40555A Networking Fundamentals

Module 7: Network services

Contents

Learning objectives based on MTA exam objectives

#	Lesson title	Learning objectives	Exam objectives mapped
1	DHCP	• Describe Dynamic Host Configuration Protocol (DHCP). • Explain how DHCP works. • Explain how to implement DHCP in the Windows Server operating system. • Discover how to configure DHCP in Windows Server.	3.5.1 Dynamic Host Configuration Protocol (DHCP)
2	Remote Access	• List and describe remote access methods. • Describe Remote Desktop. • Describe Web Application Proxy. • Explain how to implement remote access in Windows Server. • Create a Virtual Private Network (VPN) in the Windows 10 operating system. • Describe RADIUS.	3.5.4 Remote access 3.5.5 Virtual Private Network (VPN)

Module overview

So far, we've learned about the technologies and tools involved in planning, deploying, and configuring the networking components necessary to provide the network infrastructure fundamentals for an organization. In this module, we'll explore adding services that enable you to more easily configure computer devices with the necessary network settings. We'll also examine how to facilitate remote access for users who want to access organizational resources from somewhere other than the corporate network.

Objectives

After completing this module, you'll be able to:

- Describe how to implement DHCP.
- Describe how to implement remote access.

Lesson 1: DHCP

DHCP, or Dynamic Host Configuration Protocol, plays an important role in network infrastructure. It's the primary means of distributing important network configuration information to network clients, and it provides configuration information to other network-enabled services. To support and troubleshoot a modern network infrastructure, it's important that you understand DHCP.

Objectives

After you complete this lesson, you will be able to:

- Describe DHCP.
- Explain how DHCP works.
- Explain how to implement DHCP in Windows Server.
- Discover how to configure DHCP in Windows Server.

What is DHCP?

The DHCP protocol simplifies configuration of Internet Protocol Version 4 (IPv4) and IPv6 clients in a network environment. Before DHCP was widely used, each time you added a client to a network you had to configure it with information about the network on which you installed it. This information included the IP address, network's subnet mask, and default gateway for access to other networks.

When you manage many computers in a network, managing them manually becomes time-consuming. Because many corporations have thousands of computer devices, including handhelds, desktop computers, and laptops, it's not feasible to manually manage the IP configuration of networks of this size.

With DHCP, you can help to ensure that all clients have appropriate configuration information, which helps to eliminate human error during configuration. When key configuration information changes in the network, you can update it using the DHCP console without having to change the information directly on each computer.

DHCP is also a key service for mobile users who change networks often. DHCP enables network administrators to reconfigure mobile devices easily without requiring intervention from the users themselves.

DHCP is deployed as a Server role in Windows Server networks. You can also deploy DHCP functionality in wireless access points and other network infrastructure components.

How does DHCP work?

DHCP allocates IP addresses on a dynamic basis, known as a *lease*. You can configure an unlimited lease duration, but usually it's set to not more than a few hours or days. The default lease time for wired clients is eight days and three days for wireless clients. Figure 1 illustrates the DHCP lease process:

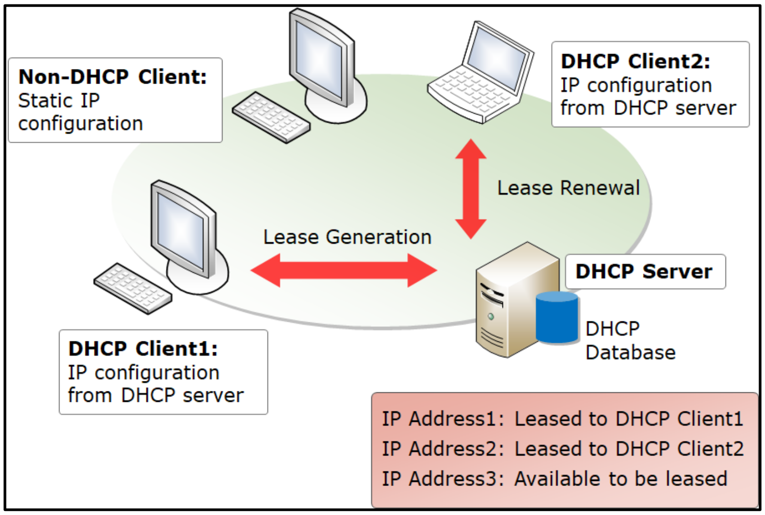

Non-DHCP Client:
Static IP configuration
DHCP Client2:
IP configuration from DHCP server
Lease Renewal
Lease Generation
DHCP Server
DHCP Database
DHCP Client1:
IP configuration from DHCP server
IP Address1: Leased to DHCP Client1
IP Address2: Leased to DHCP Client2
IP Address3: Available to be leased

Figure 1. How DHCP works

DHCP uses IP broadcasts to initiate communications. Therefore, by default, DHCP servers are limited to communication within their IP subnet. This means that in many networks, must be a DHCP server for each IP subnet. Where there are a large number of subnets, this can get expensive.

Where you want a single DHCP server to service collections of smaller subnets, you must deploy a DHCP relay agent. For the DHCP server to respond to a DHCP client request, it must be able to receive DHCP requests, and the DHCP relay agent enables.

The DHCP relay agent allows DHCP broadcast packets to be relayed into another IP subnet across a router. You then can configure the agent in the subnet that requires IP addresses. Additionally, you can configure the agent with the IP address of the DHCP server. This allows the agent to capture the client broadcasts and forward them to the DHCP server in another subnet. You can also relay DHCP packets into other subnets using a router that's compatible with passing DHCP traffic as defined by RFC 1542.

