

Lesson 11: Implementing an Advanced Dynamic Host Configuration Protocol (DHCP) Solution

MOAC 70-412: Configuring Advanced
Windows Server 2012 Services

Overview

- Objective 4.1 – Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution.
 - Create and configure superscopes and multicast scopes
 - Implement DHCPv6
 - Configure high availability for DHCP including DHCP failover and split scopes
 - Configure DHCP Name Protection

Implementing Advanced DHCP Solutions

Lesson 11: Implementing an Advanced Dynamic
Host Configuration Protocol (DHCP) Solution

Dynamic Host Configuration Protocol (DHCP)

- The **Dynamic Host Configuration Protocol (DHCP)** is a network protocol that automatically configures the IP configuration of a device including assigning an IP address, subnet mask, default gateway, and primary and secondary Domain Name System (DNS) servers.
- Most clients and some servers that connect to a network receive their address from a DHCP server including home routers/modems and office networks.
- In addition, the DHCP technology and protocol has become a necessary component of Windows Deployment Services (WDS) and Network Access Protection (NAP).

Dynamic Host Configuration Protocol (DHCP)

- DHCP is based heavily on the **Bootstrap Protocol (BOOTP)**, which was one of the early network protocols used to obtain an IP address from a configuration server.
- Although the DHCP server functions as a BOOTP server, DHCP is a more advanced protocol and includes additional functionality like the ability to reclaim allocated addresses that are no longer used.

Dynamic Host Configuration Protocol (DHCP)

- You can install the DHCP server role on a stand-alone server, a domain member server, or a domain controller.
- These components make up the DHCP technology and protocol:
 - ***DHCP server service***
 - ***DHCP scopes***
 - ***DHCP options***
 - ***DHCP database***
 - ***DHCP console***

