# **Module 8**

**Configuring and Managing Network Services**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

This module gives your students a foundation for understanding both the Domain Name System and the Dynamic Host Configuration Protocol. They learn how to install, configure, use, and troubleshoot these services for automated IP communications. They also learn how to configure a WINS server to provide for NetBIOS name resolution. At the end of the module, students learn some basic DHCP troubleshooting techniques by reviewing common problems related to DHCP and possible solutions.

# **Module Objectives**

* Describe the process used to resolve FQDNs using DNS
* Configure a DNS server
* Troubleshoot common DNS issues
* Configure a WINS server to provide for NetBIOS name resolution
* Describe the process used to obtain IP configuration using DHCP
* Configure a DHCP server
* Troubleshoot common DHCP issues

# **Teaching Tips**

**Understanding DNS**

1. Remind students that DNS is a hierarchical namespace used to identify computers on large IP networks such as the Internet.
2. Define a zone as one part of the namespace.
3. Note that DNS servers have resource records that contain the FQDN and IP information for computers in a zone.
4. Mention that DNS servers typically resolve FQDNs to IP addresses (called a forward lookup), but they can also be configured to resolve IP addresses to FQDNs (called a reverse lookup).

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Mention that before a computer performs forward lookups using DNS servers, it first checks for a line in the hosts file that can be used to resolve the FQDN to an IP address. The default hosts file on Windows systems is C:\Windows\system32\drivers\etc\hosts, and the comments at the top of this file provide examples that an administrator can follow to create entries for hosts on a network. |

**The DNS Lookup Process**

1. Mention that when an administrator contacts a Web server on the Internet using a Web browser from a home or public network, the Web browser performs a forward lookup of the FQDN, which in turn allows it to contact the IP address of the Web server.
2. Note that this forward lookup can be performed by a single DNS server or a series of DNS servers.
3. Refer to Figure 8-1. Explain each step illustrated in the DNS lookup process that takes place from a home or public network.
4. Mention that in the DNS lookup process described in Figure 8-1, the client computer is called the resolver. Distinguish between an iterative query and a recursive query.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | All DNS servers contain a root hints file that contains the IP addresses of DNS servers that hold top-level DNS zones. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | The amount of time that a computer is able to cache the result of a lookup is determined by the Time To Live (TTL) property of the resource record. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | A DNS server that contains resource records for one or more zones is said to be authoritative for those zones. For example, the microsoft.com DNS server in Figure 8-1 is authoritative for the microsoft.com zone. |

1. Explain why the process illustrated in Figure 8-1 is different when a client computer in an organization is used to resolve *docs.microsoft.com*. Emphasize that it has to do with the fact that organizations often deploy their own DNS servers that host zones needed for Active Directory.
2. Note that in this case, organization DNS servers are called default forwarders, as they forward requests they cannot resolve to other DNS servers instead of using root hints to perform recursive queries.
3. Refer to Figure 8-2. Explain the steps illustrated in the figure, which describes the typical process used to resolve the FQDN *docs.microsoft.com* from a computer in an organization.

**Authoritative DNS Server Types**

1. Introduce this topic by mentioning that each zone typically has more than one authoritative DNS server to ensure that names can be resolved if one server is unavailable.
2. Define a primary DNS server as the first DNS server in a zone. Explain that it contains a read-write copy of a zone file that stores resource records for the zone.
3. Mention that additional DNS servers are called secondary DNS servers, and contain a read-only copy of the zone file from the primary DNS server that they can use to respond to DNS lookup requests.
4. Explain the zone transfer process, noting that new resource records are added to the primary DNS server, and secondary DNS servers periodically copy the new records from the primary DNS server in the process.
5. Point out that if the organization DNS server is also a domain controller, zone files can be stored in the Active Directory database and replicated to other domain controllers that are also configured as DNS servers.
6. Mention that in this case, each DNS server is called an Active Directory-integrated primary DNS server and contains a read-write copy of the zone file in its Active Directory database.
7. Explain how new resource records added to an Active Directory-integrated primary DNS server are replicated.