Note

When you deploy multiple DHCP servers, it's important that if the ranges of addresses you want to lease overlap, you configure DHCP servers in failover configurations. How to do that is out of the scope of this course, but you can find out more at Step-by-Step: DHCP High Availability with Windows Server 2012 R2.

Lease generation

The DHCP protocol lease-generation process includes four steps that enable a client to obtain an IP address. Understanding how each step works will help you to troubleshoot problems when clients cannot obtain an IP address.

The following steps, which Figure 2 depicts, describe the DHCP protocol lease-generation process:

1. The DHCP client broadcasts a DHCPDISCOVER packet. This is a message that is broadcast to every computer in the subnet. The only computer that will respond is the one that has the DHCP server role, or a computer or router running a DHCP relay agent. In the latter case, the DHCP relay agent will forward the message to the DHCP server with which it is configured.

2. A DHCP Server responds with a DHCPOFFER packet. This packet will provide the client with a potential address.

3. The client receives the DHCPOFFER packet. It might receive packets from multiple servers. If the client receives offers from more than one server, it usually will choose the server that made the fastest response to its DHCPDISCOVER. This typically is the DHCP server closest to the client. Then, the client will broadcast a DHCPREQUEST, which contains a server identifier. This identifier informs the DHCP servers that receive the broadcast which server the client has chosen to accept the DHCPOFFER from.

4. The DHCP servers receive the DHCPREQUEST. Those servers that the DHCPREQUEST message does not accept use the message as notification that the client has declined that server's offer. The chosen server stores the IP address client information in the DHCP database and responds with a DHCPACK message. If for some reason the DHCP server cannot provide the address that was offered in the initial DHCPOFFER, the DHCP server will send a DHCPNAK message.

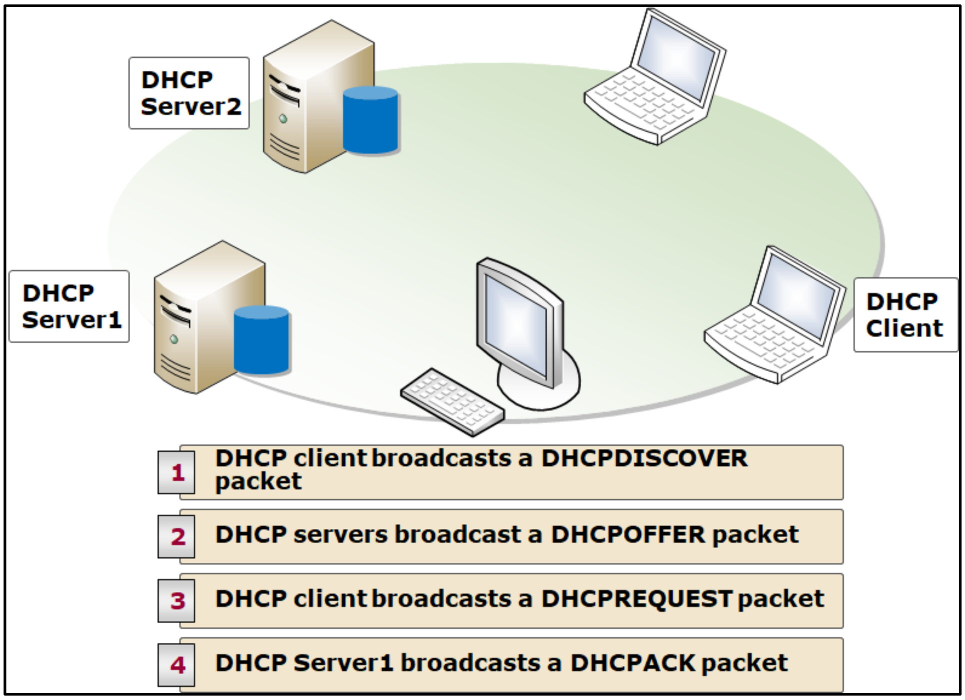

DHCP Server2
DHCP Server1
DHCP Client
1 DHCP client broadcasts a DHCPDISCOVER packet
2 DHCP servers broadcast a DHCPOFFER packet
3 DHCP client broadcasts a DHCPREQUEST packet
4 DHCP Server1 broadcasts a DHCPACK packet

Figure 2. Initial DHCP lease-generation process

Lease renewal

When a DHCP lease has reached 50 percent of the lease time, the client will attempt to renew the lease. This is an automatic process that occurs in the background, as Figure 3 illustrates. Computers might have the same IP address for a long period of time if they operate continually on a network without being shut down.