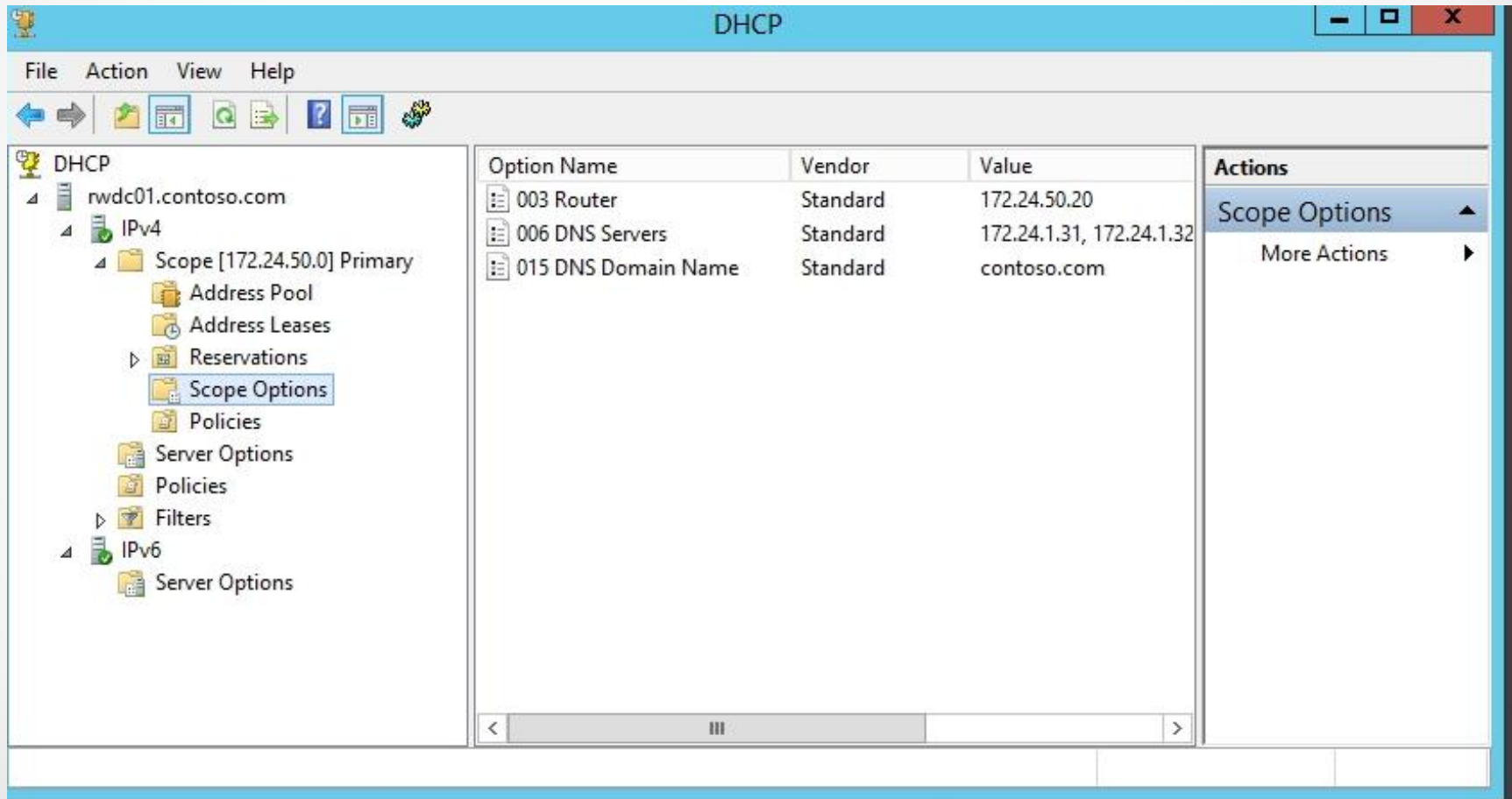
Acquiring and Renewing IP Addresses

- Assuming that a host is configured to use DHCP during startup, the host performs an IP broadcast in its subnet to request IP configuration from any DHCP server that receives the request.
- Because broadcasts are generally restricted to the local subnet, a DHCP server must be on the subnet, or a relay agent or IP helper grabs the broadcast and forwards it directly to a DHCP server on a remote subnet using unicast packets.
- DHCP allocates IP addresses using a lease.
 - The default lease time for a wired client is eight days. When the DHCP lease has reached 50 percent of the lease time, the client attempts to renew the lease.
 - If the DHCP server is down or unreachable, the client will try again from time to time. When the DHCP server comes back up or becomes reachable again, the DHCP client will succeed in contacting it and renewing its lease.

DHCP Options

- DHCP options are not required for use by DHCP.
- Organizations should automatically configure these options so that they do not have to be manually configured:
 - **Option 3 Router**
 - **Option 6 DNS servers**
 - **Option 15 Domain name**
 - **Option 44 WINS/NBNS servers**
 - **Option 46 WINS/NBT node type**

DHCP Options



The screenshot shows the DHCP console window titled "DHCP". The left pane displays a tree view of the DHCP server configuration for "rwdc01.contoso.com". Under the "IPv4" section, the "Scope [172.24.50.0] Primary" is expanded, and "Scope Options" is selected. The main pane displays a table of DHCP options for this scope.

Option Name	Vendor	Value
003 Router	Standard	172.24.50.20
006 DNS Servers	Standard	172.24.1.31, 172.24.1.32
015 DNS Domain Name	Standard	contoso.com

The right pane shows the "Actions" menu with "Scope Options" selected and "More Actions" visible below it.

DHCP and DNS

- By default, the DHCP server dynamically updates the DNS address host (A) resource records and pointer (PTR) resource records only if requested by the DHCP clients.
- By default, the client requests that the DHCP server register the DNS PTR resource record, while the client registers its own DNS A resource record.
- The DHCP server discards the A and PTR resource records when the client's lease is deleted.
- To change how DHCP registers and deletes DNS A and PTR resource records, configure it by right-clicking the IPv4 node or scope, clicking *Properties*, and clicking the *DNS* tab.

Reservations

- **DHCP client reservations** allow administrators to reserve an IP address for permanent use by a DHCP client.
- By using reservations, you can ensure that the host will always have the same IP address.
- As with any other lease, when a client receives a reserved address, the client also receives all assigned options such as addresses of the default gateway and DNS servers. If these options are changed, they will automatically be updated on the client when the lease is renewed.

DHCP Server Authorization

- A rogue DHCP server:
 - Is a DHCP server on a network that is not under the organization's administrative control.
 - Can be used to interrupt network access, bypass network security, and capture private information using a man-in-the-middle attack.
- To protect a network from rogue DHCP servers, if the DHCP server is part of an Active Directory domain, you must authorize the DHCP server before it can hand out IP addresses.
- You must be an Enterprise Admins to authorize the DHCP server.
- If the server is a stand-alone server, Windows will verify whether it is a DHCP server on the network, and it will not start the DHCP service if there is one.