**Accessing DNS Servers in Other Organizations**

1. Introduce this topic by mentioning that when an Active Directory domain is implemented, most organizations choose to use a domain name that is not registered with the top-level DNS servers on the Internet.
2. Explain why this is considered to be a secure practice.
3. Mention that there are times when one organization may need to resolve FQDNs for another organization’s Active Directory zone, and vice versa.
4. Describe one method where an administrator can configure the existing organization DNS servers in each organization as conditional forwarders that relay forward lookups for the other organization’s zone directly to one or more DNS servers in the other organization.
5. Describe a second method where an administrator can configure the DNS servers in each organization as stub DNS servers for the other organization’s zone. Note that as with conditional forwarders, a stub DNS server forwards requests for a target organization’s zone directly to a DNS server in the target organization.

**Resource Records**

1. Introduce this topic by mentioning that resource records hold information about a service, FQDN, IP address, or zone on an authoritative DNS server.
2. Point out that DNS lookups request information contained in specific resource record types.
3. Refer to Table 8-1 and review the most common types of resource records.
4. Emphasize that host records (A and AAAA) are the most common resource record types configured on a DNS server, as they provide for forward lookups. Explain how they are created.
5. Note that the dynamic update feature of DNS is also used by domain controllers to automatically create the SRV records that computers use to locate Active Directory services.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | The dynamic update feature of DNS is also called dynamic DNS (DDNS). |

1. Explain how host records can be used to perform load balancing of services on the network using a feature of DNS called round robin. Explain what happens if two identically configured Web servers have IP addresses on different networks. Mention that netmask ordering takes precedence over round robin.

**Configuring a DNS Server**

1. Emphasize that to configure a Windows Server 2019 computer as a DNS server, an administrator must install and configure the DNS Server role.
2. Note that this server role functions as a caching-only DNS server that uses root hints and cached entries to respond to lookup requests on all network interfaces.
3. Explain that an administrator can create forward and reverse lookup zones on the DNS server to provide authoritative responses for lookup requests. Note that if lookup requests cannot be resolved using the zones configured on the server, the DNS server will use its root hints to perform a recursive query.
4. Mention that an administrator can configure the DNS server as a default forwarder to relay lookup requests that cannot be resolved to another DNS server, instead of using root hints. Point out that to forward lookup requests to another organization’s DNS server that is not publicly registered with top-level DNS servers, an administrator can choose to configure either a conditional forwarder or stub zone.
5. Explain what happens if the DNS Server role was installed by the Active Directory Domain Services role on a new domain controller.
6. Refer to Figure 8-3. Explain that regardless of how the DNS Server role was installed, an administrator can manage a DNS server by clicking DNS from the Tools menu in Server Manager to start the DNS Manager tool. Discuss the examples provided in Figure 8-3. Be sure to review the forward lookup zone, the records, the folders, the DNS server, etc.

**Configuring Primary Zones**

1. Introduce this topic by mentioning that an administrator can create an unlimited number of primary forward and reverse lookup zones on a DNS server to hold resource records that are authoritative for a zone in the Domain Name Space.
2. Note that an administrator can configure each zone to either: (1) allow for dynamic updates; or (2) require that resource records be manually created by the server administrator.
3. Point out that if the DNS server is also a domain controller, an administrator can also configure the zone file to be stored in Active Directory. After the administrator creates a primary lookup zone, he or she can access the properties of the zone to modify the zone configuration.
4. Refer to Figure 8-3 and Figure 8-4 through Figure 8-8. Explain how to create a primary forward lookup zone.
5. Refer to Figure 8-3 through Figure 8-5 and Figure 8-8 through Figure 8-11. Explain how to create a primary reverse lookup zone.
6. Refer to Figure 8-12 through Figure 8-15. Explain how to manually create resource records in a zone.
7. Refer to Figure 8-16 through Figure 8-22. Explain how to configure zone properties.