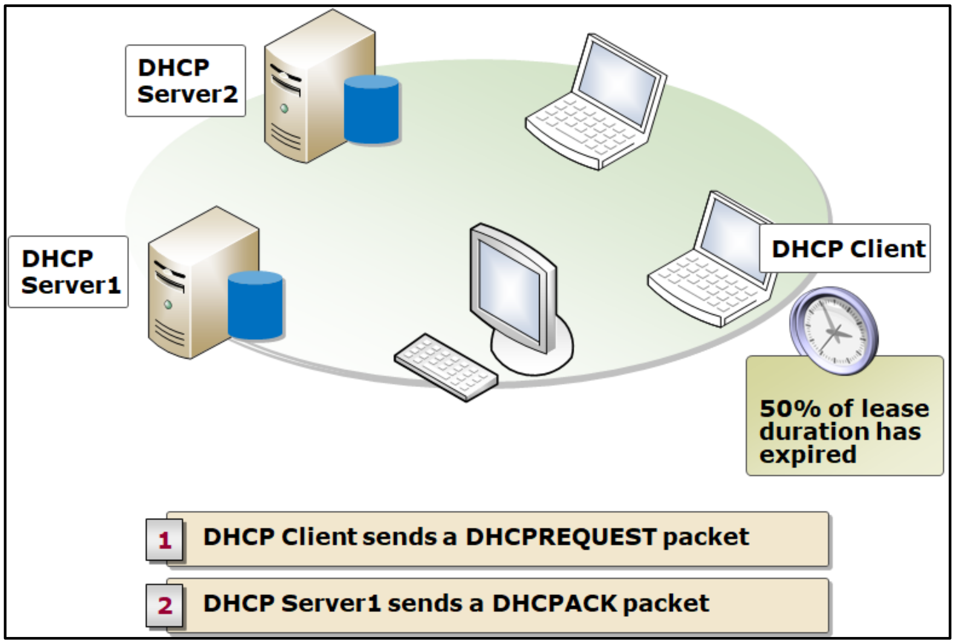

DHCP Server2
DHCP Server1
DHCP Client
50% of lease duration has expired
1 DHCP Client sends a DHCPREQUEST packet
2 DHCP Server1 sends a DHCPACK packet

Figure 3. The lease renewal process

Typically, renewal consists of two steps:

1. The renewing client sends a DHCPREQUEST to its DHCP server. Unlike during the lease generation process, this DHCPREQUEST is directed to the DHCP server by IP address.

2. The DHCP servers receive the DHCPREQUEST. The server updates the IP address client information in the DHCP database and responds with a DHCPACK message.

Client computers also attempt renewal during the startup process. This is because client computers might have been moved while they were offline; for example, a laptop computer might be plugged into a new subnet. If renewal is successful, the lease period is reset. If the renewal is unsuccessful, the client computer attempts to contact the configured default gateway. If the gateway doesn't respond, the client assumes that it's on a new subnet and reenters the Discovery phase, attempting to obtain an IP configuration from any DHCP server.

Implement DHCP in Windows Server

The first step in implementing DHCP in Windows Server is to install the DHCP server role. After that, you must authorize the server in Active Directory Domain Services (AD DS).

Note

DHCP allows a client computer to acquire configuration information about the network in which it is started. DHCP communication occurs before any authentication of the user or computer; and because the DHCP protocol is based on IP broadcasts, an incorrectly configured DHCP server in a network can provide invalid information to clients. To avoid this, the server must be authorized.

DHCP Scopes

After you deploy and authorize your DHCP Server role, you must create and configure DHCP Scopes.

A *DHCP scope* is a range of IP addresses that are available for lease. Typically, a scope is confined to the IP addresses in a given subnet, as Figure 4 depicts:

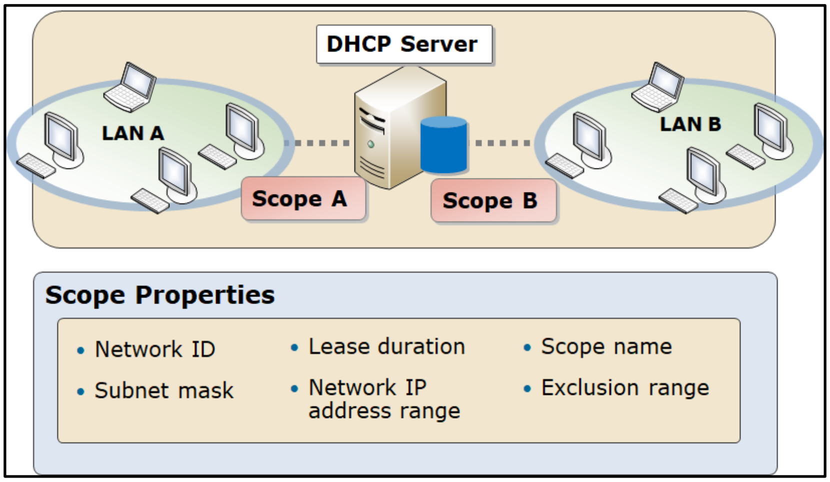


Figure 4. DHCP Scopes

For example, a scope for the network 192.168.1.0/24 (subnet mask of 255.255.255.0), supports a range of 192.168.1.1 through 192.168.1.254. When a computer or device in the 192.168.1.0/24 subnet requests an IP address, the scope that defined the range in this example would allocate an address between 192.168.1.1 and 192.168.1.254.

Note

Remember that the DHCP server, if deployed to the same subnet, consumes an IPv4 address. This address should be excluded from the address range.

IPv4 scopes

To configure an IPv4 scope, you must define the following properties:

- Name and description. This identifies the scope.
- IP address range. The range of addresses that can be offered for lease and usually the entire range of addresses for a given subnet.
- Subnet mask. This is used by the client computers to determine their location in the organization’s network infrastructure.
- Exclusions. Single addresses or blocks of addresses that fall within the IP address range but that will not be offered for lease.
- Delay. The amount of time to delay before making DHCPOFFER.
- Lease duration. Use shorter durations for scopes with limited IP addresses, and longer durations for more static networks.
- Options. You can configure several options on a scope, but typically you’ll configure option 003 – Router (the default gateway for the subnet), 006 – DNS Servers, and option 015 – DNS suffix.

Fourth Coffee

If the default lease duration is eight days, might you ever change this, and if so, why?

Let's think about the guys at Fourth Coffee. They're making their network infrastructure available to their customers by offering free Wi-Fi access. Customers who connect their phones or tablets will need an IP configuration. If they can lease a configuration for eight days, it's possible Fourth Coffee's IP address scope will be depleted of addresses quickly. Setting a short lease duration, say two hours, means that the lease is returned to the address pool almost immediately after a customer leaves the coffee shop. What are your thoughts about this approach?

