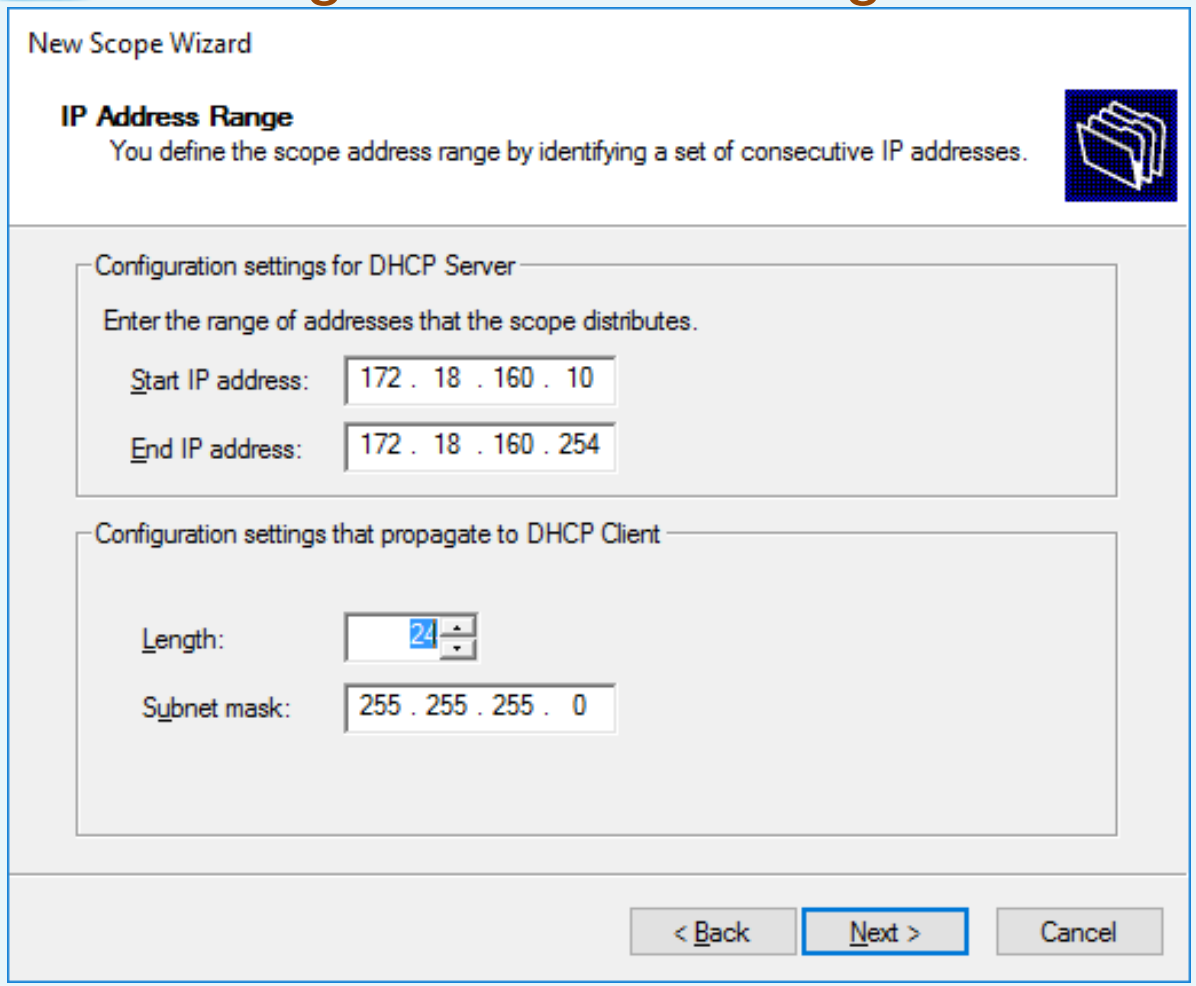
Set the scope name



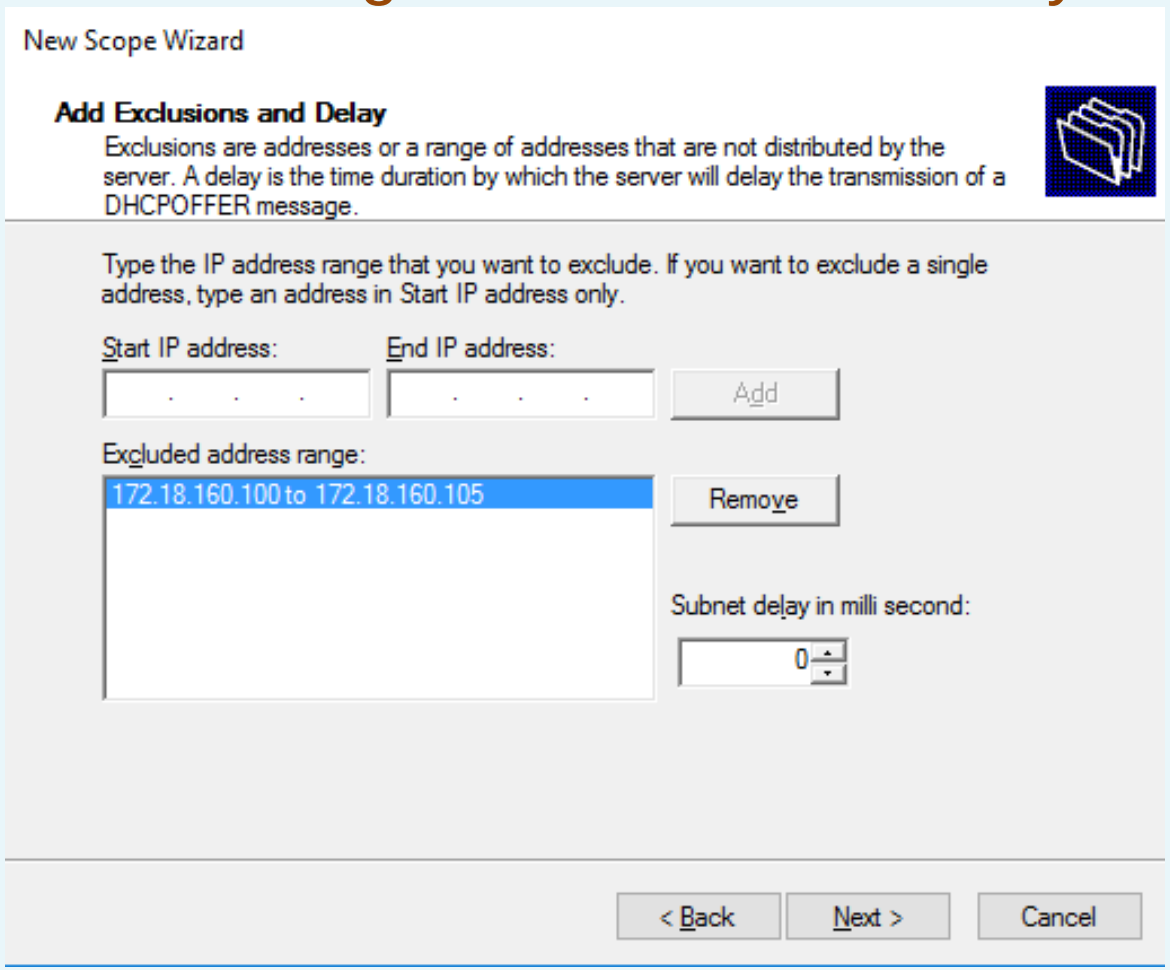
DHCP

Create a DHCP scope

Defining IP Address Range



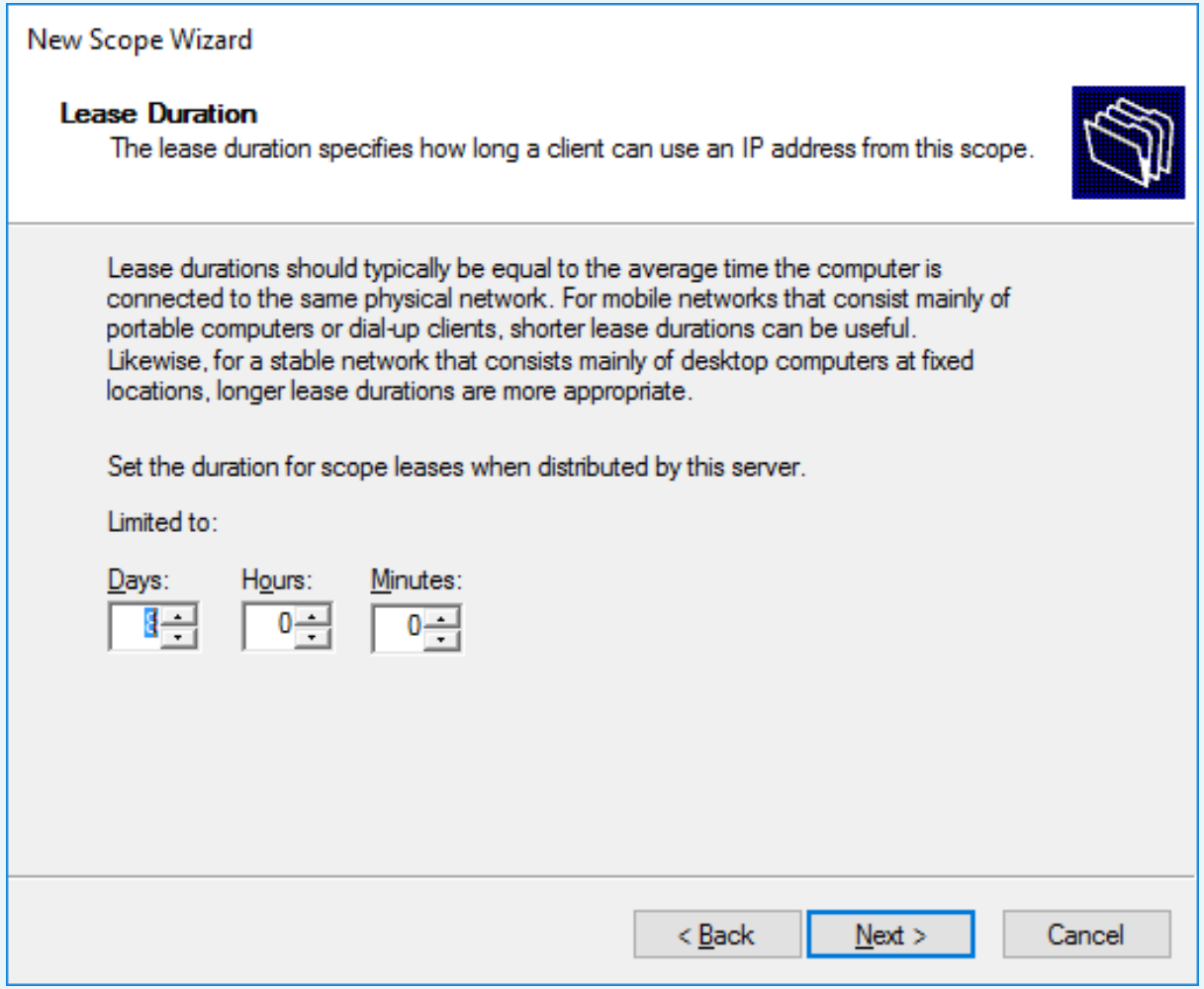
Adding Exclusions and Delay