**Creating Secondary Zones**

1. Introduce this topic by mentioning that after zone transfers have been allowed to a DNS server in the properties of a primary forward or reverse lookup zone, an administrator can create an associated secondary zone on the DNS server.
2. Refer to Figure 8-3 and explain how to start the New Zone Wizard.
3. Refer to Figure 8-4 and explain how to select *Secondary zone* as the zone type. Point out that this will deselect *Store the zone in Active Directory* as secondary zones cannot be Active Directory-integrated.
4. Refer to Figure 8-6 and to illustrate the prompt for the zone name.
5. Refer to Figure 8-23 to illustrate the prompt to specify the IP address of the DNS server that hosts the primary zone. Note that after an administrator clicks Next in Figure 8-23, he or she will click Finish to create the secondary zone.

**Creating Stub Zones**

1. Introduce this topic by explaining that unlike primary and secondary zones, stub zones are not authoritative. Note that they instead contain NS and host records that allow a DNS server to access an authoritative zone on another DNS server.
2. Refer to Figure 8-3 and explain how to start the New Zone Wizard.
3. Refer to Figure 8-4 and explain how to select Stub zone as the zone type.
4. Note that if an administrator chooses to create an Active Directory-integrated stub zone and clicks Next, an administrator is prompted to select Active Directory-integrated zone replication options, as shown in Figure 8-5.
5. Refer to Figure 8-6 and explain how to choose the name of the zone hosted by the target DNS server.
6. Refer to Figure 8-11 and explain how to choose zone file options if an Active Directory-integrated primary zone type was not selected.
7. Refer to Figure 8-24 and explain how to specify the IP address of a DNS server that is authoritative for the zone.

**Configuring Conditional Forwarders**

1. Introduce this topic by mentioning that conditional forwarders are an alternative to stub zones that provide the same functionality. Point out that rather than being displayed as an additional forward lookup zone in DNS Manager, conditional forwarders are stored in their own folder. Emphasize that as a result, server administrators often prefer to create conditional forwarders over stub zones on DNS servers that host many forward lookup zones.
2. Explain that to create a conditional forwarder, one must right-click the Conditional Forwarders folder shown earlier in Figure 8-3 and click New Conditional Forwarder to open the New Conditional Forwarder window shown in Figure 8-25.
3. Explain that in this example, the options shown in Figure 8-25 will create an Active Directory-integrated conditional forwarder that relays forward lookup requests for the lala.com zone to the DNS server with IP address 4.99.192.1.

**Configuring Default Forwarders**

1. Introduce this section by mentioning that for lookup requests that do not match an authoritative zone or conditional forwarder, DNS servers will use root hints to perform a recursive query in order to resolve the lookup request.
2. Note that this can result in a large number of recursive lookup requests in organizations that have many DNS servers. Emphasize that as a result, most organizations will instead configure their DNS servers as default forwarders that relay lookup requests that cannot be resolved to an ISP DNS server or other DNS server in the organization.
3. Explain that to configure SERVERX shown earlier in Figure 8-3 as a default forwarder, right-click SERVERX, click Properties, and highlight the Forwarders tab as shown in Figure 8-26.
4. Explain that the options shown in Figure 8-26 will forward requests to the DNS server with IP address 192.168.1.1 or the DNS server with IP address 192.168.1.2 if the first DNS server is unavailable. Explain that if both DNS servers are unavailable, root hints are used to perform a recursive query.

**Quick Quiz 1**

1. All DNS servers contain a \_\_\_\_\_\_\_\_\_\_ file that contains the IP addresses of DNS servers that hold top-level DNS zones.
2. root hosts
3. root hints
4. container
5. top level

Answer: b. root hints

1. True or False: The amount of time that a computer is able to cache the result of a lookup is determined by the Time To Live (TTL) property of the resource record.

Answer: True

1. A DNS server that contains resource records for one or more zones is said to be \_\_\_\_\_\_\_\_\_\_ for those zones.
   1. recursive
   2. iterative
   3. authoritative
   4. integrated

Answer: c. authoritative

1. True or False: A stub DNS server forwards requests for a target organization’s zone directly to a DNS server in the target organization.