DHCP Policies

- Starting with Windows Server 2012, by using **DHCP policies**, you can give granular control over scopes, which allows you to assign different IP addresses or different options based on the device type or its role.
- Policies are applicable for a specific scope with a defined processing order.
- Options can be configured at the scope or inherited from server-wide policies.

DHCP Policies

- A DHCP policy consists of conditions and settings.
- A condition allows you to identify and group clients based on whether specified criteria is equal or not equal to specified values.
- These criteria include:
 - MAC address
 - Vendor Class
 - User Class
 - Client identifier
 - Relay Agent Information (e.g., remote id, circuit id, and subscriber id)

DHCP Policies

- Every DHCP client request is evaluated against the conditions in a policy.
- If a client request matches the conditions in the policy, the specified settings (IP address and options) assigned to the policy will be applied to the DHCP client.
- A client that does not match conditions is leased an IP address from the remaining scope IP addresses, which are not assigned to a policy, and are given options assigned to the scope.

DHCP Policies

The image shows two overlapping windows from a DHCP management interface. The background window is the 'DHCP Policy Configuration Wizard' with the 'Configure Conditions for the policy' step active. It features a table with columns for 'Conditions', 'Operator', and 'Value', which is currently empty. Below the table are radio buttons for 'AND' and 'OR' (the latter is selected), and buttons for 'Add...', 'Edit...', and 'Remove'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The foreground window is the 'Add/Edit Condition' dialog. It prompts the user to 'Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.' It has dropdown menus for 'Criteria' (set to 'Vendor Class') and 'Operator' (set to 'Equals'). Below is a 'Value(s)' section with a dropdown for 'Value' (set to 'Microsoft Windows 2000 Options'), an 'Add' button, an unchecked 'Append wildcard(*)' checkbox, and a 'Remove' button. At the bottom are 'Ok' and 'Cancel' buttons. A 'Hide' button is visible at the bottom right of the overall interface.

DHCP Policy Configuration Wizard

Configure Conditions for the policy

A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

Conditions	Operator	Value
------------	----------	-------

AND OR

Add... Edit... Remove

< Back Next > Cancel

Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Equals

Value(s)

Value: Microsoft Windows 2000 Options Add

Append wildcard(*)

Remove

Ok Cancel

Hide

DHCP Policies

DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.

Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.

The current scope IP address range is 172.25.21.1 - 172.25.21.254

If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.

Do you want to configure an IP address range for the policy: Yes No

Start IP address:

End IP address:

Percentage of IP address range: No valid range specified

DHCP Policies

- You can configure more than one policy within a scope or server wide.
- When a client makes a DHCP request, each policy is evaluated and the settings are combined. If there is a conflict for a specific option, the policy higher up in processing order overrides the previous option.
- Every policy has an assigned processing order.

Superscopes

- A superscope groups multiple scopes into a single administrative entity. By using superscopes, you can support larger subnets.
- A superscope can be used if a scope runs out of addresses and you cannot add more addresses from the subnet.
- Before creating a superscope:
 - Add a new subnet to the DHCP server.
 - Perform multi-netting, where you lease addresses to clients in the same physical network, but the clients will be in a separate network logically by subnet.
 - Configure routers to recognize the new subnet so that you ensure local communications in the physical network.


Superscopes

- You can only create a superscope if you have two or more IP scopes already created in DHCP.
- You can use the New Superscope Wizard to select the scopes that you want to combine together to create a superscope.

Superscopes

New Superscope Wizard

Select Scopes
You create a superscope by building a collection of scopes.



