# **Module 9**

**Configuring and Managing Remote Access 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**

In this module, students are introduced to the basic network infrastructure model in use by most organizations today. The necessity to access resources on servers within the DMZ from locations outside an organization is explained and the three main remote access technologies supported by Microsoft—VPNs, DirectAccess, and Remote Desktop Services—are introduced. Then, each method is described in detail. Students gain an understanding of the advantages and disadvantages of each access technology and learn how to install, configure, and support the technology as well.

# **Module Objectives**

* Identify methods used to provide remote access in an organization
* Describe the components used to provide for VPN remote access
* Configure a remote access server for VPN remote access
* Configure RADIUS to support VPN remote access
* Describe how DirectAccess can be used to enable automated remote access
* Implement remote access using DirectAccess
* Identify the components that enable remote access using Remote Desktop and RemoteApp
* Configure Remote Desktop Services

# **Teaching Tips**

**Understanding Organization Networks and Remote Access**

1. Refer to Figure 9-1 and discuss the common network structure used today by many organizations. Be sure to describe how client PCs in department LANs access servers contained in a separated DMZ network. Point out that unless the organization uses IPv6 exclusively, the router that connects the DMZ to the Internet will implement NAT in order to allow networks in the organization to use a reserved IPv4.
2. Mention that the methods by which organizations connect to the Internet vary by region and technology even though most organizations implement the network structure illustrated in Figure 9-1.
3. Define and discuss what is meant by a last mile technology. Be sure to describe common last mile technologies used to connect to an ISP.
* Digital subscriber line (DSL)
* Cable broadband
* Gigabit Passive Optical Network (GPON)
* Long-range Wi-Fi

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | To communicate to an ISP using IP across a telephone network, DSL encloses Ethernet frames in a protocol called Point-to-Point Protocol over Ethernet (PPPoE). |

1. Point out that in most cases, the organization NAT router is connected to a demarcation point (demarc) that connects to the ISP using a last mile technology. Define the demarc as a translation device or router with a specialized network interface for the last mile technology that passes traffic directly between the ISP and NAT router.
2. Refer to Figure 9-1 again and explain why this network structure alone does not allow remote access to resources on the servers in the DMZ. Emphasize that remote access technology is needed.
3. Refer to Figure 9-2 and mention that to provide for remote access, at least one server in the DMZ must be configured as a remote access server that accepts requests from remote access clients on the Internet. Explain how a remote access client can access resources on other servers in the DMZ.
4. Mention that to access a remote access server, the remote access client must connect to the public IP of the NAT router (1.2.3.4), which is often resolved using a host record in a DNS zone that is publicly registered with the top-level DNS servers.
5. Describe how port forwarding (also referred to a service forwarding) allows a remote access client to access a remote access server.
6. Emphasize that if the NAT router is also a NGFW, a reverse proxy can be configured instead of port forwarding. Note that in addition to forwarding remote access requests, reverse proxies interpret all service requests, and can deny access to traffic deemed malicious as a result.
7. Refer to Figure 9-3 and explain that there is another way for a remote access client to gain access to resources on a server within a DMZ by connecting remote access servers directly to a demarc. Note that in this case, the remote access server must have two network interfaces, and explain how the interfaces are configured.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | The design of networks and remote access depends on the needs of the organization and the capabilities of the network hardware implemented. Although the example network structure shown in Figures 9-1 through 9-3 is common to many organizations, it will vary from organization to organization. However, this network structure provides a standard context that you will use when discussing remote access throughout this module. |

1. Mention that Microsoft provides three main remote access technologies that can be used to obtain access to servers in a DMZ from across the Internet. Emphasize that each of these remote access technologies provides its own protocols and supports different authentication and encryption types.
* Virtual private networks (VPNs)
* DirectAccess
* Remote Desktop Services

**Understanding VPNs**

1. Introduce and discuss virtual private networks (VPNs), noting they can be used for remote access.
2. Mention that there are different VPN protocols and authentication types available and RADIUS can be used to provide for centralized VPN authentication, logging, and policies.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | More information regarding VPNs can be found on this website: <https://vpnoverview.com/vpn-information/what-is-a-vpn/>  |