Answer: True

**Troubleshooting DNS**

1. Open this section by mentioning that by resolving FQDNs to IP addresses, DNS provides one of the most important services on a network. Point out that if a DNS server is unable to perform forward lookups, computers will be unable to contact the services running on other systems on the network or Internet.
2. Note that in many cases, an administrator can solve DNS server-related problems by restarting the DNS Server service on the DNS server. Explain how to restart the DNS Server service.
3. Mention that many DNS-related problems are caused by missing or misconfigured resource records. Explain how to manually run the dynamic update process on the DNS client to attempt to resolve the issue.
4. Mention that missing resource records in a secondary zone are often caused by zone transfer issues. Note that zone transfers may not occur successfully if the network bandwidth is saturated at the time the zone transfer is initiated. Explain how to remedy this by performing a zone transfer manually.
5. Mention that DNS-related problems can also be caused by an invalid entry in the DNS cache. Remind students that both the DNS server and resolver cache the result of a DNS lookup request for the time specified in the TTL of the cached record. If a resource record is modified, any DNS servers and resolvers that performed a lookup request will have invalid information in their DNS cache until the TTL expires. Explain how to resolve this by clearing the entries in the DNS cache to ensure that the correct information is obtained using a DNS lookup.
6. Summarize this topic by mentioning that restarting the DNS Server service, manually performing a dynamic update or zone transfer, and clearing DNS caches are common solutions to many DNS-related problems.
7. Emphasize that they do not work in all situations.
8. Mention that an administrator should troubleshoot each DNS issue based on the information that he or she can obtain regarding the problem. Moreover, there are several tools that can help an administrator troubleshoot DNS-related problems, including the nslookup command, DNS manager, and DNS logs.

**Using nslookup**

1. Mention that when troubleshooting most DNS-related problems, the first step typically involves testing forward lookups from a resolver using the nslookup command at a Command Prompt or Windows PowerShell window.
2. Explain that the nslookup command can perform both forward and reverse lookups and will list the DNS server that is used to perform the lookup, as well as identify whether the result was authoritative (obtained from a zone file on the DNS server) or non-authoritative (obtained from the DNS server cache).
3. Refer to Figure 8-27 as an example of using the nslookup command.
4. Explain that the output of nslookup provides information that an administrator can use to determine the nature of the problem and possible solutions.
5. Refer to Table 8-2 and review some common solutions to problems identified by nslookup.

**Using DNS Manager**

1. Introduce this topic by explaining that to test whether a DNS server is functioning correctly, one can access the Monitoring tab of DNS server properties in DNS Manager.
2. Explain that if an administrator right-clicks SERVERX in Figure 8-3, clicks Properties, and highlights the Monitoring tab, the administrator is able to perform a simple or recursive test, as shown in Figure 8-28.
3. Refer to Figure 8-28 again and review the other options an administrator can select.
4. Review some of the solutions for the different types of failures.

* If a simple query test fails, there is likely a misconfigured zone on the DNS server or the DNS Server service needs to be restarted.
* If a recursive query test fails, the organization firewall may be blocking DNS requests to the top-level DNS servers.
* If the firewall is not blocking these requests, then the root hints file on the DNS server may have become corrupted. Explain that because every DNS server uses the same root hints file, an administrator can copy the root hints file from another DNS server in the organization to fix the issue. Explain how to do this by highlighting the Root Hints tab in Figure 8-28, clicking Copy from Server, and specifying another DNS server on the network.

**Using Log Files**

1. Introduce this topic by mentioning that log files are often used to troubleshoot unusual DNS problems that cannot be resolved using other methods.
2. Point out that by default, the DNS Service logs all information to the DNS Server log. Explain how to view the entries in this log.
3. Mention that if the information in the DNS Server log is not sufficient to locate a solution to the problem, an administrator can enable debug logging to obtain more detailed information.
4. Explain that debug logging allows an administrator to record packet-by-packet information about the queries that the DNS server receives.
5. Refer to Figure 8-3 to illustrate how to select a server. Refer to Figure 8-29 and explain how to enable debug logging on the selected DNS server.
6. Emphasize that because debug logging records a large amount of information in the log file that specified in Figure 8-28, an administrator should only enable it when troubleshooting a DNS-related issue and only for a short period of time.