IPv6 scopes

You can configure the IPv6 scope options as a separate scope in the DHCP console's IPv6 node. There are several different options available, and an enhanced lease mechanism.

When configuring a DHCPv6 scope, you must define the following properties:

- Name and description. This identifies the scope.
- Prefix. The IPv6 address prefix is analogous to the IPv4 address range; in essence, it defines the network address.
- Exclusions. Any single addresses or blocks of addresses that fall within the IPv6 prefix but will not be offered for lease.
- Preferred lifetimes. Define how long leased addresses are valid.
- Options. As with IPv4, you can configure many options.

DHCP options

DHCP servers can configure more than just an IP address; they also provide information about network resources such as DNS servers and the default gateway. You can apply DHCP options at the server, scope, user, and vendor levels. Common options include:

- DNS servers
- DNS name
- Default gateway
- Windows Internet Name Service (WINS) servers
- NetBIOS node type

An option code identifies the DHCP options, and most option codes come from the Request for Comments (RFC) documentation found on the Internet Engineering Task Force (IETF) website. The following table lists the common option codes that Windows-based DHCP clients request.

Option code	Name
1	Subnet mask
3	Router
6	DNS servers
15	DNS domain name
44	WINS/NBNS servers
46	NetBIOS node type
47	NetBIOS scope ID

Demonstration: Configuring DHCP in Windows Server

In this demonstration, you'll review how to deploy and configure DHCP in Windows Server.

Install the DHCP server role

1. Sign into the appropriate server as **Adatum\Administrator** with the password **Pa55w.rd**.

2. Open **Server Manager**, and then use the **Add Roles and Features Wizard** to install the **DHCP Server** role. Accept all the default settings.

Perform post-installation tasks

1. In the top menu bar, select the **Notifications** icon, and then select the **Complete DHCP configuration** link.

2. Complete the **DHCP Post-Install Configuration Wizard** by accepting all the default settings, and then close the wizard.

3. Restart the DHCP Server service.

Create a DHCP scope

1. On the DHCP server, in Server Manager, start the DHCP management console.

2. Select the local server icon to open the **IPv4** node.

3. Right-click or access the context menu of the **IPv4** node, and then create a new scope with the following parameters:

    - Name: **Adatum**

    - Start IP address: **10.0.0.100**

    - End IP address: **10.0.0.150**

    - Subnet mask: **255.255.255.0**

    - Lease Duration: **1 Day**

4. Do not configure DHCP options at this time.

Configure DHCP options

1. Expand the **IPv4** node, expand the **Scope [10.0.0.0] Adatum** folder, and then select the **Scope Options** folder.

2. Right-click or access the context menu of the **Scope Options** folder, and then configure the following options:

   - 003 Router: **10.0.0.1**

   - 006 DNS Servers: **172.16.0.10**

3. Activate the scope.

Lesson 2: Remote access

How often do you check your email on your phone? How often do you save a document to the cloud, and then access it using a different device from somewhere else? These days, a mobile workforce is to be expected.

To support an organization’s distributed workforce, we need to be familiar with technologies that enable remote users to connect to their organization’s network infrastructure. These technologies include Remote Desktop, Web Application Proxy, and VPNs. We should also know how to provide for authentication and authorization for remote access user using RADIUS.

Objectives

After you complete this lesson, you will be able to:

- List and describe remote access methods.
- Describe Remote Desktop.
- Describe Web Application Proxy.
- Explain how to implement remote access in Windows Server.
- Create a VPN in Windows 10.
- Describe RADIUS.

Types of remote access

Today, more people work away from their offices. Their work enables and sometimes necessitates that they work from home or while traveling. In Module 1, we reviewed some remote access solutions that provide a more secure way of accessing your internal data and applications from user devices that attach to the internet. There are several additional remote access technologies, including:

- Remote Desktop. Remote Desktop is a Windows operating system feature that uses RDP to enable users to access files on their work computer from another computer, such as one located at their home. Additionally, Remote Desktop allows administrators to connect to multiple sessions of the Windows Server operating system simultaneously for remote administration purposes.
- Reverse web proxy. This provides access for users who must connect to their organization's internal web applications from the internet. The reverse web proxy, such as the Web Application Proxy server role, is deployed in the perimeter network. Publishing rules define what type of network applications are available from the internal network to users connected to the internet.
- VPN. Enable users that are working offsite (such as from home, a customer site, or a public wireless access point) to access a server on an organization's private network using a public network such as the internet. From the user's perspective, the VPN is a point-to-point connection between a computer, the VPN client, and an organization's server. The exact infrastructure of the shared or public network is irrelevant because it appears as if the data is sent over a dedicated private link.

Remote Desktop

Remote Desktop Services (RDS) helps provide users with access to a full remote desktop experience. Using RDS, users securely connect to a remote session via their local Remote Desktop Connection (RDC) client. After they authenticate, users are presented with a full desktop experience as if they were signed in locally.

The user's remote client machine sends keystrokes and mouse movements to the remote device, and screen images are delivered back to the client machines. Users have access to applications as if the applications are running locally, even though they're running remotely.