**Using VPNs for Remote Access**

1. Define a virtual private network (VPN) as a remote access technology that provides encryption for data that is sent across the Internet between a remote access client and server. Describe what happens when a remote access client connects to a VPN.
2. Refer to Figure 9-4 to define a VPN tunnel and describe how VPN tunnels work. Explain why the default gateway configured in the VPN network interface on the remote access client is automatically set to 0.0.0.0.
3. Mention that because all IP packets are sent to the remote access server across a VPN, requests for Internet resources from remote access clients are forwarded by the remote access server to the NAT router or NGFW in the organization, before being sent to the Internet. Note that this allows the NAT router or NGFW in an organization to perform malware scanning or restrict access to certain Internet sites for remote access clients.
4. Explain that if remote access clients configure split tunneling in the properties of their VPN network interface, they will be able to access the resources in their organization’s DMZ across the VPN tunnel, but will use the default gateway on their physical network interface to access Internet resources.

**Using VPNs to Protect Network Traffic**

1. Remind students that VPNs can be used to encrypt IP traffic that passes across the Internet between a remote access client and server.
2. Inform your students that VPNs can be used to encrypt IP traffic that passes across the Internet between two routers at different locations in an organization. Refer to Figure 9-5 to illustrate how this works.

**VPN Protocols**

1. Introduce this topic by mentioning that VPN technologies use a specific VPN protocol to tunnel traffic.
2. Point out that when an administrator implements a remote access server using Windows Server 2019, four different VPN protocols are supported.
3. Define and describe the Point-to-Point Tunneling Protocol (PPTP). Mention that it encrypts data using Microsoft Point-to-Point Encryption (MPPE).
4. Define and describe the Layer Two Tunneling Protocol (L2TP). Mention that it provides for tunneling only and relies on IP Security (IPSec) for the encryption of data packets using encryption keys varying in length from 56 to 256 bits.
5. Define and describe Internet Key Exchange version 2 (IKEv2). Mention that it uses 256-bit encryption keys and requires that remote access clients and servers authenticate to each other using an IPSec encryption certificate or preshared key.
6. Define and describe the Secure Socket Tunneling Protocol (SSTP). Mention that it originally used Secure Sockets Layer (SSL) encryption with 128-bit keys. However, modern SSTP implementations use 256-bit keys alongside Transport Layer Security (TLS) encryption. Point out that to use SSTP, the remote access server must contain an HTTPS encryption certificate.
7. Describe the special configuration considerations for a remote access server that is connected to a NAT router or NGFW.
8. Describe the special configuration considerations for a remote access server that connects directly to the demarc.
9. Mention that if the configuration tool for the NAT router, NGFW, or firewall does not allow an administrator to specify the name of each VPN protocol, he or she must instead specify the associated port numbers. Refer to Table 9-1 to review a list of the port numbers and associated transport protocols (TCP or UDP) used for each VPN protocol supported by Windows Server 2019.

|  |  |
| --- | --- |
|  ***Teaching*** ***Tip*** | Point out that in addition to port 1723/TCP, PPTP also requires that an administrator allow for the Generic Routing Encapsulation (GRE) protocol in a port forwarding, reverse proxy, or firewall configuration. GRE is identified by protocol number 47. |

**VPN Authentication**

1. Point out that before a VPN tunnel can be established, the remote access client must first authenticate to the remote access server using credentials.
2. Refer to Table 9-2 and review a summary of the different authentication methods that can be used to protect the credentials as they pass from the remote access client to a Windows Server 2019 remote access server.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Remote access clients and servers will use the most secure authentication method that both computers support. The authentication methods summarized in Table 9-2 are listed in order from least secure (PAP) to most secure (EAP). |

1. Mention that after the remote access server receives credentials from the remote access client, it must validate them before providing remote access.
2. Describe how credentials are validated if the remote access server is joined to an Active Directory domain.