**Configuring WINS**

1. Remind students that each Windows system contains a NetBIOS name that is generated from the first 15 characters of the computer name. Mention that NetBIOS is a legacy protocol that has been used in Microsoft operating systems since 1985 to identify computers on a network.
2. Point out that while FQDNs are the preferred method for identifying computers on networks today, modern Microsoft operating systems such as Windows 10 and Windows Server 2019 still use NetBIOS to identify systems on a network, and many apps still support NetBIOS.
3. Explain how NetBIOS names must be resolved to IP addresses before an administrator is able to connect to them.
4. Explain that to reduce NetBIOS name broadcasts, as well as ensure that NetBIOS names can be resolved for computers on other LANs in an organization, an administrator can implement one or more Windows Internet Name Service (WINS) servers to provide centralized NetBIOS name resolution that does not use broadcasts.

**Using WINS for NetBIOS Name Resolution**

1. Refer to Figure 1-24 and explain that to configure a Windows computer to use a WINS server for NetBIOS name resolution, an administrator can access the properties of the IPv4 protocol for a network interface.
2. Mention that the administrator will then click Next, click the Advanced button, select the WINS tab, and add the IP address of one or more WINS servers as shown in Figure 8-30.
3. Explain that during boot time, the computer will contact the first available WINS server listed in the IPv4 configuration of the network interface to create (or update) a NetBIOS name record that includes the NetBIOS name and IP address.
4. Mention that following this, the computer will contact the first available WINS server each time a NetBIOS name must be resolved, instead of sending a NetBIOS broadcast on the LAN.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | An administrator can also run the nbtstat -RR command in a Command Prompt window to create or update the NetBIOS name record for the computer on the WINS server. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If the computer does not contact a WINS server within 6 days, the NetBIOS name record is automatically removed from the WINS server. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To disable NetBIOS for a computer, select *Disable NetBIOS over TCP/IP* in Figure 8-30. |

**Configuring a WINS Server**

1. Introduce this topic by mentioning that to configure a Windows Server 2019 computer as a WINS server, an administrator must install and configure the WINS Server feature.
2. Refer to Figure 8-31 and explain how to start the WINS tool.
3. Refer to Figure 8-31 again. Explain that NetBIOS name records can be used to identify unique computers as well as groups (workgroups or domains). Mention that in addition to the 15 characters used to identify the NetBIOS name, NetBIOS name records contain a special character that identifies a service that is provided by the computer or group.
4. Explain that although NetBIOS name records are normally added to a WINS server automatically, an administrator can also add them manually. Refer to Figure 8-32 and explain that within the New Static Mapping window an administrator can create a NetBIOS name record for a computer.
5. Point out that if multiple WINS servers are deployed on the network, an administrator can configure them to share their NetBIOS name records. Mention that in this case, each WINS server is called a replication partner and can resolve all of the NetBIOS names in the organization.
6. Refer to Figure 8-31 and Figure 8-33. Explain how to configure a replication partner for the WINS server.

**Understanding DHCP**

1. Remind students that an administrator can configure a network interface manually, or the administrator can use Dynamic Host Configuration Protocol (DHCP) to have it configured automatically.
2. Describe the process that takes place if the network interface is configured using DHCP.
3. Point out that in addition to IP addresses, DHCP servers can also send client computers other IP configuration settings, such as a default gateway or DNS server. Explain that these IP configuration settings are called DHCP options and are identified by number. Refer to Table 8-3 and review common DHCP options that are often provided by DHCP servers.

**The DHCP Lease Process**

1. Mention that the process by which a DHCP client requests IP configuration from a DHCP server involves several stages. Refer to Figure 8-34 and explain the process.

**DHCP Relay**

1. Explain that because DHCPDISCOVER packets are broadcast to an entire LAN, routers do not forward them to other LANs by default. Mention that if no DHCP server is available on a LAN, DHCP clients will not be able to obtain an IP address lease.
2. Mention that it is costly to place a DHCP server on each LAN in an organization, so each router in an organization is usually configured as a DHCP relay agent. Explain what happens when a DHCP relay agent receives a DHCPDISCOVER packet.