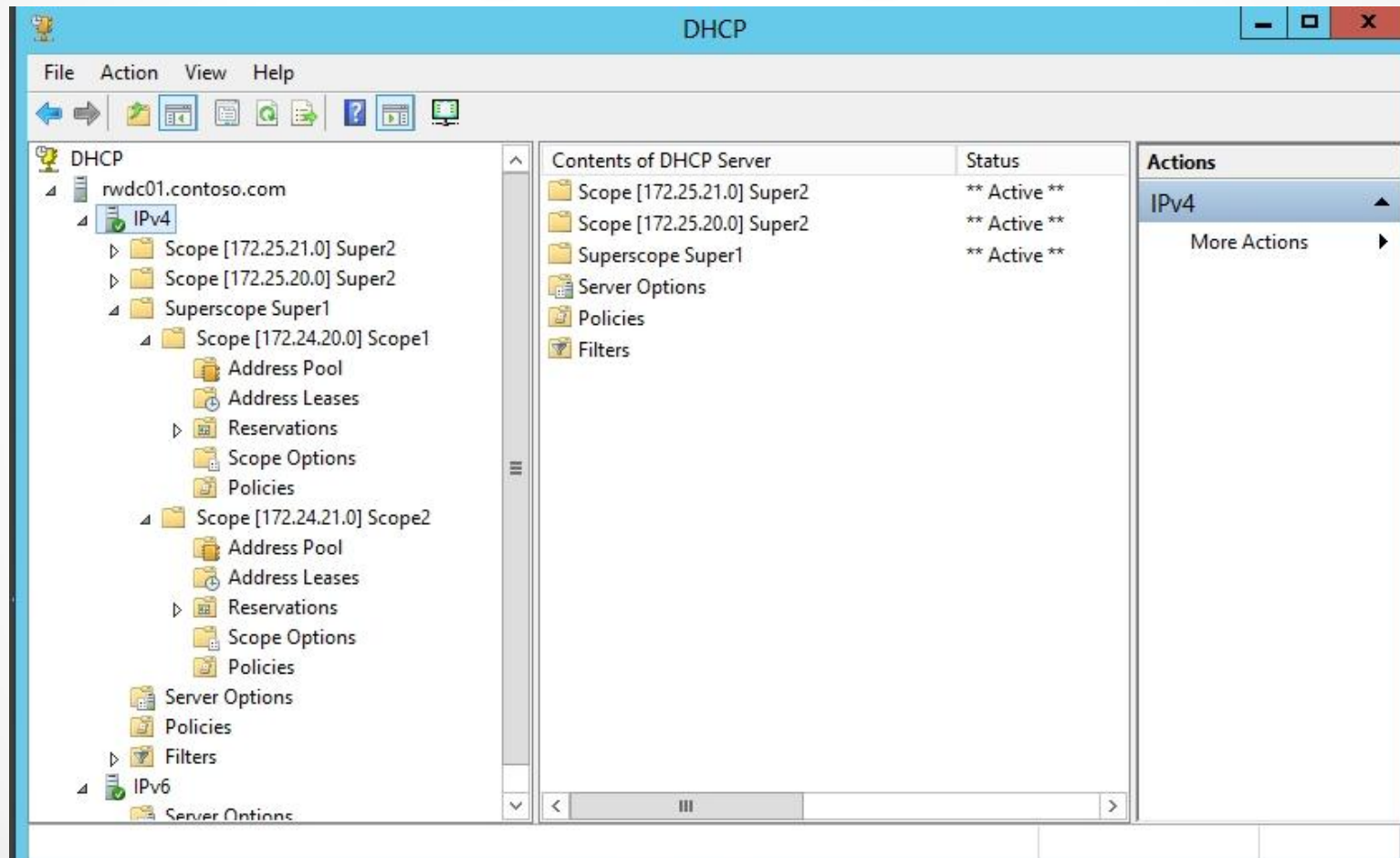
Select one or more scopes from the list to add to the superscope.

Available scopes:

- [172.24.20.0] Scope1
- [172.24.21.0] Scope2

< Back Next > Cancel

Superscopes



Unicast, Broadcast, and Multicast

- **Unicast:** A host sends packets to a single host (single point to single point).
- **Broadcast:** Packets are sent from one host to all other hosts (one point to all other points).
- **Multicast:** Packets are sent from one host to multiple hosts (one point to a set of other points).

Multicast Scopes

- Class D addresses—defined from 224.0.0.0 to 239.255.255.255—are used for multicast addresses.
- In DHCP, **multicast scopes**, commonly known as *Multicast Address Dynamic Client Allocation Protocol (MADCAP) scopes*, allow applications to reserve a multicast IP address for data and content delivery.
- Applications that use multicasting request addresses from the scopes needed to support the MADCAP application programming interface (API).