**Using RADIUS**

1. Introduce this topic by mentioning that an administrator can optionally configure a remote access server to forward credentials it receives from a remote access client to a Remote Access Dial-In User Authentication Service (RADIUS) server instead of a domain controller.
2. Introduce and describe the RADIUS protocol. Mention that RADIUS is a protocol designed to centralize authentication and logging for large distributed networks.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Mention that if an administrator configures a remote access server to forward credentials or logging events to a RADIUS server, the remote access server is called a RADIUS client. |

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | To provide centralized authentication and logging, an administrator can configure multiple remote access servers as RADIUS clients that forward credentials and logging events to a single RADIUS server. |

1. Describe how a RADIUS server performs authentication after it receives credentials from a remote access server. Be sure to mention that as part of the process, the RADIUS server checks its remote access policies to ensure that the user meets necessary requirements before allowing the remote access connection and forwarding the Kerberos ticket to the remote access server.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Mention that remote access policies can specify restrictions that must be met prior to obtaining a VPN tunnel, such as time of day, VPN protocol, or authentication method. Additionally, remote access policies can specify restrictions that must be enforced by the remote access server after a VPN connection has been created, such as the maximum time that an idle session can remain connected. |

**Implementing VPNs**

1. Point out that to implement remote access using VPNs in an organization, an administrator must install and configure a remote access server, and optionally configure a RADIUS server to provide for centralized authentication and logging, as well as remote access policies.
2. Mention that an administrator must also configure remote access clients to connect to the remote access server.
3. Explain that to protect traffic between two networks using VPNs, an administrator can configure demand-dial interfaces on the routers in their organization.

**Configuring a Remote Access Server**

1. Emphasize that to configure Windows Server 2019 as a remote access server for VPN access, an administrator must first install the Remote Access server role.
2. Explain that an administrator selects the Remote Access server role in the Add Roles and Features Wizard and progresses through the wizard.
3. Refer to Figure 9-6 and explain the possible choices for role services.
4. Refer to Figure 9-7 and explain how an administrator can configure and manage VPN remote access by clicking Routing and Remote Access from the Tools menu in Server Manager to start the Routing and Remote Access tool.
5. Explain that alternatively, an administrator can open the Routing and Remote Access tool from the final page of the Add Roles and Features Wizard. Mention that to do this, an administrator clicks *Open the Getting Started Wizard*, and then clicks *Deploy VPN only*.
6. Explain how an administrator starts the Routing and Remote Access Server Setup Wizard using the Routing and Remote Access tool following the installation of the Remote Access server role.
7. Refer to Figure 9-8 and explain how an administrator chooses the type of remote access server configuration.
8. Refer to Figure 9-9 to illustrate how an administrator continues through the Routing and Remote Access Server Setup Wizard and manually selects the services that he or she might need.
9. Explain that at this point, an administrator clicks Next and then clicks Finish to complete the wizard. Note that an administrator can then click Start service to start their remote access services.
10. Emphasize that after an administrator has completed the Routing and Remote Access Server Setup Wizard, he or she may need to perform additional remote access server configuration tasks, depending on their needs.
11. Mention that one additional task that may need to be completed is configuring VPN protocol connections. Explain that remote access servers can use one or more VPN protocols to provide VPN access to many different remote access clients at the same time. Also, mention that by default, after a custom configuration for VPN access is performed using the Routing and Remote Access Server Setup Wizard, two simultaneous VPN connections are allowed for each VPN protocol.
12. Refer to Figure 9-7 and explain how to increase the number of connections for each VPN protocol to match the number of remote access clients configured to use the protocol, an explain how to disable any VPN protocols that are not used.
13. Mention that a second additional task that may need to be completed is to specify a VPN IP configuration. Remind students that the virtual network interface at each end of a VPN tunnel must contain an IP address. Mention that these IP addresses can be obtained from a DHCP server in the DMZ using a DHCP relay agent that is configured on the remote access server, or configured manually in remote access server properties.
14. Refer to Figure 9-7 again and explain that DHCP relay agents are located under the IPv4 or IPv6 sections in the Routing and Remote Access tool if the remote access server is also configured as a router.
15. Refer to Figure 9-11 and Figure 9-12 to illustrate and explain how to configure relay agents and their properties on the remote access server.
16. Refer to Figure 9-13 and Figure 9-14. Explain how to manually configure a DHCP relay agent.
17. Mention that a third additional task that may need to be completed is to configure security options and authentication methods. Note that these options are specific to the VPN protocol used.
18. Explain that to configure these options, an administrator highlights the Security tab in Figure 9-14 and specifies the appropriate options, as shown in Figure 9-15. Explain the options available in Figure 9-15.
19. Explain that by default, only EAP and MS-CHAP v2 authentication methods are allowed by the remote access server. Refer to Figure 9-16 and explain that an administrator can click the Authentication Methods button to provide additional or fewer authentication methods.
20. Mention that a fourth additional task that may need to be completed is to set dial-in permissions. Explain that VPN remote access is only granted if the properties of the user account used during authentication allow dial-in permission.
21. Refer to Figure 9-17 and explain how to reach and modify the dial-in properties for a specific user account.