**Configuring a DHCP Server**

1. Emphasize that to configure Windows Server 2019 as a DHCP server, an administrator must first install and authorize the DHCP Server role.
2. Refer to Figure 8-35 and explain why authorizing the DHCP Server role after installation is necessary in an Active Directory environment.
3. Refer to Figure 8-36. Explain that after the DHCP Server role is installed, an administrator can manage a DHCP server by clicking DHCP from the Tools menu in Server Manager to start the DHCP tool.
4. Mention that the DHCP tool uses scopes to organize the settings for each IPv4 and IPv6 network that it can provide IP configuration for. Refer to Figure 8-36 for an example of using scopes. Note that to configure a DHCP server, an administrator must create scopes that represent each of the networks for which the administrator wishes to provide IP configuration. Note that following this, an administrator can optionally configure scope and server features that provide additional functionality.

**Creating a New Scope**

1. Refer to Figure 8-36 through Figure 8-45. Explain how to create a new scope using the New Scope Wizard.

**Configuring Scopes**

1. Refer to Figure 8-36 and mention that by default, a newly created scope contains several folders.
2. Note that each folder allows an administrator to view or configure certain features of the scope.

* Address Pool
* Address Leases
* Scope Options
* Policies
* Reservations

1. As an example, refer to Figure 8-46 and explain how to create a reservation that always provides the IP address 192.168.100.100 to a network-attached printer called Ricoh 8220LP (with MAC address 80:a2:f4:77:4f:8b).
2. Mention that an administrator can modify other scope features by accessing the properties of the scope.
3. As an example, if an administrator highlights the Accounting LAN scope in Figure 8-36 and clicks More Actions, Properties in the Actions pane, the administrator is able to modify the name, description, IP range, and lease duration, as shown in Figure 8-47.
4. Remind students that the DNS dynamic update process runs as a low priority process and may fail to update host and PTR records if a client computer is too busy. Mention that DHCP clients running legacy (pre-Windows 2000), Linux, or macOS operating systems do not perform dynamic updates unless additional software is configured to deliver this functionality.
5. Mention that to provide reliable dynamic updates for all DHCP clients in an organization, an administrator can configure a DHCP server to dynamically update host and PTR records on behalf of each DHCP client when they obtain or renew a DHCP lease. Refer to Figures 8-47 and 8-49 and explain how to do this task for the Accounting LAN scope.
6. Remind students that DHCP can provide backward compatibility for BOOTP clients. Note that this feature is not enabled by default on a new scope. Explain that to allow both DHCP and BOOTP clients to obtain an IP configuration from the Accounting LAN scope, for example, highlight the Advanced tab in Figure 8-48 and select the Both option shown in Figure 8-49.
7. Refer to Figure 8-49. Mention that by default, BOOTP clients receive a 30-day lease. Mention that an administrator can modify this lease duration as shown in the figure. Additionally, point out that an administrator can modify the Subnet delay in the figure to provide a delay for DHCPOFFER packets if immediate responses cause problems with the DHCP relay agents in their organization.

**Configuring Filters**

1. Mention that some organizations configure MAC address filtering on a DHCP server to restrict IP leases to computers that were purchased by the organization.
2. Point out that alternatively, MAC address filtering can be used to prevent one or more computers from obtaining an IP lease from a DHCP server while allowing all others.
3. To configure MAC address filtering in the DHCP tool, access the Filters folder shown in Figure 8-36 and perform one of two procedures.

* To configure the DHCP server to respond only to DHCPDISCOVER packets that contain a MAC address from an organization computer, an administrator selects the Allow subfolder and clicks More Actions, Enable in the Actions pane. Next, the administrator must add the MAC address of each allowed computer to the Actions folder.
* To configure the DHCP server to respond to all DHCPDISCOVER packets except for those that contain a blacklisted MAC address, an administrator selects the Deny subfolder and clicks More Actions, Enable in the Actions pane. Next, the administrator must add the MAC address of each blacklisted computer to the Actions folder.

1. Refer to Figure 8-50. Explain that to add a MAC address to an Allow or Deny folder, and administrator highlights the folder in the DHCP tool and clicks More Actions, New Filter in the Actions pane. Next, the administrator must specify a MAC address and description.