Multicast Scopes

- Creating and managing a multicast scope is similar to creating and managing a normal scope.
- Multicast scopes cannot use reservations and you cannot set additional options such as DNS and routing.
- Because multicast is shared by groups of computers, the default duration of a multicast scope is 30 days.

Multicast Scopes

New Multicast Scope Wizard

IP Address Range
You set the range of IP addresses that define this multicast scope.



The valid IP address range is 224.0.0.0 to 239.255.255.255.

Start IP address:

End IP address:

Time to Live (TTL) is the number of routers that multicast traffic passes through on your network.

TTL:

DHCPv6 Addresses

- **IPv6 addresses** utilize a 128-bit address space to provide addressing for every device on the Internet with a globally unique address.
- Because IPv6 addresses use 128 bits, the addresses are usually divided into groups of 16 bits, written as 4 hex digits. Hex digits include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. Colons separate the groups.
- This is an example of an IPv6 address:

FE80:0000:0000:0000:02C3:B2DF:FEA5:E4F1

DHCPv6 Addresses

- Like IPv4 addresses, IPv6 addresses are divided into network bits and host addresses.
- IPv6 supports automatic configuration. However, with a Windows DHCP server, you can perform stateful address autoconfiguration.

DHCPv6 Addresses

- The first 64 bits of an IPv6 address define the network address, and the second 64 bits define the host address.
- In the previous example address, FE80:0000:0000:0000 defines the network bits and 02C3:B2DF:FEA5:E4F1 defines the host bits.
- The network bits are also further divided where 48 bits are used for the network prefix and the next 16 bits are used for subnetting. The remaining host bits are 64 bits.

IPv6 Addressing

- With IPv6, unicast addressing can be divided into the following:
 - **Global unicast addresses:** Public addresses, globally routable and reachable on the IPv6 portion of the Internet.
 - **Link-local addresses:** Private non-routable addresses, confined to a single subnet and used to communicate with neighboring hosts on the same link.
 - Equivalent to Automatic Private IP addresses (169.254.x.x) used by IPv4 when a DHCP server cannot be contacted.
 - Used to set up permanent small LANs.
 - Also used to create temporary networks or ad-hoc networks.
 - Routers process packets sent to link-local addresses but do not forward the packets to other links.
 - **Unique local addresses:** Intended private addressing, used to join two subnets together without creating any addressing problems.

IPv6 Addressing

- IPv6 host addresses can be configured with stateful or stateless mode.
- Because the two address configuration modes are independent of each other and will not trample over each other, a host can use both stateless and stateful address configuration.

Stateless Mechanism

- Stateless mechanism is used to configure both link-local addresses and additional non-link-local addresses based on Router Solicitation and Router Advertisement messages with neighboring routers.
 - With stateless autoconfiguration, the MAC address is used to generate the host bits.
 - When using stateless configuration, the address is not assigned by a DHCP server.
 - However, a DHCP server can still assign other IPv6 configuration settings.
- Stateful configuration has IPv6 addresses and additional IPv6 configuration assigned by a DHCPv6 server.

IPv6 Scopes

- When creating IPv6 scopes, you define the following properties:
 - **Prefix**
 - **Preference**
 - **Exclusions**
 - **Valid and preferred lifetimes**
 - **DHCP options**

IPv6 Scopes

New Scope Wizard

Scope Prefix
You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.

Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.

Prefix /64

Preference

< Back Next > Cancel

IPv6 Scope Options

- 00021 SIP Server Domain Name List
- 00022 SIP Servers IPv6 Address List
- 00023 DNS Recursive Name Server IPv6 Address
- 00024 Domain Search List
- 00027 NIS IPv6 Address List
- 00028 NIS + IPv6 Address List
- 00029 NIS Domain List
- 00030 NIS + Domain Name List
- 00031 SNTP Servers IPv6 Address List

High Availability for DHCP

- To make DHCP highly available, you can use one of the following methods:
 - ***Split scopes***
 - **Server cluster**
 - ***DHCP failover***
 - **Standby server**


Configuring Split Scopes

- For years, if you wanted high availability, you would use a split-scope configuration:
 - Also known as *80/20 configuration*
 - Uses two DHCP servers with the same scopes and options
- However, the scopes have complementary exclusion ranges, so there is no overlap in the addresses that they lease to clients. You do not want the two servers to hand out the same address to different clients.