**Configuring RADIUS**

1. Introduce this topic by explaining that to use a Windows Server 2019 system as a RADIUS server, an administrator must first install the Network Policy and Access Services role.
2. Refer to Figure 9-18 and explain that after this role has been installed, an administrator can use the Network Policy Server tool to configure the RADIUS server.
3. Explain how to start the Network Policy Server tool.
4. Mention that if the RADIUS server is joined to an Active Directory domain, it will authenticate remote access user accounts using Active Directory instead of the local SAM database. Refer to Figure 9-18 again and explain how to allow this functionality.
5. Introduce the topic of configuring remote access policies by explaining that policies are used to configure the functionality of a RADIUS server.
6. Refer to Figurer 9-18 and describe the two folders under the Policies section.
* Connection Request Policies
* Network Policies
1. Refer to Figure 9-18 through Figure 9-24. Explain how to create a new remote access policy.
2. Introduce the topic of configuring logging by mentioning that RADIUS servers log the details of each remote access connection to a text file. Review the naming convention of the text file.
3. Refer to Figure 9-18 again, and explain that an administrator can highlight the Accounting folder, then click one of the following hyperlinks to modify the logging configuration. Review the items that can be configured.
4. Introduce the topic of configuring remote access servers to use RADIUS. Mention that remote access servers do not forward requests to a RADIUS server until they are configured as a RADIUS client.
5. Emphasize that RADIUS servers only respond to RADIUS clients that contain the same shared secret (password) in their configuration. Point out that this means an administrator must add an entry for each RADIUS client on his or her RADIUS server that includes a shared secret, and configure each RADIUS client with the same shared secret.
6. Refer to Figure 9-18 and Figure 9-25. Explain how to add a RADIUS client in the Network Policy Server tool.
7. Refer to Figure 9-15 and Figure 9-26 through Figure 9-27. Explain how to configure a remote access server as a RADIUS client.

**Connecting to a VPN Server**

1. Introduce this topic by mentioning that after an administrator has configured a remote access server for VPN remote access, remote access clients can create a VPN connection.
2. Refer to Figure 9-28 and explain how to create a VPN connection on a Windows 10 or Windows Server 2019 system. Note that when an administrator clicks Save in Figure 9-28, a new VPN connection is created in the Settings window.
3. Explain that to connect to the VPN, click the VPN connection, click Connect, and supply user credentials, if necessary.
4. Explain how to close a remote access connection.
5. Explain how to view VPN connections in the Routing and Remote Access tool on the remote access server.
6. Explain how to view remote access statistics.

**Creating a Demand-Dial Interface**

1. Introduce this topic by mentioning that if a router is a Windows Server 2019 system, an administrator can create a demand-dial interface in the Routing and Remote Access tool to protect traffic that is passed to another network in the organization.
2. Refer back to Figure 9-5 to illustrate the idea of wanting to configure a demand-dial interface on the Toronto NAT router that creates an IKEv2 VPN to the Chicago NAT router when traffic needs to be routed to the Chicago DMZ (172.17.0.0/24 network).
3. Refer to Figure 9-7. Explain how to do this by right-clicking the Network Interfaces folder and clicking New Demand-dial Interface to start the Demand-Dial Interface Wizard.
4. Refer to Figures 9-29 through 9-35. Explain how to use the wizard to create the demand-dial interfaces for this desired setup.