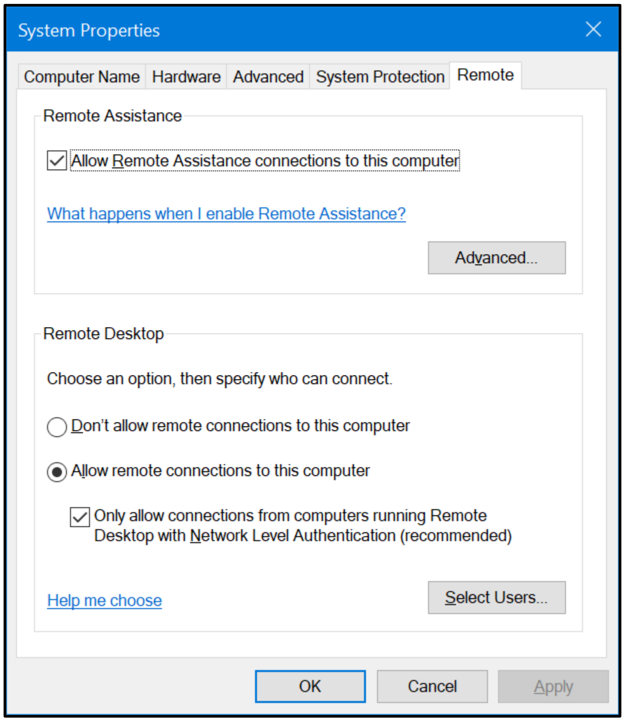
Remote desktop sessions perform well over limited bandwidth, making this a suitable solution for branch offices where information technology support might be limited. Another common use for remote desktops is to enable users to access their organizational desktop. For example, users can work from home by connecting to their workstations. Remote desktops are also well suited to single-task users, such as point-of-sale terminals or data entry workers.

Note

During the time that a Remote Desktop session is active, Remote Desktop locks the target computer, prohibiting interactive sign-ins for the session's duration.

Enabling Remote desktop

On a computer or device running Windows 10, you can enable Remote Desktop in the **System Properties** dialog box. You access **System Properties** through the Control Panel, which Figure 5 depicts:



Remote Assistance

☑ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Only allow connections from computers running Remote Desktop with Network Level Authentication (recommended)

Figure 5. Enabling Remote Desktop

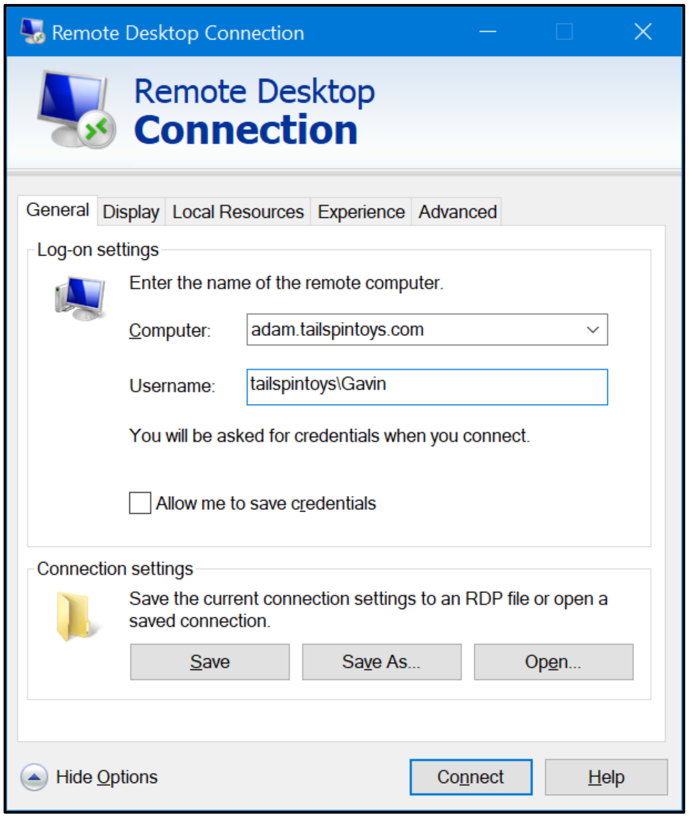
Alternatively, you can enable Remote Desktop by right-clicking or accessing the context menu of **This PC**, selecting **Properties**, and then selecting **Remote settings**.

Remote Desktop has three settings:

- **Don't allow remote connections to this computer**. This is the default setting, in which remote connections are disabled.
- **Allow remote connections to this computer**. If you are unsure of the version of the Remote Desktop client software, this is the best choice.
    - **Only allow connections from computers running Remote Desktop with Network Level Authentication (recommended)**. This check box option is a subset of **Allow remote connections to this computer**. When selected, Network Level Authentication completes user authentication before the user establishes a Remote Desktop connection and the sign-in screen appears. This is more secure.

Using Remote Desktop

The RDC client software is already built into Windows 10. To launch the Remote Desktop Connection app, in the **Search** box, enter **mstsc.exe.** This launches a remote session. To connect to the remote computer, you can enter in either the name or the IP address of the remote computer. Figure 6 depicts the Remoted Desktop Connection dialog box.



Enter the name of the remote computer.

Computer: adam.tailspintoys.com

Username: tailspintoys\Gavin

You will be asked for credentials when you connect.

□ Allow me to save credentials

Save the current connection settings to an RDP file or open a saved connection.

Figure 6. Remote Desktop Connection dialog box

Note

For devices running iOS or Android, you can download a Microsoft Remote Desktop client app from the Apple or Google Play stores.

When you connect, you will be asked for credentials. If another user is already signed in when you attempt to connect, that user has 30 seconds to refuse to allow your connection. If the signed in user allows your connection or does not respond, your connection will occur successfully.

The following table lists the client options you can configure using the various tabs in the **Remote Desktop Connection** dialog box.

Tab	Option
General	Enter the computer and user name, and select whether to save the connection as an RDP file.
Display	Select the remote display's screen size and color quality.
Local Resources	Use remote computer resources in your session, such as a printer or clipboard.
Experience	Configure the way you want the remote session to appear visually. The more features that you add, the more bandwidth it utilizes.
Advanced	Tell the Remote Desktop client how to behave if the RDP server fails to prove its authenticity. You can choose whether to connect without warning or to receive a warning, and whether to connect or prevent the connection.