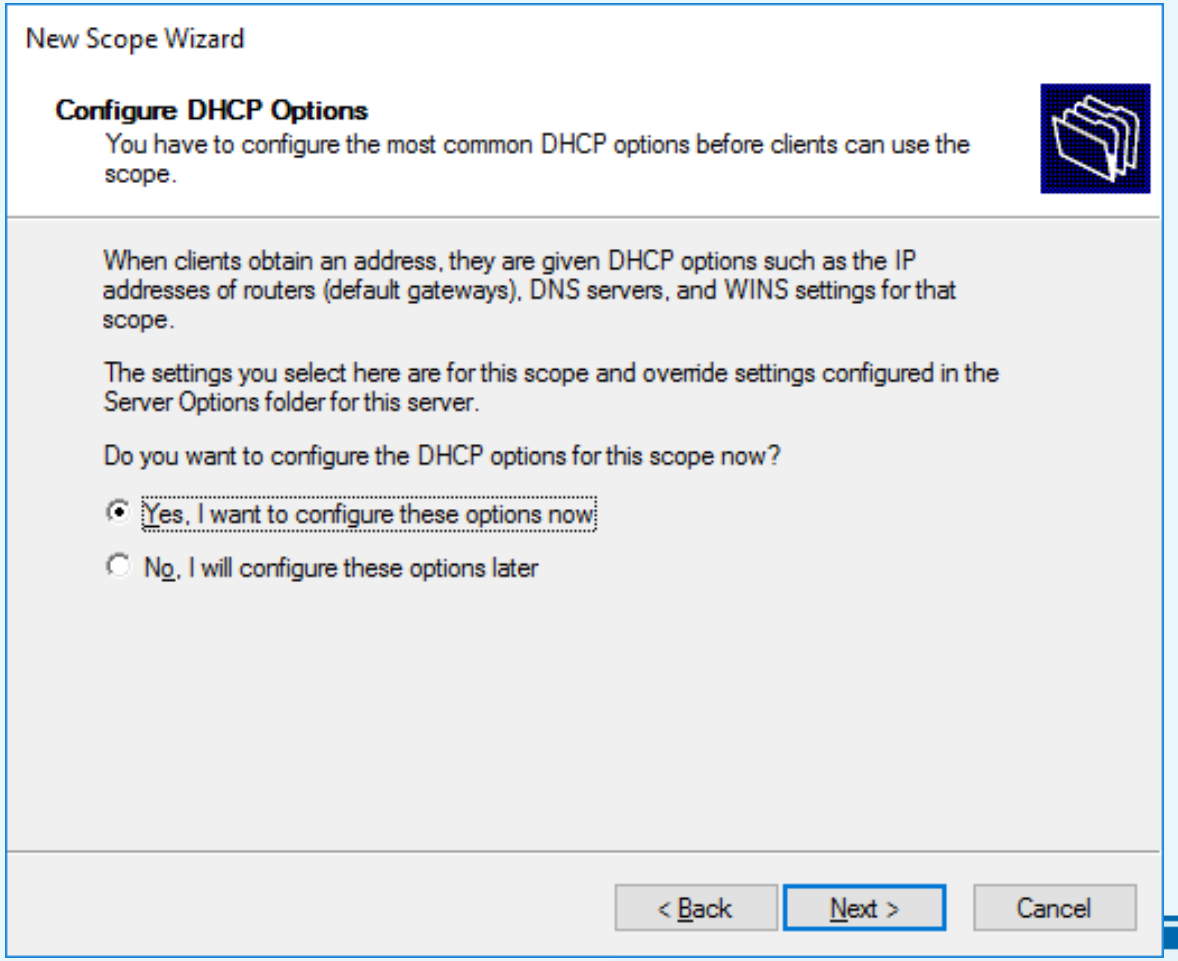
DHCP

Create a DHCP scope

Setting a Lease Duration



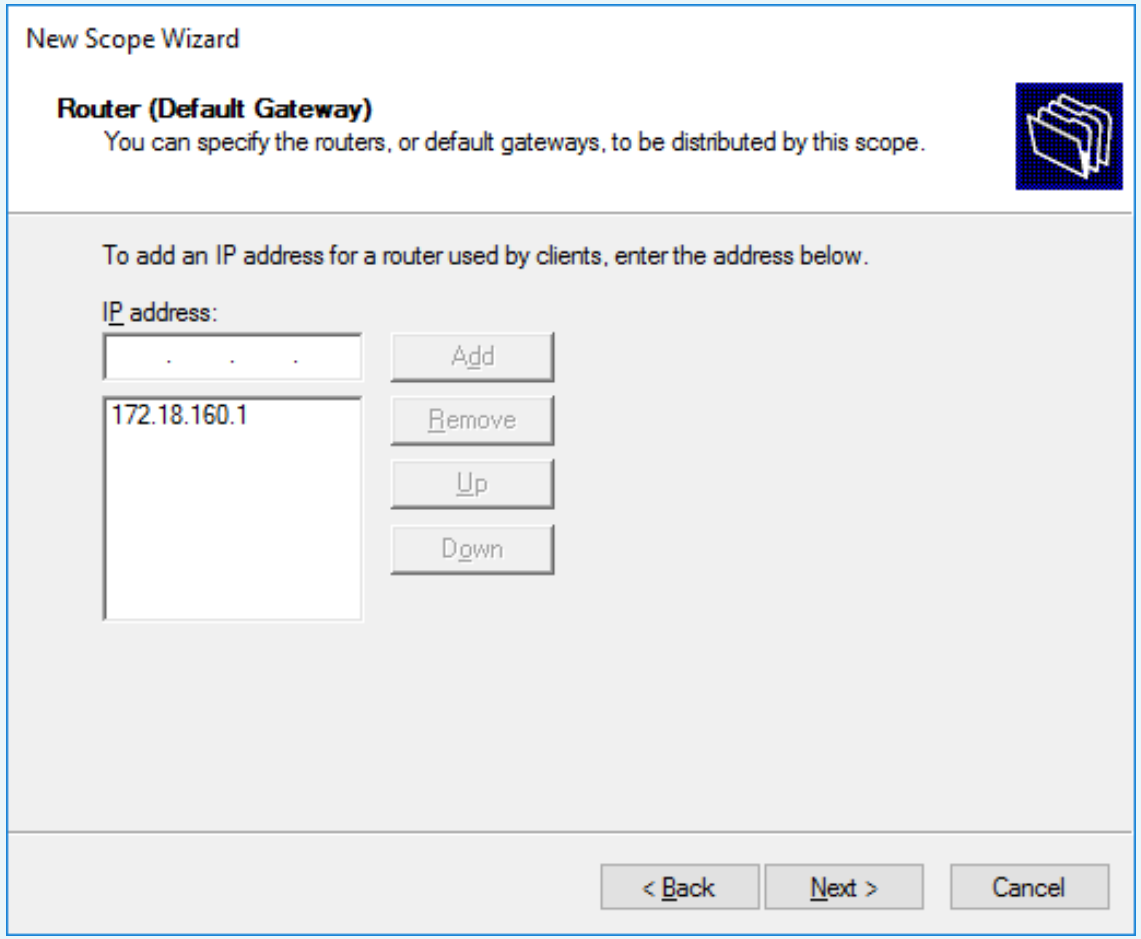
Configuring Basic DHCP Options



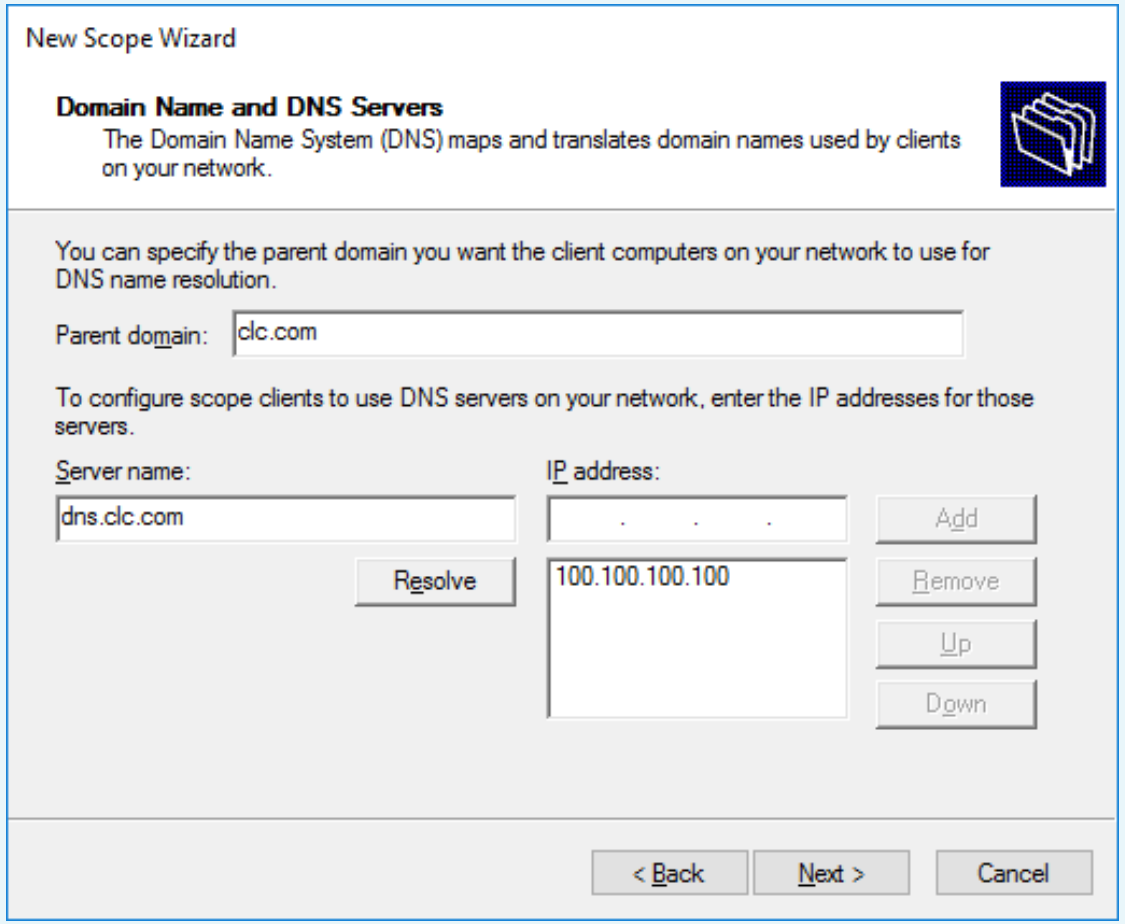
DHCP

Create a DHCP scope

Configuring Default Gateway