80/20 Split


Dhcp Split-Scope Configuration Wizard

Percentage of Split
Select the percentage of IP addresses that will be allocated to each of the split-scope servers.



Scroll the slider to choose the percentage of split of IPv4 address range of this scope:

172.25.20.50 172.25.20.254



Percentage of IPv4 Addresses

	Host DHCP Server	Added DHCP Server
Percentage of IPv4 Addresses Served:	<input type="text" value="80"/>	<input type="text" value="20"/>

Following is the Exclusion IPv4 Address Range:

Start IPv4 Address:	<input type="text" value="172 . 25 . 20 . 214"/>	<input type="text" value="172 . 25 . 20 . 50"/>
End IPv4 Address:	<input type="text" value="172 . 25 . 20 . 254"/>	<input type="text" value="172 . 25 . 20 . 213"/>

Note: The existing exclusions will also be configured appropriately on the DHCP Servers.

80/20 Split

Dhcp Split-Scope Configuration Wizard

Delay in DHCP Offer
Specify the delay (in milli seconds) with which the added DHCP server distributes addresses.

Delay in DHCP Offer (milli seconds):

Host DHCP Server:	Added DHCP Server:
<input type="text" value="0"/>	<input type="text" value="0"/>

< Back Next > Cancel

DHCP Failover

- Starting with Windows Server 2012, DHCP can replicate lease information between two DHCP servers for IPv4 scopes and subnets.
- If one DHCP server fails or becomes overloaded, the other server services the clients for the entire subnet.
- DHCP failover establishes a failover relationship between the two DHCP servers.
- Each relationship has a unique name, which is exchanged during configuration.
- A single DHCP server can have multiple failover relationships with other DHCP servers as long as each relationship has a unique name.

DHCP Failover

- DHCP failover supports two modes:
 - **Load Sharing:** Both servers simultaneously supply IP configuration to clients. By default, the load is distributed evenly, 50:50. However, you can adjust the ratio if you prefer one server over another. Load Sharing is the default mode.
 - **Hot Standby:** One server is the primary server that actively assigns IP configuration for the scope or subnet, and the other is the secondary server that assumes the DHCP role if the primary server becomes unavailable. Hot Standby mode is best suited when the disaster recovery site is located at a different location.