**Quick Quiz 1**

1. Which last mile technology used to connect to an ISP uses a telephone network?
2. digital subscriber line (DSL)
3. cable broadband
4. Gigabit Passive Optical Network (GPON)
5. long-range Wi-Fi

Answer: a. digital subscriber line (DSL)

1. Which VPN protocol uses 256-bit keys alongside Transport Layer Security (TLS) encryption?
	1. Point-to-Point Tunneling Protocol (PPTP)
	2. Layer Two Tunneling Protocol (L2TP)
	3. Internet Key Exchange version 2 (IKev2)
	4. Secure Socket Tunneling Protocol (SSTP)

Answer: d. Secure Socket Tunneling Protocol (SSTP)

1. \_\_\_\_\_\_\_\_\_\_ is a protocol designed to centralize authentication and logging for large distributed networks.
	1. DirectAccess
	2. VPN
	3. RADIUS
	4. CHAP

Answer: c. RADIUS

1. True or False: RADIUS servers only respond to RADIUS clients that contain the same shared secret (password) in their configuration.

Answer: True

**Understanding DirectAccess**

1. Introduce this section by mentioning a disadvantage of VPNs, namely remote users must manually initiate a VPN connection each time they wish to connect to the resources in their organization.
2. Mention that for organizations deploying laptop computers that are joined to an Active Directory domain, secure remote access for these computers can be automated using DirectAccess.
3. Point out that the advantage is that when laptop computers connect to a network outside of the organization, DirectAccess automatically initiates an IPSec tunnel that functions like a VPN to provide remote access to the organization DMZ.
4. Mention that to determine whether they are located on a network outside the organization, each remote access client that participates in DirectAccess contains a Network Connectivity Assistant service that probes a network location server using HTTPS each time their network interface is activated on a network.
5. Point out that if the remote access client determines that it is on a network outside of the organization, it automatically creates an IPSec tunnel to the remote access server after prompting the user to log into the Active Directory domain, if necessary.

**Implementing DirectAccess**

1. Emphasize that to implement DirectAccess, an administrator must first install the Remote Access server role on the Windows Server 2019 system that will function as the remote access server and network location server.
2. Refer to Figure 9-6 and mention that an administrator must select the DirectAccess and VPN (RAS) role service during the Add Roles and Features Wizard.
3. Refer to Figure 9-36. Mention that an administrator can configure and manage DirectAccess by clicking Remote Access Management from the Tools menu in Server Manager to start the Remote Access Management Console.
4. Point out that the Dashboard section is shown in the Remote Access Management Console by default and displays the status of remote access services, as well as VPN and DirectAccess client statistics.
5. Explain how to view detailed information regarding remote access services.
6. Mention that to configure DirectAccess, an administrator can highlight VPN under the Configuration section in the navigation pane and click Enable DirectAccess in the Tasks pane to start the Enable DirectAccess Wizard.
7. Refer to Figure 9-37. Explain how to enter the various DirectAccess client configuration options.
8. Refer to Figure 9-38. Explain how to enter the DirectAccess network topology options.
9. Refer to Figure 9-39. Note that after an administrator specifies the correct network topology options, he or she is prompted to configure DirectAccess remote access clients with a list of domain name suffixes.
10. Mention that Group Policy is used to automatically configure the remote access clients and servers in the organization for DirectAccess. Refer to Figure 9-40. Explain how to modify the default names for the Group Policy objects that will be created to provide DirectAccess configuration for clients and servers in a domain.
11. Refer to 9-40 again and explain that an administrator can also use an existing Group Policy object to store a DirectAccess client or server configuration by clicking the associated Browse button and selecting the desired Group Policy object.
12. When an administrator clicks Next in Figure 9-40, he or she can click Finish to configure their server as a DirectAccess remote access server and network location server, and ensure that the associated client computers in their domain are enabled for DirectAccess.
13. Refer to Figure 9-41 and explain how to modify a DirectAccess configuration or specify configuration options that were not available in the Enable DirectAccess Wizard.
14. Note that the Remote Access Setup pane shown in Figure 9-41 is divided into four steps that represent the different components of DirectAccess. Review each component.