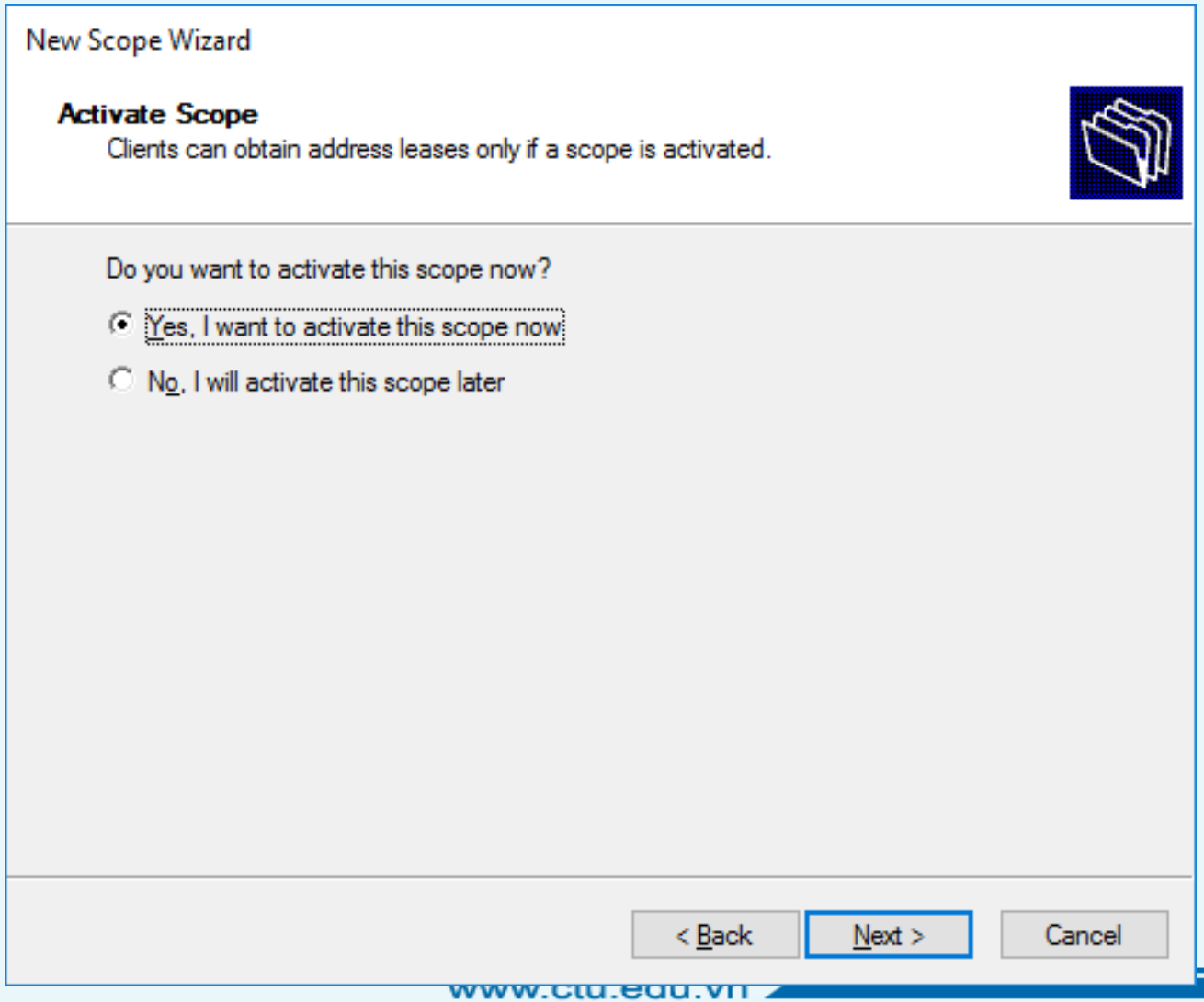


Providing DNS Settings



Activating the Scope

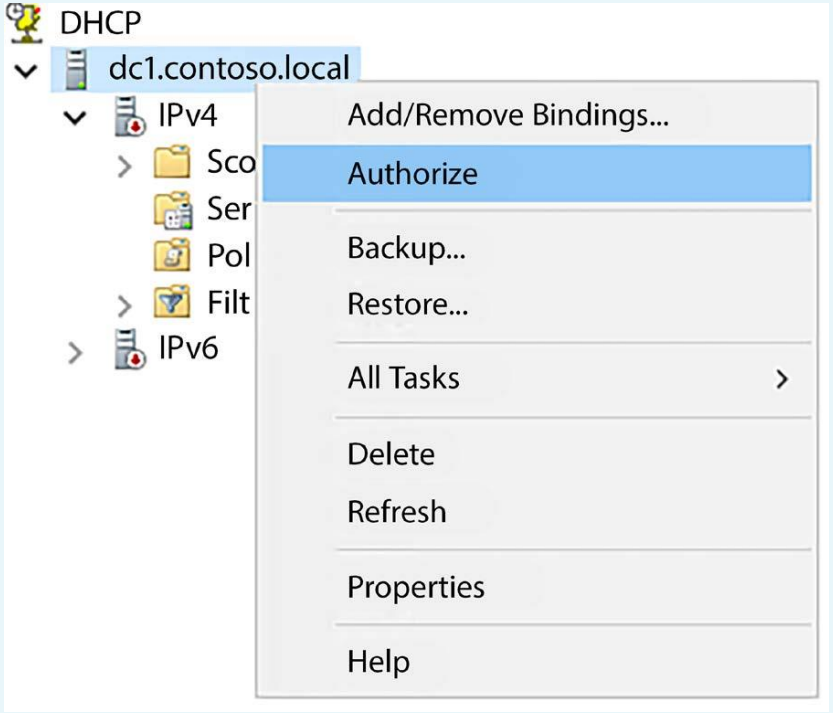
- After finishing creating the scope, it is immediately active and any computer can obtain address from a DHCP server