DHCP Name Protection

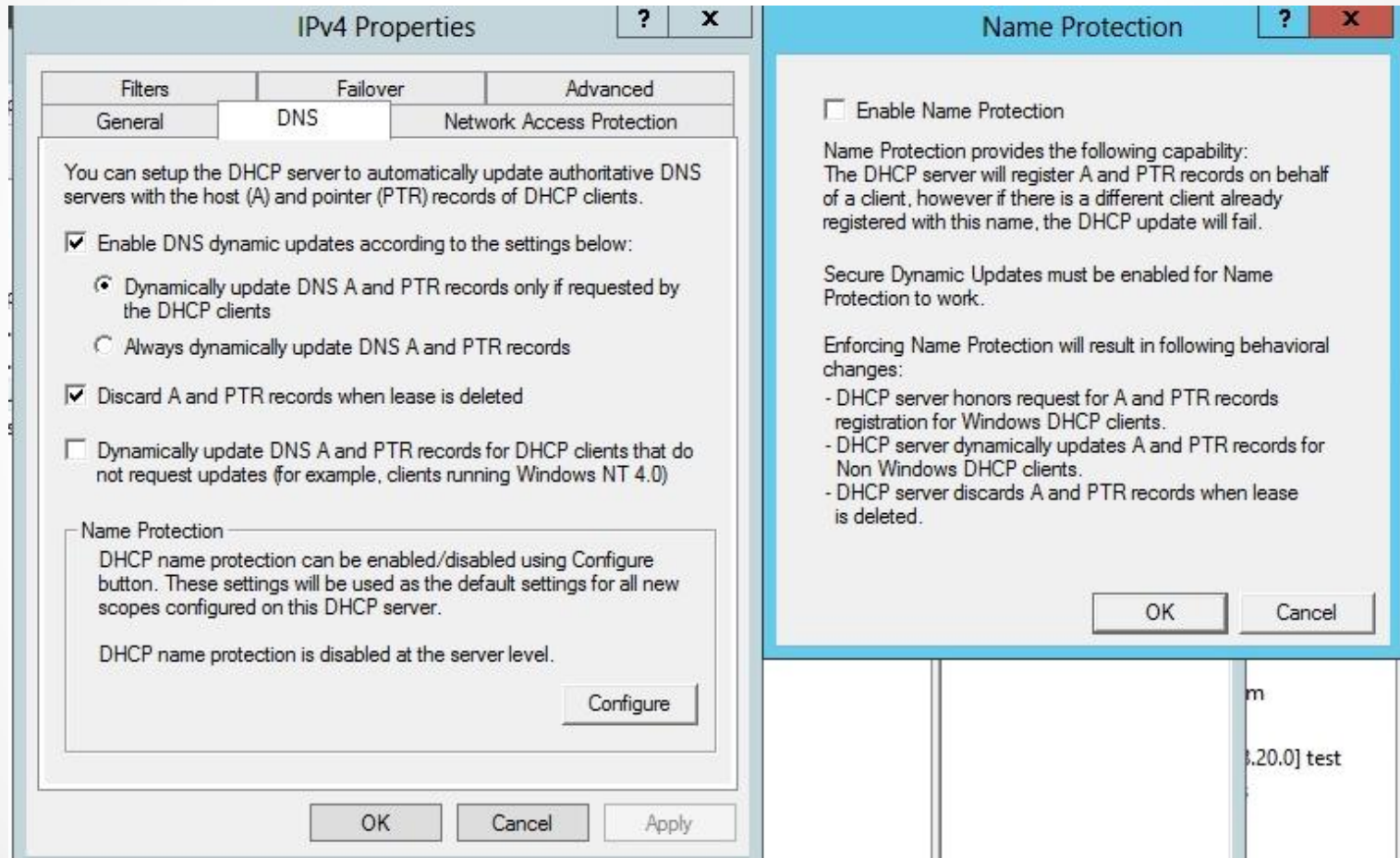
- If an organization uses only Windows systems that are part of an Active Directory domain, each computer will have its own unique computer name, which DHCP registers in DNS on behalf of the client.
- Name squatting is when a non-Windows-based computer registers a name in DNS that is already registered to a Windows-based computer.
- To prevent conflicts when non-Microsoft systems overwrite systems that use static addresses, Windows Server 2012 introduced **DHCP Name Protection**.

DHCP Name Protection

DHCP Name Protection:

- Can be used for both IPv4 and IPv6.
- Can be configured at the server level or at the scope level.
- When configured at the server level, it applies only to newly created scopes.

DHCP Name Protection



Lesson Summary

- The Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically configures the IP configuration of a device including assigning an IP address, subnet mask, default gateway, and primary and secondary DNS servers.
- A superscope groups multiple scopes into a single administrative entity. By using superscopes, you can support larger subnets.
- Multicast is when one host sends packets to multiple hosts (one point to a set of other points). Multicasting delivers the same packet simultaneously to a group of clients, which results in less bandwidth usage.

Lesson Summary

- In DHCP, multicast scopes, commonly known as *Multicast Address Dynamic Client Allocation Protocol (MADCAP)* scopes, allow applications to reserve a multicast IP address for data and content delivery.
- IPv6 addresses utilize a 128-bit address space to provide addressing for every device on the Internet with a globally unique address.
- Stateless mechanism is used to configure both link-local addresses and additional non-link-local addresses based on Router Solicitation and Router Advertisement messages with neighboring routers.
- Stateful configuration has IPv6 addresses and additional IPv6 configuration assigned by a DHCPv6 server.

Lesson Summary

- DHCP is an essential service that allows most clients and some servers to communicate on the network. As clients are turned on, or when a client renews a lease, the DHCP server must be available to assign or renew the lease.
- Split-scope configuration uses two DHCP servers with the same scopes and options. However, the scopes have complementary exclusion ranges, so that there is no overlap in the addresses that they lease to clients. You do not want the two servers to hand out the same address to different clients.
- Split-scope configuration is known as *80/20 configuration* because the primary server is assigned 80 percent of available addresses, whereas the secondary server is assigned 20 percent.

Lesson Summary

- Starting with Windows Server 2012, DHCP can replicate lease information between two DHCP servers for IPv4 scopes and subnets. If one DHCP server fails or becomes overloaded, the other server services the clients for the entire subnet.
- To prevent conflicts when non-Microsoft systems overwrite systems that use static addresses, Windows Server 2012 introduced DHCP Name Protection.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.