**Understanding Remote Desktop**

1. Introduce this section by mentioning that Remote Desktop uses a different method to achieve remote access compared to VPNs and DirectAccess.
2. Emphasize that instead of relaying network traffic through an encrypted tunnel to a DMZ, remote access clients use a Remote Desktop app to log into a remote access server to obtain a graphical desktop session on the remote access server itself (called session-based desktop deployment), or a graphical desktop session from a Hyper-V virtual machine running on the remote access server (called virtual machine-based desktop deployment).
3. Mention that after a remote access client obtains a graphical desktop session, they can run programs on the remote access server and access resources on the DMZ network to which the remote access server is connected.
4. Explain how the Remote Desktop app uses Remote Desktop Protocol (RDP) to transfer desktop graphics, keystrokes, and mouse movements to and from the remote access server.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | There are Remote Desktop apps available for Windows, macOS, Linux, UNIX, Android, and iOS remote access clients. The Remote Desktop app available by default on Windows systems is called Remote Desktop Connection. |

1. Explain that the collection of services that provide for remote access using Remote Desktop on Windows Server 2019 is called Remote Desktop Services, and can be obtained by installing the Remote Desktop Services server role. Refer to Table 9-3. Summarize each of these services as well as the ports and transport protocols that they use.
2. Emphasize that at minimum, an administrator must install either Remote Desktop Session Host or Remote Desktop Virtualization Host, as well as Remote Desktop Licensing on a remote access server to provide for remote access using Remote Desktop.
3. Note that when configuring firewall exceptions, port forwarding, or reverse proxy to the remote access server, an administrator must specify the RDP and HTTPS protocols, or the port numbers listed in Table 9-3 for Remote Desktop Session Host or Remote Desktop Virtualization Host.
4. Note that to provide access to RemoteApp, as well as HTTPS encryption for RDP traffic, an administrator can optionally install Remote Desktop Web Access and Remote Desktop Gateway on the same remote access server, without having to modify the firewall, port forwarding, or reverse proxy configuration.
5. Mention that if an administrator deploys multiple Remote Desktop Session Host or Remote Desktop Virtualization Host remote access servers in their DMZ, then the administrator could install a single server that contains the Remote Desktop Connection Broker to distribute RDP requests across all of the remote access servers. Explain how the remote access clients will connect in this case. Describe the services that the server hosting the Remote Desktop Connection Broker can host.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Many server administrators install the Remote Desktop Connection Broker when there is only one remote access server that contains the Remote Desktop Session Host or Remote Desktop Virtualization Host role service. If additional servers are installed with the Remote Desktop Session Host or Remote Desktop Virtualization Host role service afterwards, they are automatically linked with the Remote Desktop Connection Broker, and no additional firewall, port forwarding, or reverse proxy configuration is necessary. |

**Implementing Remote Desktop Services**

1. Mention that to implement Remote Desktop Services, an administrator must install and configure Remote Desktop Services, and create and configure collections that include remote access servers.
2. Note that afterwards, an administrator must ensure that users can connect to Remote Desktop sessions, as well as any programs made available using RemoteApp.