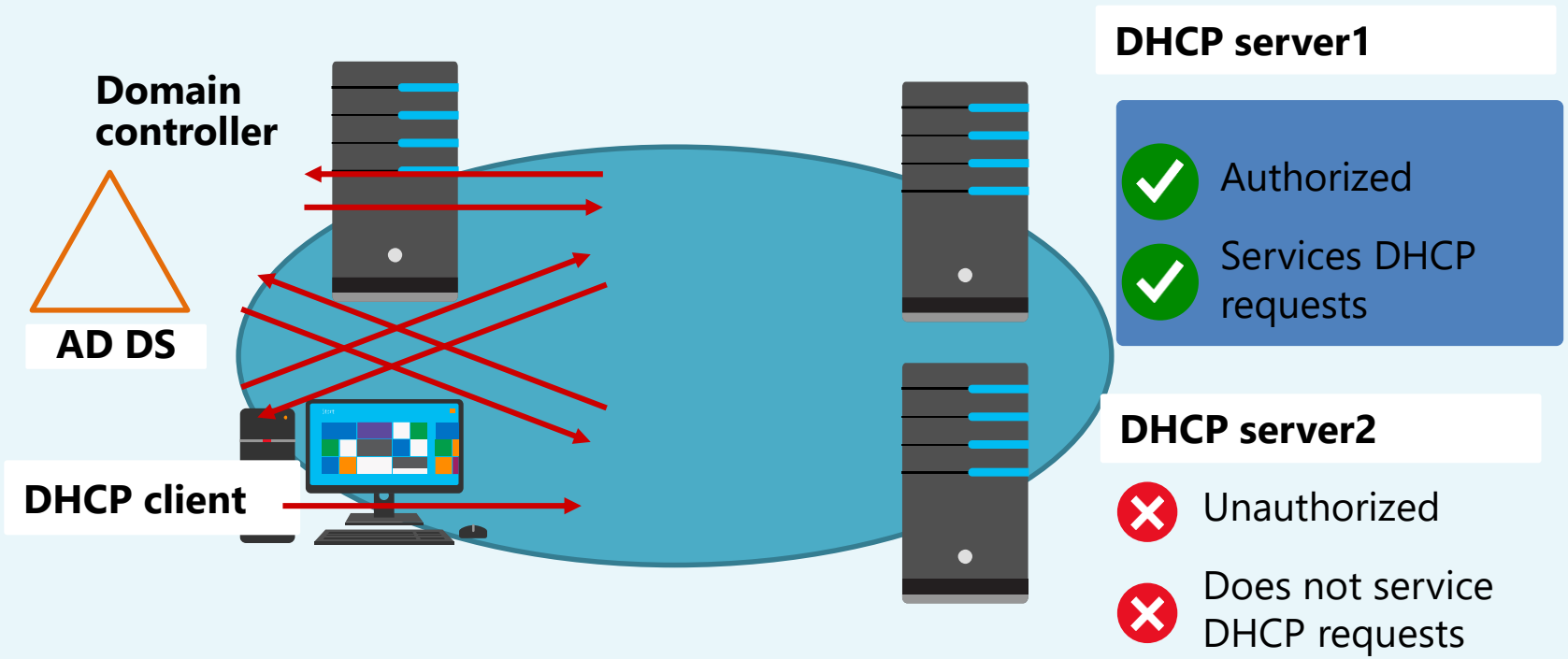


DHCP

Authorize the DHCP server

- Register the DHCP Server in the AD to support DHCP clients





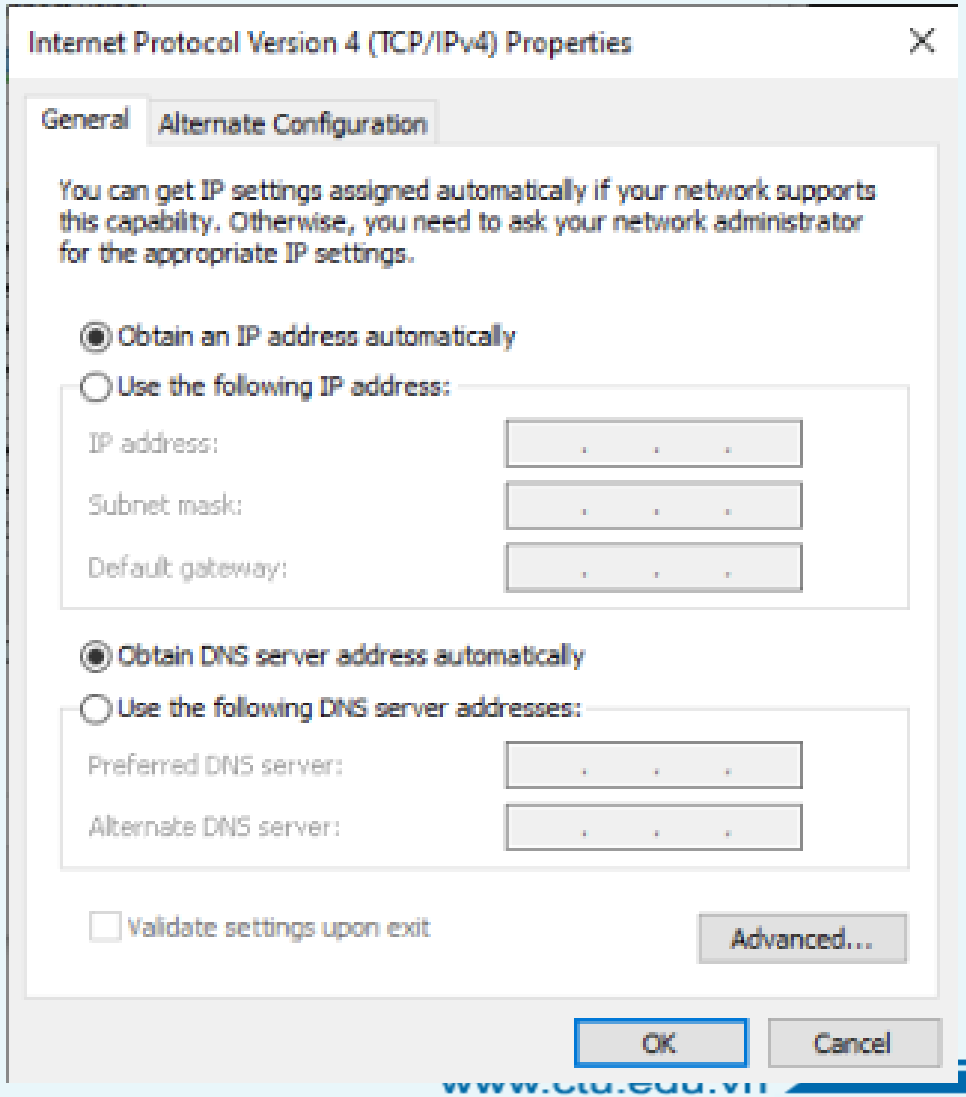
- If DHCP Server1 finds its IP address on the list, the service starts and supports DHCP clients