When establishing a Remote Desktop session, you can configure local devices and resources to be redirected to a remote computer. Doing this enables you to use these resources. For example, by redirecting a local audio device to a remote computer, you can perform audio playback on that remote computer. It's not necessary to reconfigure firewall settings to support resource redirection. When you enable resource redirection, the traffic for each redirected resource is added to the existing connection over port 3389.

Web Application Proxy

Web Application Proxy is Microsoft's implementation of a reverse web proxy. Part of the Remote Access role service, it provides access to internal organizational web applications for users who remotely connect to the organization's network.

After you deploy the Web Application Proxy and finish configuring it, you can publish applications to the internet. Typically, the Web Application Proxy server is placed in the perimeter network between two firewall devices. The published applications are located in the organizational network with domain controllers and other internal servers, and they are protected by the second firewall. This scenario helps provide more secure access to organizational applications for users on the internet. At the same time, this scenario helps protect the organization’s IT infrastructure from security threats from the internet.

Demonstration: Enabling remote access in Windows Server

Your instructor will now demonstrate how to deploy and configure DHCP in Windows Server.

Install the Remote Access server role

1. On **LON-SVR1**, open **Server Manager**, select **Manage**, and then start the **Add Roles and Features Wizard**.

2. In the wizard, on the **Before you begin** page, select **Next**.

3. On the **Select installation type** page, select **Next**.

4. On the **Select destination server** page, select **Next**.

5. On the **Select server roles** page, select **Remote Access**, and then select **Next**.

6. On the **Select features** page, select **Next**.

7. On the **Remote Access** page, select **Next**.

8. On the **Select** role services page, select **DirectAccess and VPN (RAS)**.

9. In the **Add Roles and Features Wizard** dialog box, select **Add Features**, and then select **Next**.

10. On the **Confirm installation selections** page, select **Install**.

11. When the installation finishes, select **Close**.

Manage the Remote Access server role

1. In the **Server Manager** console, open the **Remote Access Management** console and review the options for configuring and managing remote access.

2. From the **Server Manager** console, open the **Routing and Remote Access** console and review the options for configuring and managing remote access.

Creating a VPN in Windows 10

A VPN provides a point-to-point connection between components of a private network, through a public network such as the internet. Tunneling protocols enable a VPN client to establish and maintain a connection to a VPN server's "listening" virtual port.

Note

Remember, we learned about VPNs in Module 1, "Overview of Networking," Lesson 4: Virtual Private Networks.

To create a VPN connection in Windows 10, use the following procedure:

1. Select the **Network** icon in the notification area, and then select **Network & Internet** settings.

2. In the **Network & Internet** dialog box, select the **VPN** tab.

3. Select **Add a VPN connection**.

4. In the **Add a VPN connection** dialog box, in the **VPN provider** list, select **Windows (built-in)**.

5. In the **Connection name** box, enter a meaningful name, such as **Office Network**.

6. In the **Server name or address** text box, enter the FQDN of the server to which you want to connect. (This is usually the name of the VPN server.)

7. In the **VPN type** list, select from the following VPNs:

    - **Point to Point Tunneling Protocol (PPTP)**
    - **L2TP/IPsec with certificate**
    - **L2TP/IPsec with pre-shared key**
    - **Secure Socket Tunneling Protocol (SSTP)**
    - **IKEv2**

    This setting must match the setting and policies configured on your VPN server. If you are unsure, select **Automatic**.

8. In the **Type of sign-in info** list, select from:

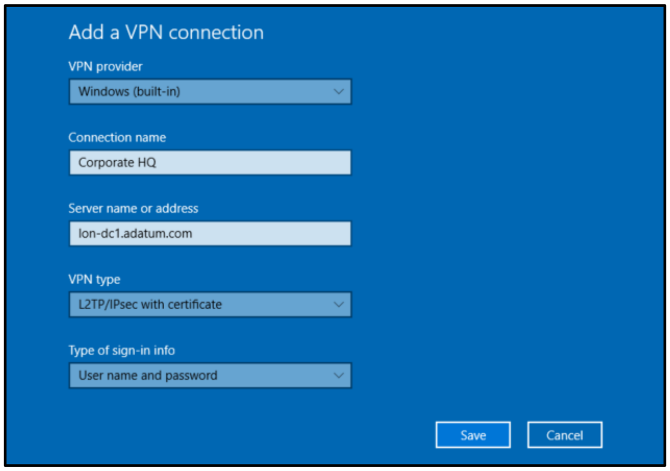
    - **User name and password**
    - **Smart card**
    - **One-time password**
    - **Certificate**

    Again, this setting must match your VPN server policies.

9. In the **User name (optional)** text box, enter your user name, and then in the **Password (optional)** text box, enter your password.

10. Select the **Remember my sign-in info** check box, and then select **Save**.

To manage your VPN connection, from within **Network & Internet**, on the **VPN** tab, select the VPN connection, and then select **Advanced** options. You can then reconfigure the VPN settings as needed. Figure 7 depicts the Add a VPN connection wizard:



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: Corporate HQ

Server name or address: lon-dc1.adatum.com

VPN type: L2TP/IPsec with certificate

Type of sign-in info: User name and password

Figure 7. Add a VPN connection

Note

Your VPN connection will appear on the list of available networks when you select the network icon in the notification area.

What is RADIUS?