**Configuring DHCP Fault Tolerance**

1. Mention that to provide fault tolerance for DHCP in an organization, an administrator can configure two DHCP servers in the DMZ with scopes for each network as well as configure the DHCP relay agents in the organization to forward DHCPDISCOVER packets to these DHCP servers.
2. Point out that if a DHCP relay agent is configured with the IP address of two DHCP servers, it will forward DHCPDISCOVER packets to the first DHCP server listed and to the second DHCP server if the first is unreachable.
3. Emphasize that an administrator can alternate the DHCP server that is listed first in the configuration of each DHCP relay agent to distribute DHCPDISCOVER packets between the two DHCP servers in the DMZ.
4. Explain that to prevent these two DHCP servers from independently issuing duplicate IP address leases for a network, the scope on each DHCP server must include a different IP address range for that network.
5. Emphasize that an administrator can also configure DHCP failover to provide fault tolerance for IPv4 scopes on two DHCP servers.
6. Mention that DHCP failover works in either *load balance* or *hot standby* mode. Describe how each mode works.
7. Refer to Figure 8-51 and explain how to configure DHCP failover.

**Troubleshooting DHCP**

1. Introduce this section by mentioning that after DHCP scopes have been configured for the networks in an organization, an administrator may need to troubleshoot problems related to the DHCP server configuration and problems that prevent DHCP clients from accessing the network or DHCP server.
2. Refer to Table 8-4 and review some common problems related to DHCP and possible solutions.

**Quick Quiz 2**

1. True or False: When troubleshooting most DNS-related problems, the first step typically involves testing forward lookups from a resolver using the nslookup command at a Command Prompt or Windows PowerShell window.

Answer: True

1. True or False: If an administrator types nslookup with no arguments, it will run in an interactive mode that allows the administrator to perform multiple lookups.

Answer: True

1. What technique can be used to prevent one or more computers from obtaining an IP lease from a DHCP server while allowing all others?
   1. DHCP load balancing
   2. DHCP hot standby monitoring
   3. MAC address filtering
   4. scavenging

Answer: c. MAC address filtering

1. Which DHCP failover mode has each DHCP server containing identical scope and lease information and coordinates all responses to DHCPDISCOVER packets with the other DHCP server to distribute the load?
   1. hot standby
   2. load balance
   3. warm mirror
   4. parallel process

Answer: b. load balance

# **Class Discussion Topics**

1. Discuss in detail the creation of a DNS implementation plan.
2. What are the advantages and disadvantages of using DHCP?

# **Additional Projects**

1. DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. Ask your students to read the article “Deploy DHCP Using Windows PowerShell” and to write a report summarizing the steps involved. Refer to this article so that all students use common information: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-deploy-wps>.
2. Have students read the following article about IPAM, then discuss IP address management: <https://www.manageengine.com/products/oputils/what-is-ipam.html>.

# **Additional Resources**

1. What is an IP address?

<https://computer.howstuffworks.com/internet/basics/what-is-an-ip-address.htm>

1. How DHCP Server works Explained with Examples

<https://www.computernetworkingnotes.com/networking-tutorials/how-dhcp-server-works-explained-with-examples.html>