CANTHO UNIVERSITY

DHCP

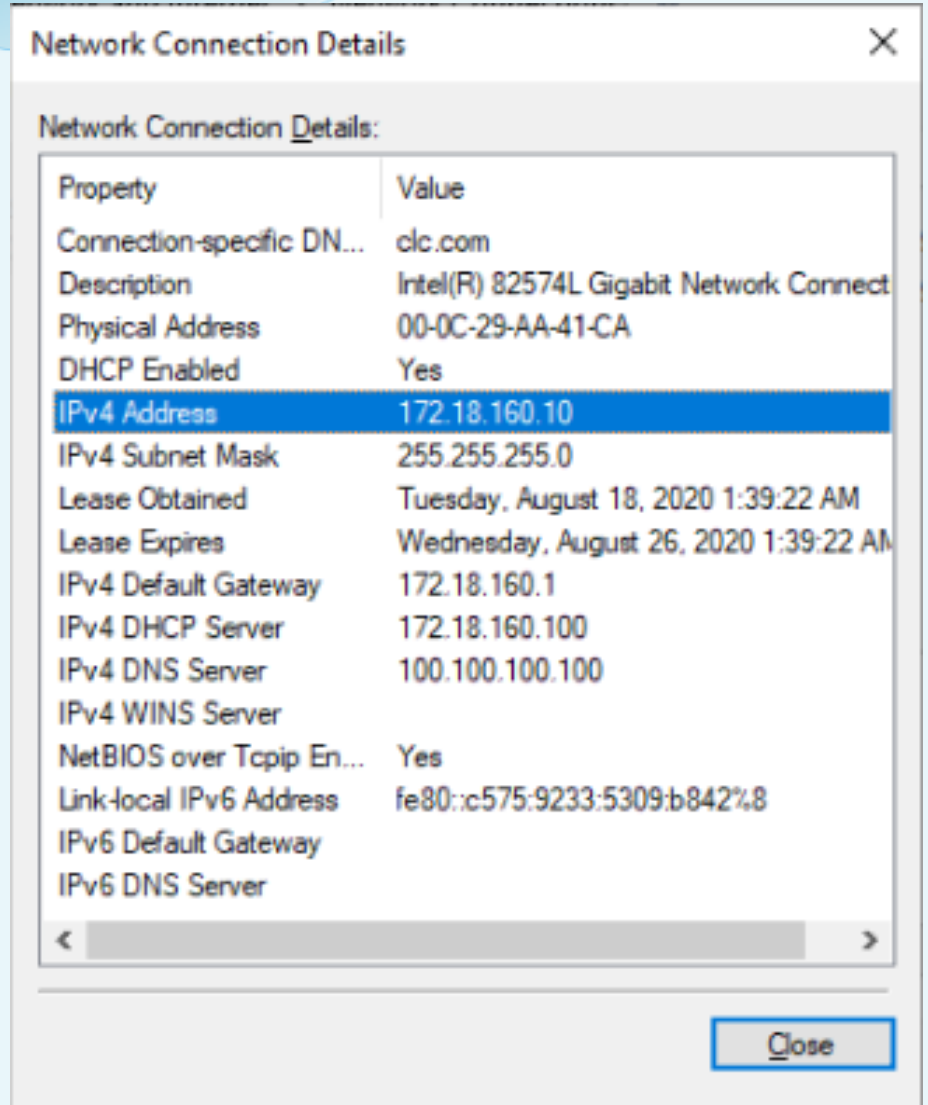
Verifying DHCP

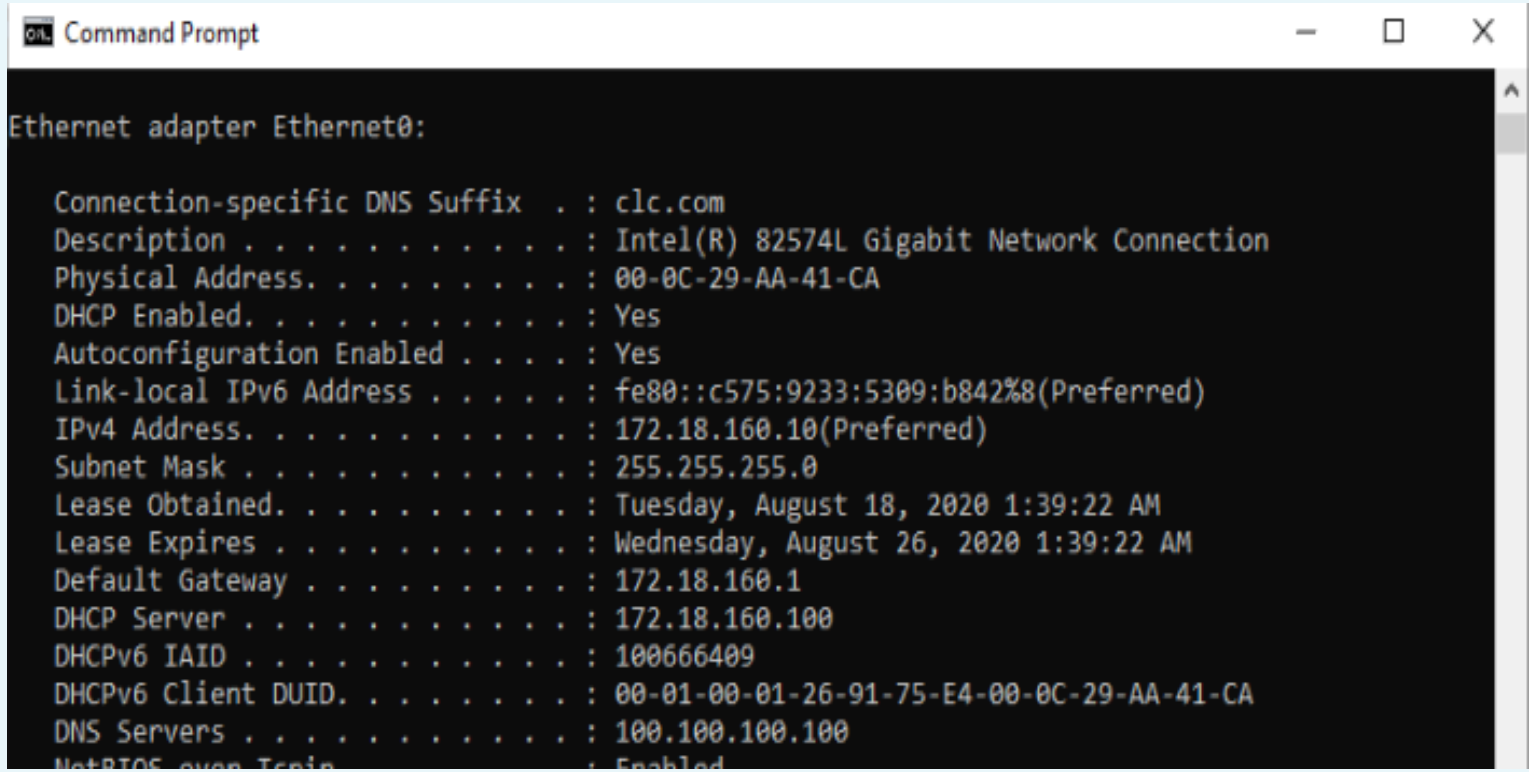
- To test the operation of DHCP server, start a windows 10 client and configuring it to obtain IP from DHCP