**Installing Remote Desktop Services**

1. Emphasize that to install Remote Desktop Services, an administrator must install the Remote Desktop Services server role on a Windows Server 2019 system that will function as the remote access server.
2. Refer to Figure 9-42. Explain that when an administrator selects the Remote Desktop Services server role in the Add Roles and Features Wizard and progresses through the wizard, he or she is prompted to choose the role services that they wish to install.
3. Mention that at the end of the Add Roles and Features Wizard, the administrator must reboot the server before continuing the installation of Remote Desktop Services.
4. Refer to Figure 9-43. Explain that after the server has rebooted, the administrator must start the Add Roles and Features Wizard again, but instead select *Remote Desktop Services installation* at the Select installation type page.
5. Refer to Figure 9-44. Explain that the administrator must now select deployment options.
6. Refer to Figure 9-45. Explain that the administrator must now choose whether to configure virtual machine-based desktop deployment or session-based desktop deployment. Note that the option selected in Figure 9-45 matches the Remote Desktop Session Host role service installed earlier.
7. Refer to Figure 9-46 and explain that a summary of the role services that will be installed is displayed. Note that this summary should match the role service that was selected earlier, with the exception of Remote Desktop Licensing, which is configured afterward.
8. Refer to Figure 9-47 and explain that the administrator must now choose a server that hosts the Remote Desktop Connection Broker.
9. Refer to Figure 9-48 and explain that an administrator can specify a Remote Desktop Web Access server. In this case, explain that a Remote Desktop Web Access role service on the local server alongside the Remote Desktop Connection Broker is being installed.
10. Refer to Figure 9-49 and explain that an administrator now specifies one or more remote access servers that host the Remote Desktop Session Host role service.
11. Explain that these remote access servers are linked to the Remote Desktop Connection Broker server identified earlier to ensure that remote access clients can access them. They will also be linked to the Remote Desktop Web Access server identified earlier, to allow access to RemoteApp and Remote Desktop sessions using a Web browser.
12. Finally, explain that an administrator can click Deploy to apply the selections. The administrator must then reboot the server to complete the installation of Remote Desktop Services.

**Configuring Remote Desktop Services**

1. Refer to Figure 9-50. Explain that after an administrator has rebooted the server, he or she can configure and manage Remote Desktop Services by highlighting Remote Desktop Services in the navigation pane of Server Manager.
2. Refer to Figure 9-50 again, and describe the Overview section.
3. Explain how an administrator could install the RD Gateway role service now if it was not selected at installation time.
4. Point out that although the Remote Desktop Licensing role service was installed alongside the other role services, it is not configured by default.
5. Refer to Figure 9-51 and Figure 9-52. Explain how to configure the Remote Desktop Licensing role service.
6. Remind students that the Remote Desktop Web Access and Remote Desktop Gateway role services require that an administrator obtain and install an HTTPS encryption certificate. Refer to Figure 9-52 and explain how to configure an existing HTTPS encryption certificate for use with these role services.
7. Mention that over time, an administrator may find that a single Remote Desktop Session Host server is not adequate to support the number of Remote Desktop sessions. Explain how to add additional remote access servers to a configuration that has the Remote Desktop Session Host role service installed.

**Configuring Collections**

1. Introduce and define a collection, noting that after an administrator has configured the appropriate role services, he or she must create one or more collections that contain remote access servers.
2. Mention that each collection allows specific groups of users in an Active Directory domain to access Remote Desktop, and provides configuration for RemoteApp and Remote Desktop sessions.
3. Refer to Figure 9-50 and Figure 9-53 through Figure 9-56. Explain how to create a new collection for session-based desktop deployment.
4. Mention that if a collection consists of multiple remote access servers, the Remote Desktop Connection Broker may connect a user to a different remote access server when that user requests a new Remote Desktop session.
5. Note that after creating a collection, an administrator can use Server Manger to configure and manage Remote Desktop for the remote access servers in the collection. Refer to Figure 9-57 and explain how to do this.
6. Refer to Figure 9-57 again and explain how to modify the options that were configured when creating the collection, as well as configure session limits, load balancing settings for remote access servers, security settings, and remote access client settings (including the ability to access local volumes and printers).
7. Explain how to add additional remote access servers to a collection.
8. Refer to Figure 9-57 and describe function of the CONNECTIONS pane.