RADIUS is an industry-standard authentication protocol used by many vendors to support the exchange of authentication information between elements of a remote access solution. A RADIUS solution consists of the following components:

- RADIUS client
- RADIUS proxy
- RADIUS server

RADIUS clients

A *network access server* is a device that provides some level of access to a larger network. A network access server using a RADIUS infrastructure is also referred to as a RADIUS client. The RADIUS client originates connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting. In other words, if you deploy a VPN server on a Windows Server computer, the VPN server (a network access server) is a RADIUS client.

Note

Client computers such as wireless laptop computers and other computers that are running client-operating systems are not RADIUS clients. RADIUS clients are network access servers—including wireless access points, 802.1X authenticating switches, VPN servers, and dial-up servers—because they use the RADIUS protocol to communicate with RADIUS servers such as Network Policy Server (NPS) servers.

Examples of network access servers include:

- Servers that provide remote access connectivity to an organization network or the internet. This includes computers that are running both the Windows Server operating system, and the Routing and Remote Access service that provides either traditional dial-up or VPN remote access services to an organization’s intranet.
- Wireless access points that provide physical-layer access to an organization’s network using wireless-based transmission and reception technologies.
- Switches that provide physical-layer access to an organization’s network using traditional local area network (LAN) technologies, such as Ethernet.
- RADIUS proxies that forward connection requests to RADIUS servers that are members of a remote RADIUS server group that you configure on the RADIUS proxy, or other RADIUS proxies. (We’ll discuss RADIUS proxies in a moment).

RADIUS proxies

You can use a RADIUS proxy to route RADIUS messages between RADIUS clients (network access servers) and RADIUS servers, which perform user authentication, authorization, and accounting for the connection attempt. When you a RADIUS proxy, it acts a central switching or routing point through which RADIUS access and accounting messages flow. The proxy can also record information in an accounting log about forwarded messages.

You can use a RADIUS proxy when:

- You are a service provider who offers outsourced dial, VPN, or wireless network access services to multiple customers. The RADIUS proxy makes a determination about which RADIUS server should be used for authentication.
- You want to provide authentication and authorization for user accounts.
- You want to process a large number of connection requests. In this case, instead of configuring your RADIUS clients to attempt to balance their connection and accounting requests across multiple RADIUS servers, you can configure them to send their connection and accounting requests to an NPS RADIUS proxy. The NPS RADIUS proxy dynamically balances the load of connection and accounting requests across multiple RADIUS servers, and it increases processing of large numbers of RADIUS clients and authentications each second.
- You want to provide RADIUS authentication and authorization for outsourced service providers and minimize intranet firewall configuration.

RADIUS servers

Internet service providers (ISPs) and organizations that maintain network access have the increased challenge of managing all types of network access from a single administration point, regardless of the type of network-access equipment they use. The RADIUS standard supports this functionality in homogeneous and heterogeneous environments. RADIUS is a client-server protocol that enables network-access equipment, used as RADIUS clients, to submit authentication and accounting requests to a RADIUS server.

A RADIUS server performs centralized connection authentication, authorization, and accounting for wireless, authenticating switch, and dial-up and VPN connections.

Note

The NPS role is the Microsoft implementation of a RADIUS server. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access. These include wireless, authenticating switch, dial-up and VPN remote access, and router-to-router connections.

A RADIUS server has access to user account information and can check network access authentication credentials. If the user's credentials are authentic and RADIUS authorizes the connection attempt, the RADIUS server then authorizes the user's access based on specified conditions, and logs the network-access connection in an accounting log. Using RADIUS allows the network-access user authentication, authorization, and accounting data to be collected and maintained in a central location, rather than on each access server. A common RADIUS infrastructure, which Figure 8 illustrates.

Making it real

Generally, a RADIUS server is defined by its relationship with network access servers. In a Windows Server network, you point VPN servers at an NPS, and you have therefore defined a RADIUS client and RADIUS server relationship, as Figure 8 depicts.

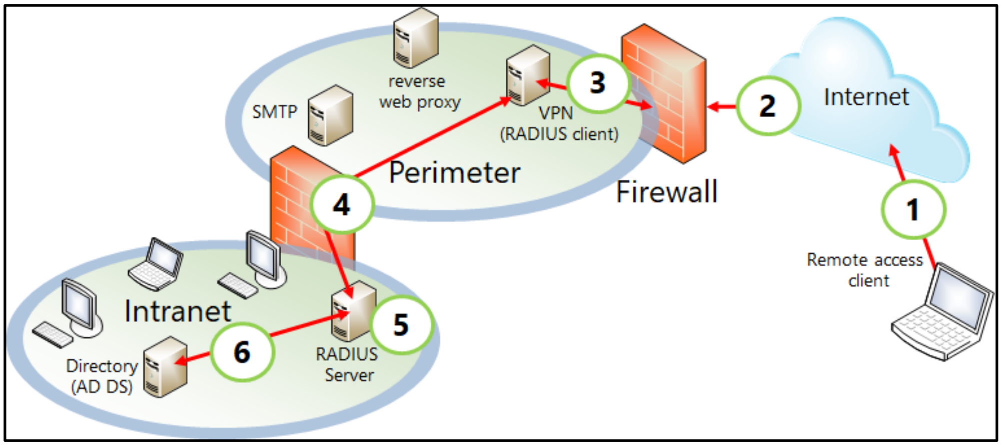


Figure 8. How RADIUS works

When a user initiates a remote access connection attempt, the following happens:

1. The remote access client (perhaps a computer running Windows 10) initiates a VPN connection.

2. A tunnel is created through the internet to the external firewall that protects the organization's network. The firewall allows the passage of the VPN traffic to the perimeter network.