1. How DNS Works

<https://technet.microsoft.com/en-us/library/cc772774.aspx>

1. Dynamic DNS

<https://en.wikipedia.org/wiki/Dynamic_DNS>

**Key Terms**

* **Active Directory-integrated primary DNS server** A DNS server that is also a domain controller, where zone files can be stored in the Active Directory database and replicated to other domain controllers that are also configured as DNS servers.
* **authoritative** A DNS server that contains resource records for one or more zones is said to be authoritative for those zones.
* **caching-only DNS server** A DNS server that does not contain any zones, but instead relays forward lookups and caches the results.
* **debug logging** A logging option that obtains more detailed information if the information in the DNS Server log is not sufficient to locate a solution to a problem.
* **default forwarder** A DNS server that forwards requests it cannot resolve to other DNS servers instead of using root hints to perform recursive queries.
* **DHCP failover** A configuration that provides fault tolerance for IPv4 scopes on two DHCP servers.
* **DHCP option** Tagged data items that provide information to a DHCP client. The options are sent in a variable-length field at the end of a DHCP message.
* **DHCP policy** Provides a specific IP range or DHCP options for DHCP clients based on criteria in the DHCPDISCOVER packet.
* **DHCP relay agent** Any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.
* **DHCP Server** A server that dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP.
* **DNS Server** A server that maintains a directory of domain names and translates them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines access websites based on IP addresses.
* **DNS Server log** The primary log where the DNS records information.
* **dynamic DNS (DDNS)** The dynamic update feature of the DNS.
* **forward lookup** Forward DNS lookup is using an Internet domain name to find an IP address.
* **hosts file** A file used to map hostnames (in other words, domains) to IP addresses.
* **IP Address Management (IPAM)** A software product that provides for centralized management of servers.
* **iterative query** A DNS query where the client communicates directly with each DNS server involved in the lookup. This is in contrast to a recursive query lookup, where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client.
* **MAC address filtering** Adds an extra layer of security that checks the device's MAC address against a list of agreed addresses. If the client's address matches one on the router's list, access is granted, otherwise, it does not join the network.
* **NetBIOS name record** A record containing a NetBIOS name, which is a 16-byte name for a networking service or function on a machine running Microsoft Windows Server. NetBIOS names are a more friendly way of identifying computers on a network than network numbers and are used by NetBIOS-enabled services and applications.
* **netmask ordering** If enabled on a DNS server, the DNS server will look at the IP address of the client that is performing the DNS query. When multiple DNS records exist on the same host name, the DNS server will respond back with a host name that is in the same network as the client when possible. In some cases there may be multiple DNS records in the same network as the client. If round robin is also enabled, the DNS records that are on that network will be cycled through.
* **Network Time Protocol (NTP)** A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.
* **primary DNS server** The first DNS server in a zone.
* **recursive query** A lookup where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client. This is in contrast to an iterative DNS query, where the client communicates directly with each DNS server involved in the lookup.
* **replication partner** A WINS server deployed on the network that is configured to share its NetBIOS name records.
* **reservation** Allows an administrator to provide the same IP address each time a DHCPDISCOVER packet is received from a DHCP client that has a certain MAC address.
* **resolver** A client computer.
* **resource record** Record that contains the FQDN and IP information for computers in a zone.
* **reverse lookup** Configuring the DNS to resolve IP addresses to FQDNs. Reverse DNS lookup is using an Internet IP address to find a domain name.
* **root hints** DNS data stored in a DNS server. The root hints file provides a list of preliminary resource records that can be used by the DNS service to locate other DNS servers that are authoritative for the root of the DNS domain namespace tree.
* **round robin** A technique of load distribution, load balancing, or fault-tolerance provisioning of multiple, redundant Internet Protocol service hosts, e.g., Web server and FTP servers, by managing the Domain Name System's (DNS’s) responses to address requests from client computers according to an appropriate statistical model.
* **scavenging** Removing stale resource records.
* **scope** A way to organize the settings for each IPv4 and IPv6 network so that the DHCP tool can provide IP configurations for them.
* **secondary DNS server** An additional DNS server in a DNS zone that contains a read-only copy of the zone file from the primary DNS server that can be used to respond to DNS lookup requests.
* **stale resource records** Records that are no longer valid but have accumulated in zone data over time.
* **stub DNS server** A stub DNS server forwards requests for a target organization’s zone directly to a DNS server in the target organization.
* **Time To Live (TTL)** The amount of time that a computer is able to cache the result of a lookup.
* **Windows Internet Name Service (WINS)** Microsoft's implementation of NetBIOS Name Service. It is a name server and service for NetBIOS computer names. Effectively, WINS is to NetBIOS names what the DNS is to domain names: a central mapping of host names to network addresses.
* **WINS Server** A server used to resolve DNS names.
* **zone** Any distinct, contiguous portion of the domain name space in the Domain Name System (DNS) for which administrative responsibility has been delegated to a single manager. The domain name space of the Internet is organized into a hierarchical layout of subdomains below the DNS root domain.
* **zone file** Stores resource records for the zone.
* **zone transfer** The process of copying newly added resource records from the primary DNS server to a secondary DNS server.