DHCP

Verifying DHCP





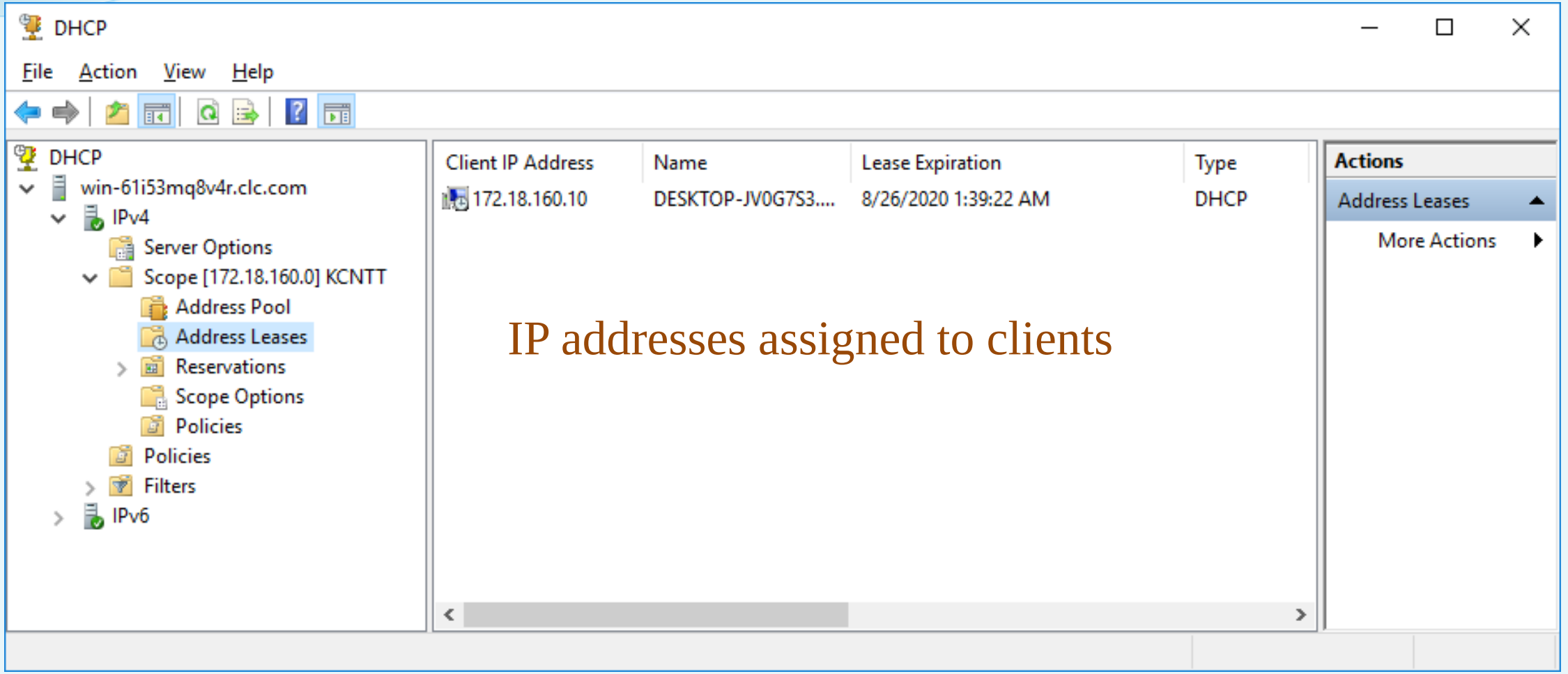
DHCP

Managing DHCP scope

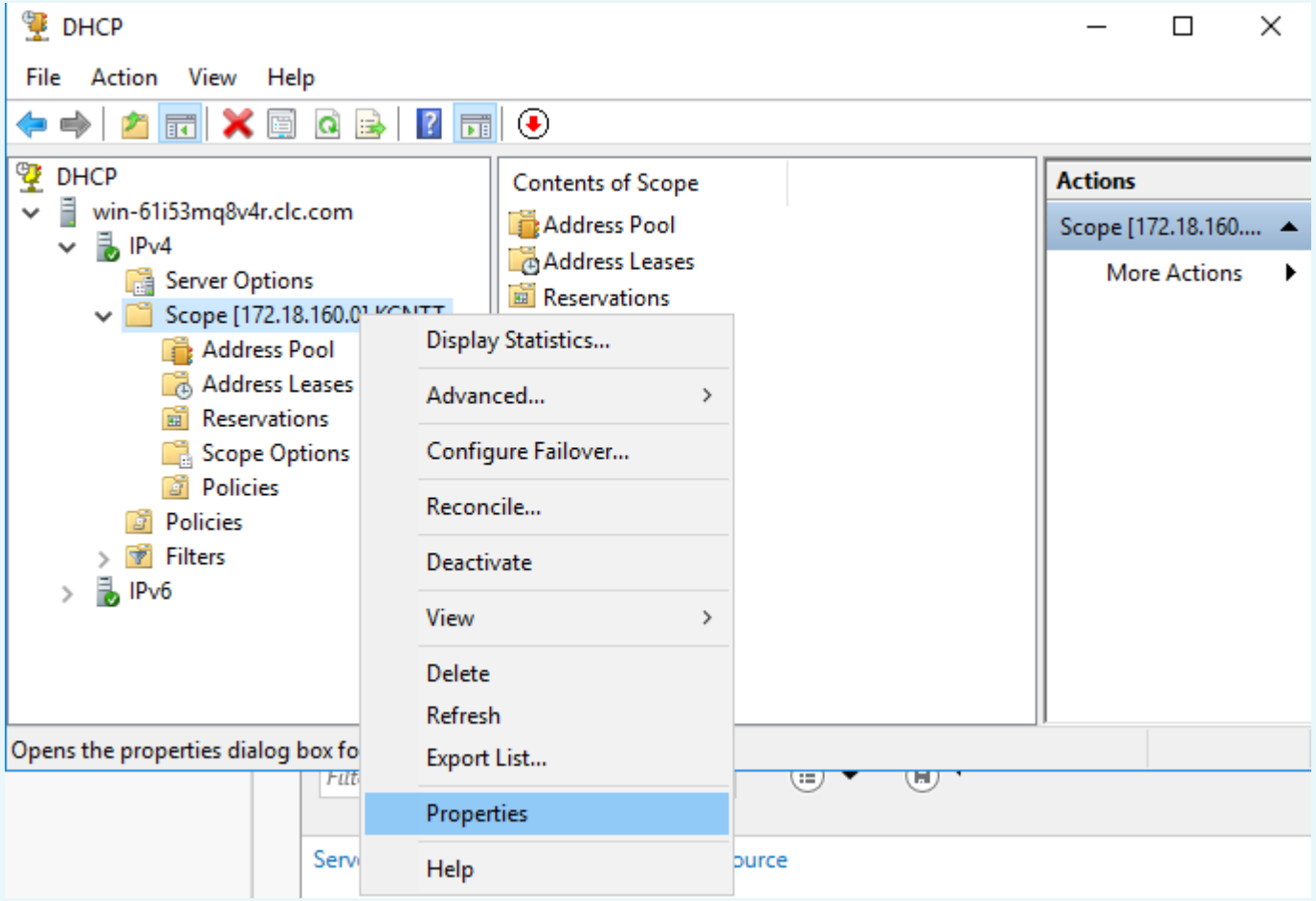
- From **Server Manager**, click on **Tools** menu and then choose **DHCP**