3. The VPN server receives the connection attempt. This is a network access server, and therefore functions as a RADIUS client.

4. The VPN server (RADIUS client) forwards a request for authentication to its configured RADIUS server. There's no need for the RADIUS server to be in the perimeter network, so the traffic is directed through the internal firewall to the organization's intranet.

5. The RADIUS server checks the properties of the connection attempt, including example authentication method, encryption settings, and tunnel type.

6. The RADIUS server also checks the credentials being offered (username and password) against a directory service. Assuming that the user account has permissions to connect remotely, and assuming the characteristics of the connection attempt meet the configured requirements, the connection attempt is successful. The remote access client is joined to the organization's network.

Learning in action: Implement network services

Scenario 1

Things are going well for you at Lucerne Publishing. The network infrastructure is largely in place across the new offices and retail outlets. Recently, the managing director called you in to her office and asked about facilitating remote access for some of the editors. There's also a new requirement to support remote access from authors that write for the company. You have been tasked with creating a proposal to define a remote access strategy for the company.

Questions

1. **Remote authors require access to a web application that's hosted on a web server in the London, England offices. What remote access component would serve this need best?**

   A. Deploying a VPN

   B. Installing a Web Application Proxy

   C. Deploying a DHCP server

   D. Deploying RDS

2. **The financial director has requested access to the accounts system. It's installed on his computer in the office. He wants to be able to access the material from a tablet running iOS. What could you do to address this need?**

   A. Deploy a VPN.

   B. Install a Web Application Proxy.

   C. Deploy a DHCP server.

   D. Deploy RDS.

3. **You want to make sure that all editors can securely gain access to all company resources from any network. What's the best remote access technology for addressing this requirement?**

   A. VPN

   B. Web Application Proxy

   C. A DHCP server

   D. RDS

Scenario 2

Lucerne Publishing has a need for a new warehouse. The physical building they've leased and all the network infrastructure (such as cabling and routers) are installed. The location will support a range of wireless and wired Windows 10 and iOS devices. You want to simplify the process of allocating IP configurations to these devices and decide to deploy a DHCP server.

Questions

1. **To complete the process of configuring DHCP, how would you order the following steps?**

   A. Authorize the DHCP server in AD DS.

   B. Install the DHCP server role.

   C. Create the required scopes in DHCP.

   D. Configure DHCP options and activate scopes.

2. **After a few months, you notice that wireless access attempts are being made from the parking lot outside the building. You decide to secure things a little more. What could you do?**

   A. Make the lease duration shorter for wireless clients.

   B. Stop using wireless access points.

   C. Deploy a RADIUS configuration and require wireless clients to authenticate with the wireless access point using RADIUS.

   D. Monitor the parking lot for people with computers.

Test your knowledge

1. **When a computer initially attempts to obtain an IPv4 configuration from a DHCP server, it broadcasts which of the following packets onto the network?**

   A. DHCPACK

   B. DHCPOFFER

   C. DHCPDISCOVER

   D. DHCPREQUEST

2. **The default lease duration for a wired network configuration in DHCP is:**

   A. Eight hours

   B. Eight days

   C. Four hours

   D. Four days

3. **In Windows Server, which of the following provides RADIUS server functionality?**

   A. Remote Access Server

   B. AD DS domain controller

   C. NPS

Fill in the blanks for the following sentences.

4. **A computer that obtains an IPv4 configuration from a DHCP server is said to (   ) the configuration.**

5. **A Web Application Proxy should be placed in the (   ) network.**

6. **A Windows 10 computer configured with a VPN, is an example of a (   ) client.**

7. **True or false: Client computers with a DHCP-configured IPv4 address renew their addresses at startup.**

   True

   False

8. **True or false: A VPN server is an example of a RADIUS server.**

   True

   False

Study the scenario and answer the question.

9. **At Fourth Coffee, Josh wants his clients to be able to obtain an IP configuration from his network. However, he has limited IPv4 addresses available for customer devices.**

   What could he do to address this issue?

10. **You deploy a DHCP server for Josh at Fourth Coffee. You create and configure the necessary scopes. Then one day, Josh calls you to tell you that no one can connect to the network. You pop into the coffee shop on your way back from work and you find that the DHCP server is offline. You bring it back online, but you want to try to avoid the same problem in the future.**

    What could you do?

Glossary

Term	Definition
Firewall	A device or software component that can filter network traffic based on its characteristics and determine whether to allow or block that traffic
Perimeter network	The network between an external and an internal firewall. Using a perimeter network, no traffic can pass directly from the internet to the protected internal network, and no traffic can pass directly from the protected internal network to hosts on the internet.
RDP	The Remote Desktop Protocol (RDP) provides remote display and input capabilities over network connections for Windows-based applications.
Remote Desktop	Remote Desktop uses RDP to enable users to access files on their office computer from another computer, such as one located at their home.
Reverse proxy	Allows you to enable remote internet-based access to specific services on your internal network without placing the servers hosting those services in the perimeter network. Using reverse proxy, you can publish those services.
Router	An internetwork device that propagates and receives network packets at layer 3 of the OSI reference model. Routers enable network administrators to separate networks into distinct subnets to help to manage network traffic. Routers are also used to join remote LANs to create WANs. A router is network transport specific; that's to say, it runs a specific network protocol, such as TCP/IP.
Virtual private network	A tunnel created by authentication and networking protocols that enables an organization to use the public internet as a transport for private communications.
Web proxy	Clients on the internal network use this server to access web-related content on the internet. It will also store cached copies of

Term	Definition
	commonly accessed sites. This server might be configured to check web content for malware and could also be used to block certain sites and content from being accessed by clients on the internal network.