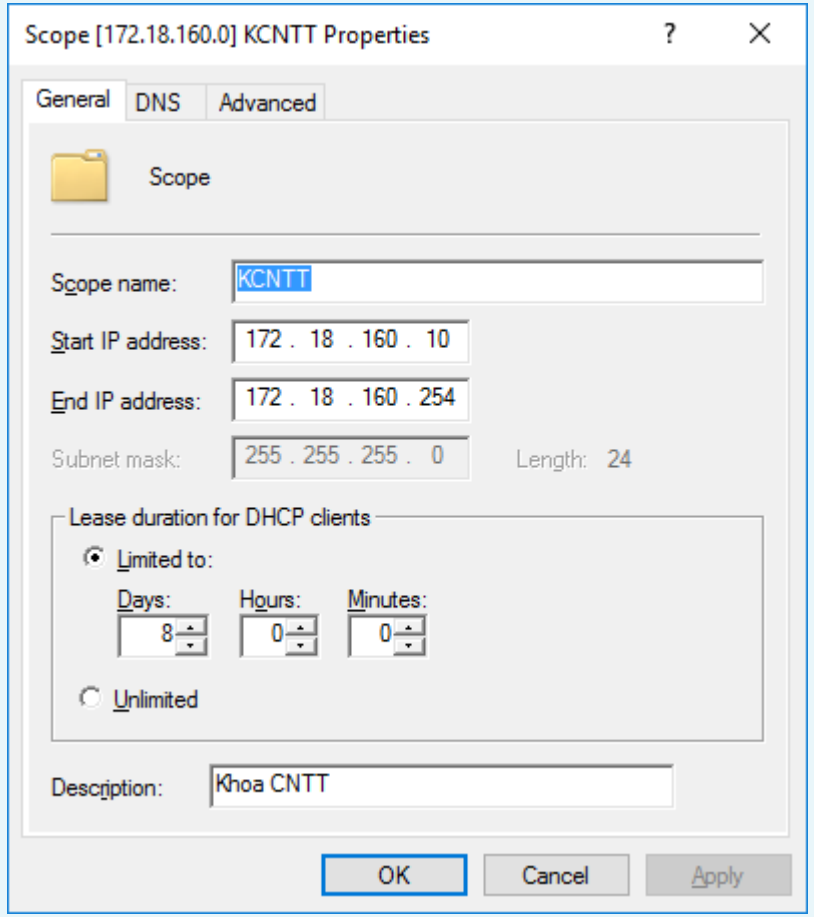
DHCP

Managing DHCP scope

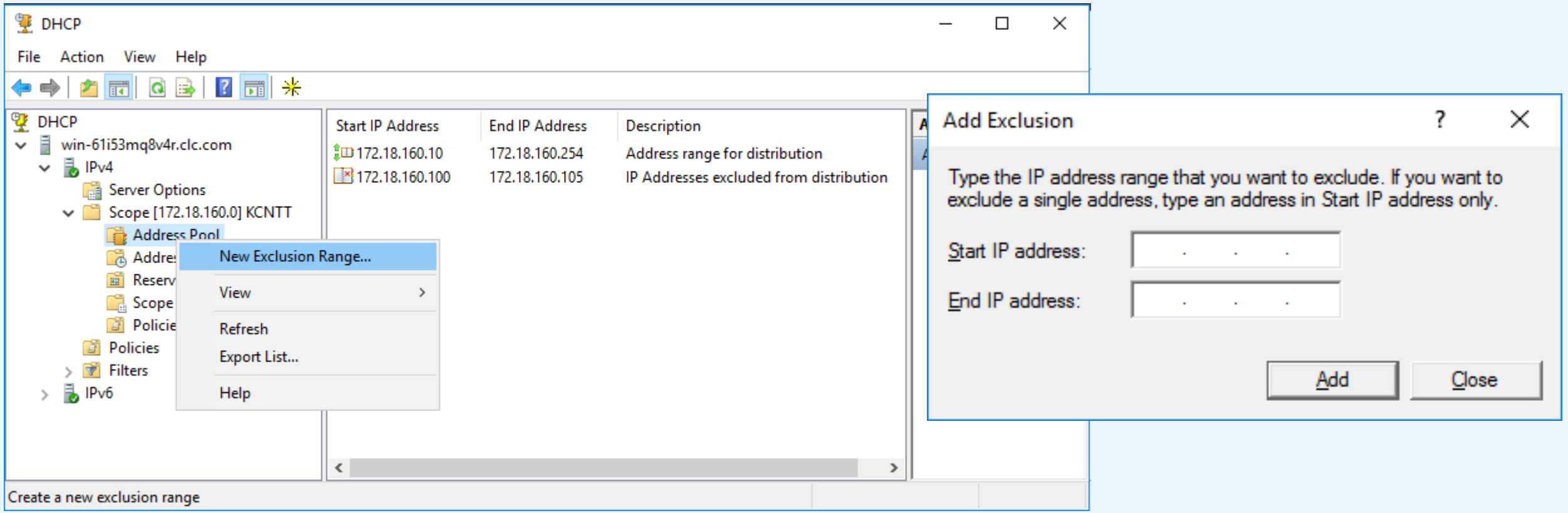


Changing the IP address range

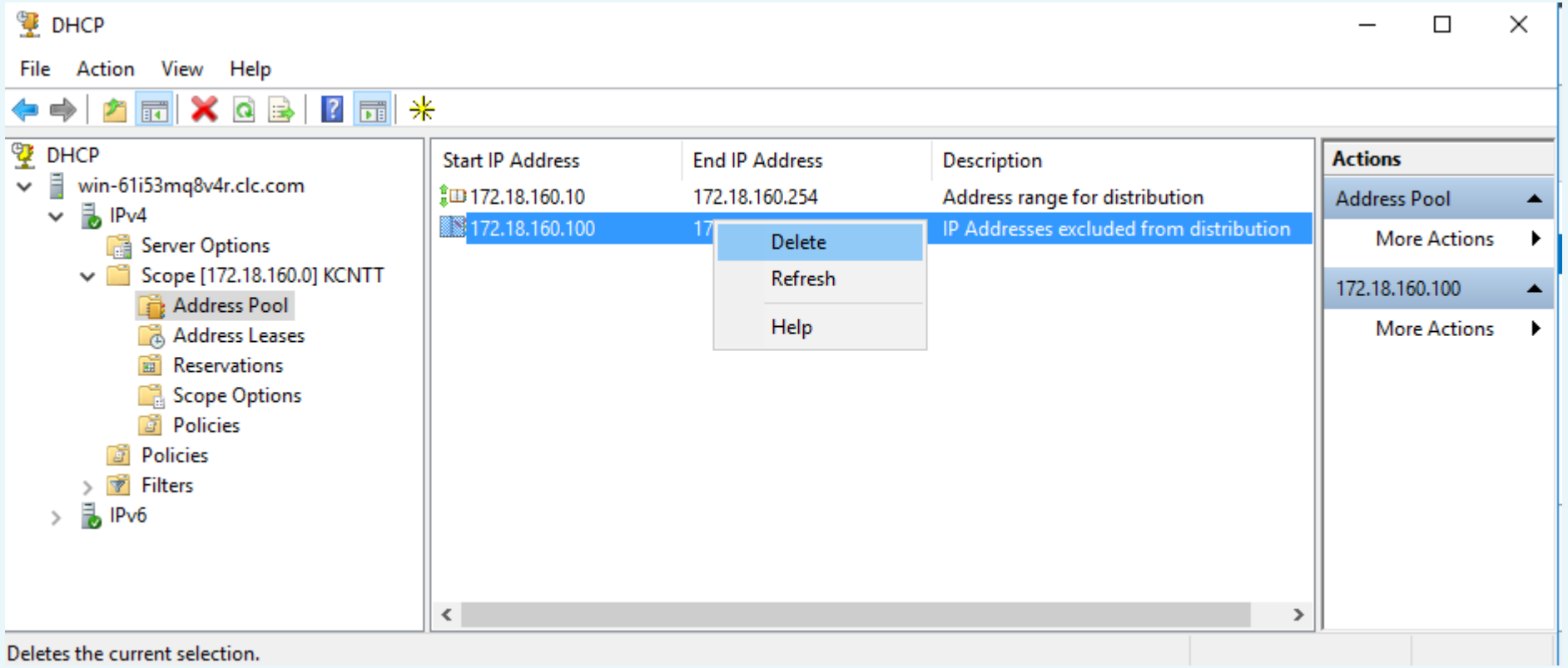




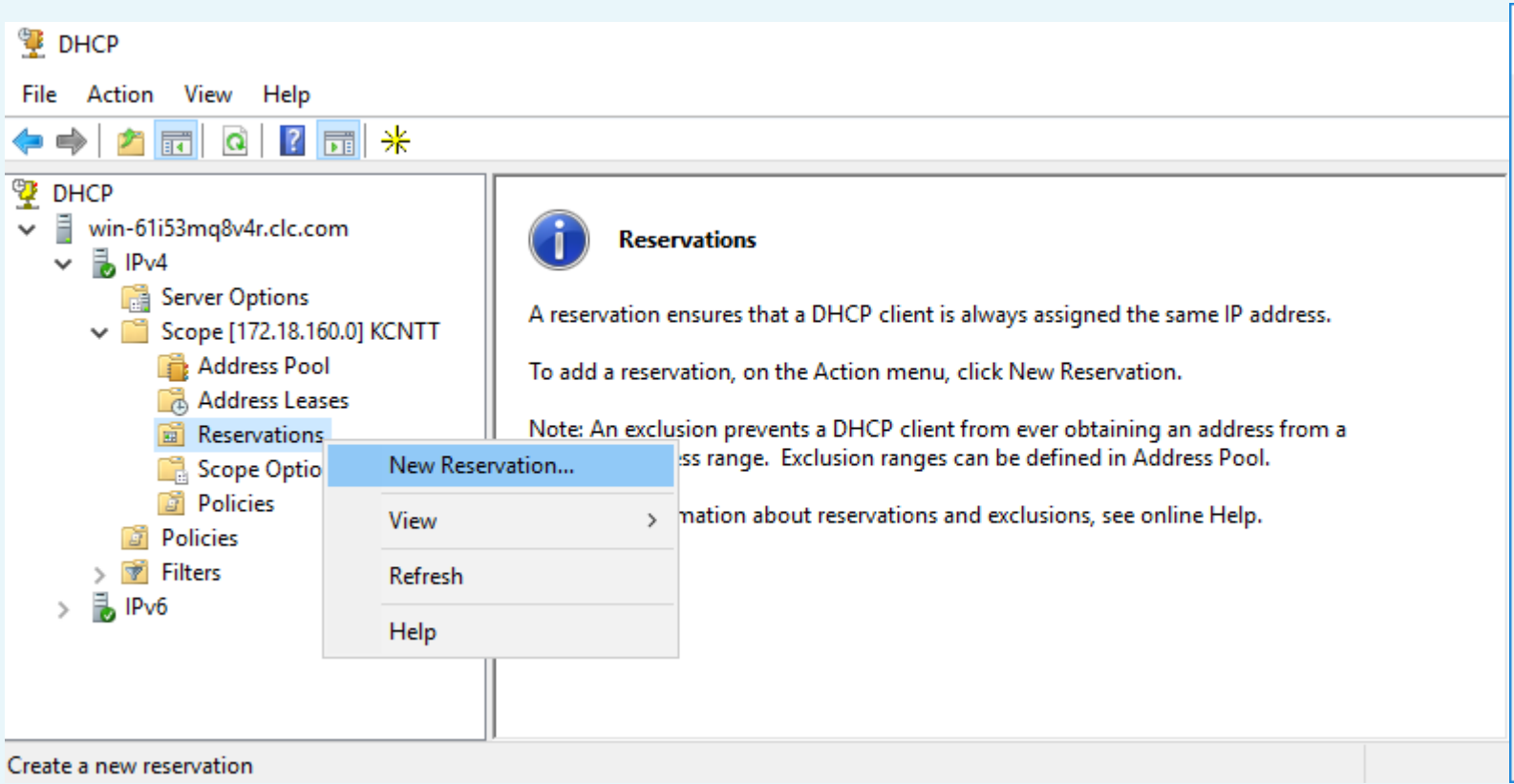
Adding exclusion address range

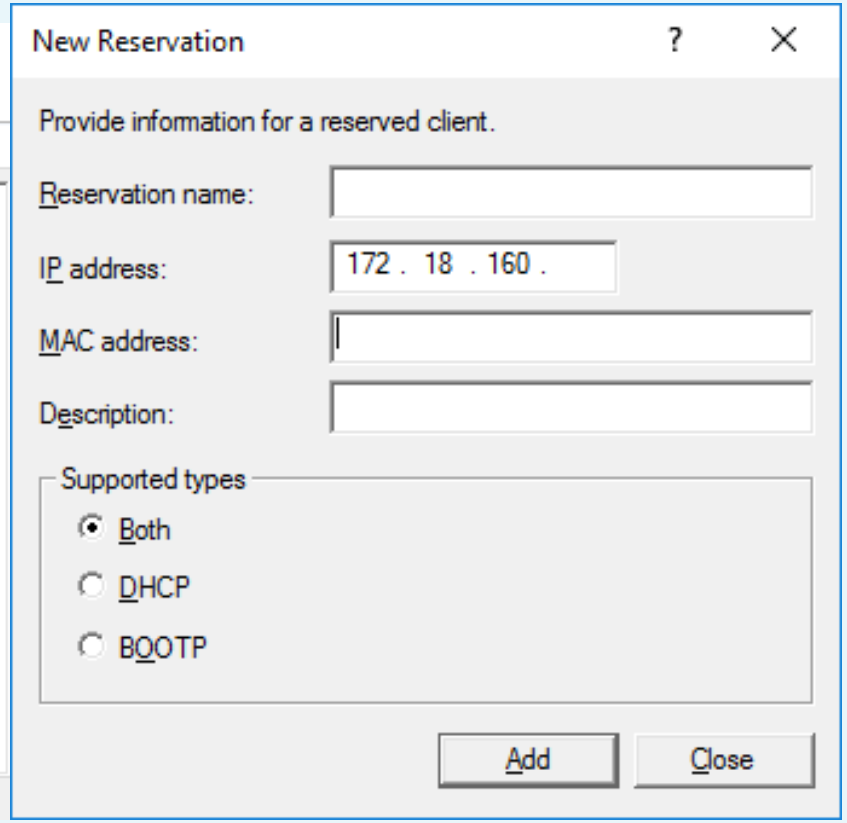


Remove exclusion address range



Add a reservation

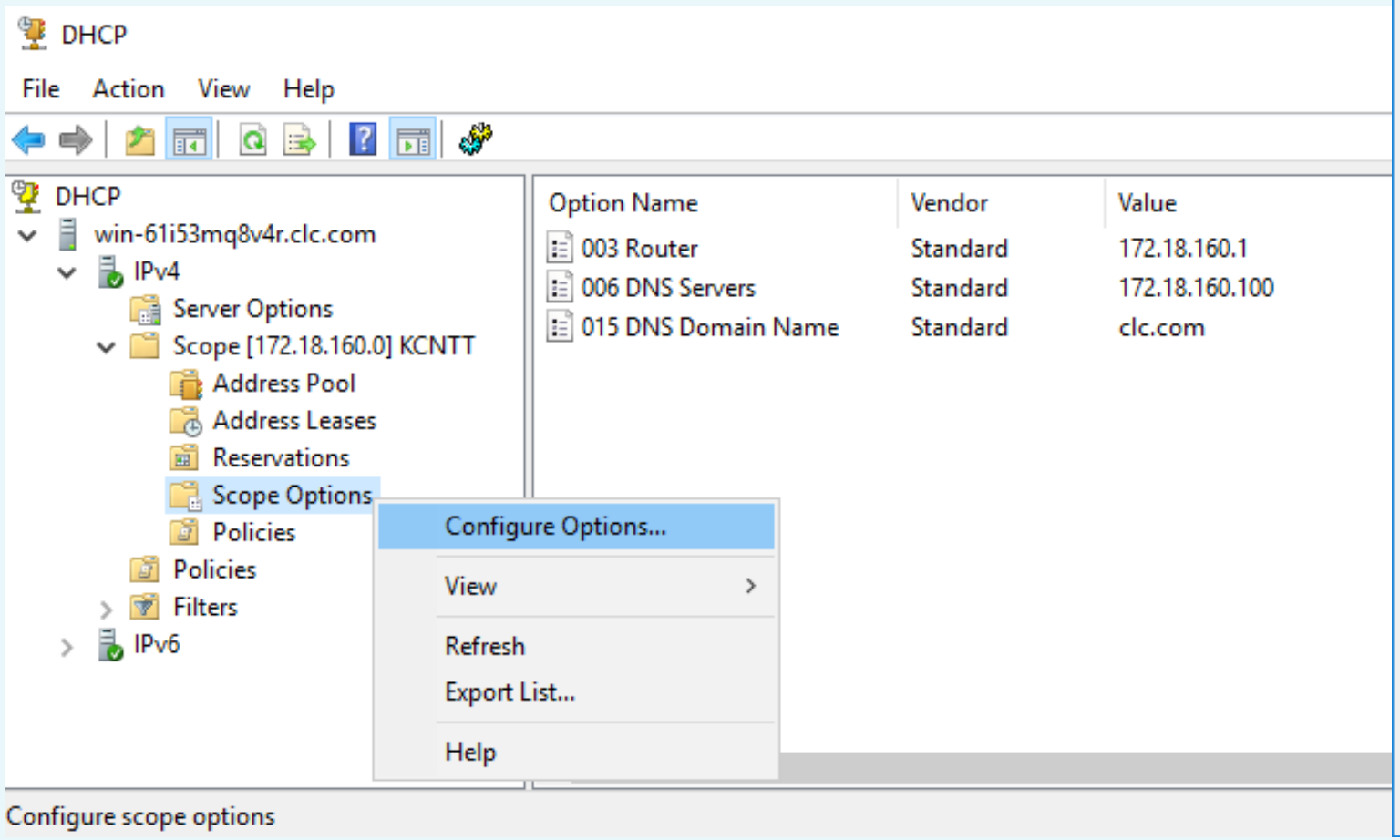


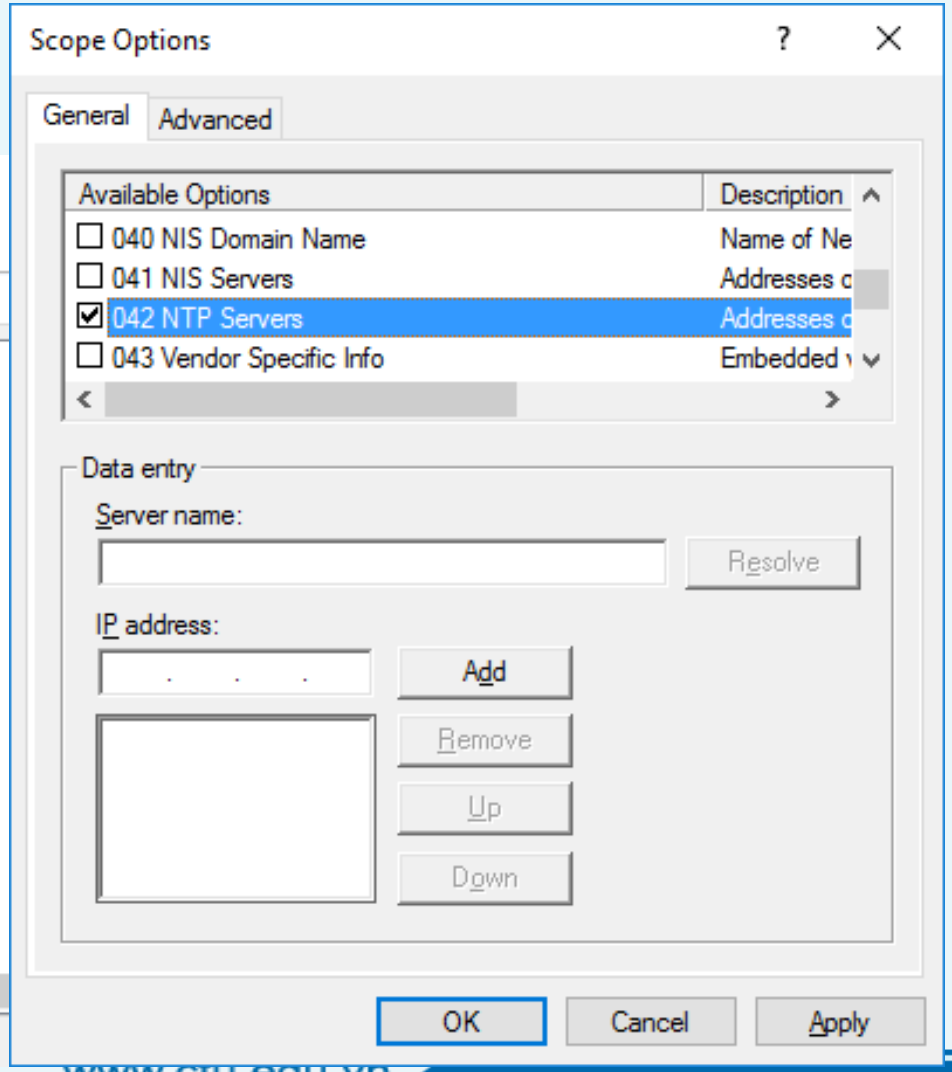


DHCP

Managing DHCP scope

Setting Scope options





DHCP

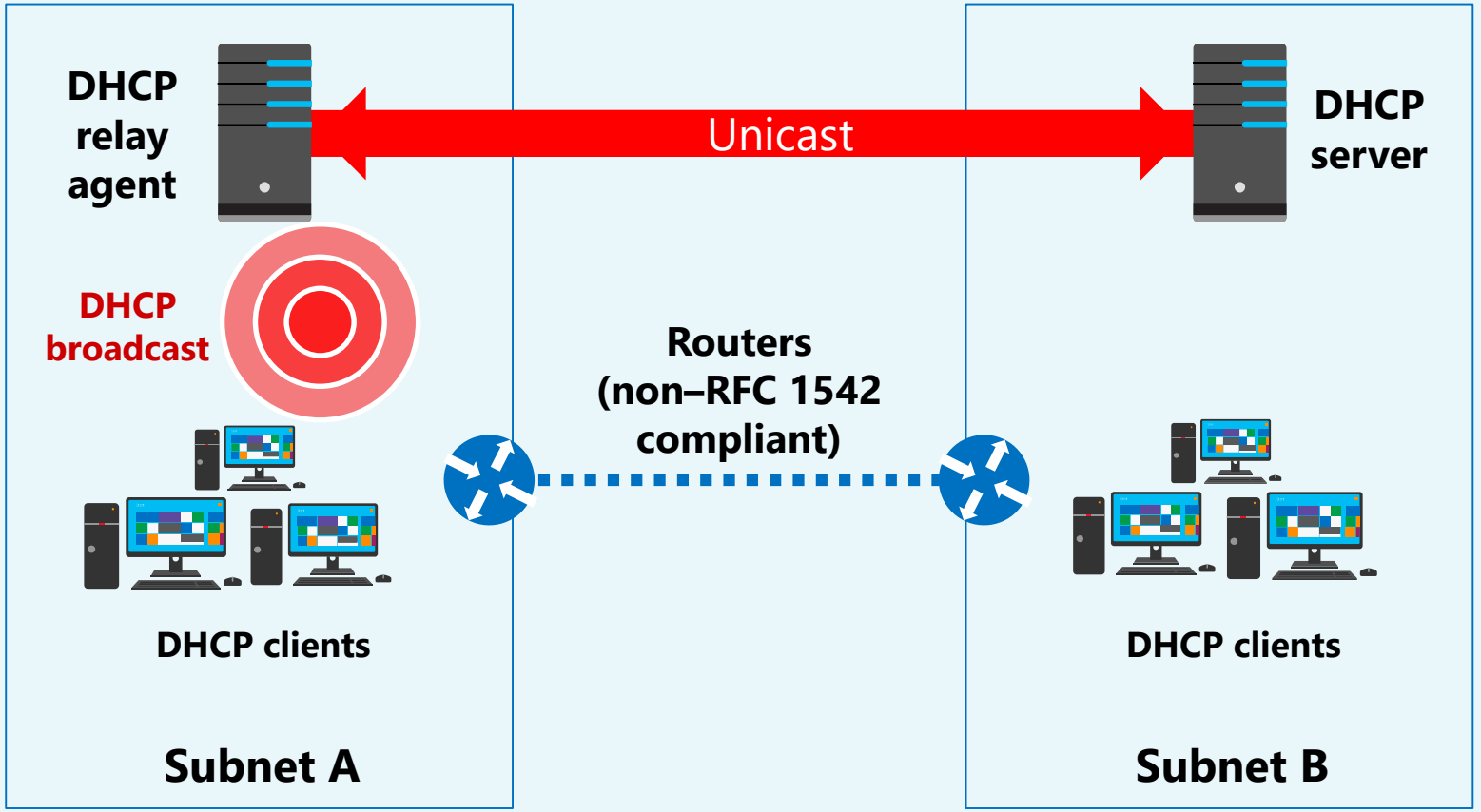
DHCP Relay Agent

- By design, DHCP is intended to work with clients and servers on a single IP network
- When the client and server are on different IP networks:
  - If no DHCP server is available on the client's network: use a DHCP relay agent to forward DHCP broadcasts from the client's network to the DHCP server.
  - The relay agent acts like a repeater: listening for DHCP client requests and retransmitting them through the router to the server.

DHCP

DHCP relay agent

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



CANTHO UNIVERSITY

Summary

- DNS, and DHCP are the core services that underlie and support your entire infrastructure
- DHCP can help your company by issuing all of the TCP/IP settings to your corporate clients
- DNS was designed to be a robust, scalable, and high-performance system for resolving friendly names to TCP/IP host addresses.
- Learned how to install, configure, and manage these necessary services