**Connecting to Remote Desktop Services**

1. Refer to Figure 9-58 and explain how to obtain a Remote Desktop session to a remote access server on a Windows remote access client.
2. Point out that the FQDN or IP address that is specified in the Computer text box in Figure 9-58 should match the server that hosts the Remote Desktop Session Host, or the server that hosts Remote Desktop Connection Broker, if used.
3. Explain that if an administrator configured the Remote Desktop Web Access role service, he or she can also obtain a Remote Desktop session or access RemoteApp programs by navigating to https://*server*/RdWeb in a Web browser, where *server* is the FQDN of the Remote Desktop Web Access server.
4. Mention that after an administrator logs into this website using domain credentials, he or she can select options to connect to a Remote Desktop session in the Web browser, or download a file that automatically connects to a Remote Desktop session using the Remote Desktop Connection app, as well as access or create Start menu shortcuts for one or more RemoteApp programs that are available on the remote access server.
5. Mention that an administrator can open the RemoteApp and Desktop Connections tool in Control Panel and click *Access RemoteApp and desktops* to perform the same actions.

**Quick Quiz 2**

1. True or False: Remote Desktop, VPNs, and DirectAccess all use the same method to achieve remote access.

Answer: False

1. Which Remote Desktop services server role allows remote access users the ability to reconnect to a disconnected remote desktop session, and balances requests for remote desktop sessions across servers?
	1. Remote Desktop Connection Broker
	2. Remote Desktop Session Host
	3. Remote Desktop Virtualization Host
	4. Remote Desktop Web Access

Answer: a. Remote Desktop Connection Broker

1. \_\_\_\_\_\_\_\_\_\_ contain remote access servers.
	1. Canisters
	2. Containers
	3. Collections
	4. Connections

Answer: c. Collections

1. The Remote Desktop app available by default on Windows systems is called \_\_\_\_\_\_\_\_\_\_.
	1. Desktop Control
	2. Remote Desktop Connection
	3. ClientApp
	4. RemoteAPP

Answer: b. Remote Desktop Connection

# **Class Discussion Topics**

1. What is the main purpose of using Secure Sockets Layer (SSL)?
2. What are the advantages and disadvantages of using Remote Desktop instead of a VPN?

# **Additional Projects**

1. Create a proposal for a VPN installation in a local small business that conducts most of its transactions via the Internet.
2. Ask your students to read the article about SSTP (Secure Socket Tunneling Protocol) at the following site: <https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp>. Have them write a report summarizing its most important points.

# **Additional Resources**

1. How a VPN (Virtual Private Network) Works

<https://computer.howstuffworks.com/vpn3.htm>

1. Understanding the Remote Desktop Protocol (RDP)

<https://support.microsoft.com/en-us/help/186607/understanding-the-remote-desktop-protocol-rdp>

1. Microsoft DirectAccess Overview

<http://techgenix.com/microsoft-directaccess-overview/>

1. Point to Point Protocol (PPP)

<https://www.tutorialspoint.com/point-to-point-protocol-ppp>

1. Overview of Remote Desktop Licensing

[https://technet.microsoft.com/en-us/library/cc725933(v=ws.11).aspx](https://technet.microsoft.com/en-us/library/cc725933%28v%3Dws.11%29.aspx)

**Key Terms**

* **cable broadband** A last mile technology that uses a television cable network.
* **collection** An entity that contains remote access servers. Each collection allows specific groups of users in your Active Directory domain access to Remote Desktop, as well as provides configuration for RemoteApp and Remote Desktop sessions.
* **constraint** Asection of a remote access policy that contains characteristics that must be met for remote access.
* **demand-dial interface** An interface that automatically creates a VPN connection to a NAT router when it receives traffic destined for a network.
* **demarc** The point in a network infrastructure that connects to the ISP using a last mile technology.
* **demarcation point** The point in a network infrastructure that connects to the ISP using a last mile technology.
* **dial-in permission** Permission to access a network remotely.
* **dial-up remote access** Access used before Internet access became common. In this case, remote access clients used a dial-up modem to dial the telephone number of a modem bank that was connected to a remote access server in the organization.
* **digital subscriber line (DSL)** A last mile technology that uses a telephone network.
* **DirectAccess** A remote access technology that automatically creates IPSec tunnels to a remote access server when remote access clients are outside of the organization.
* **DirectAccess Connectivity Assistant** A tool administrators use to improve an enterprise's DirectAccess connection.
* **Generic Routing Encapsulation (GRE)** A protocol that provides a private, secure path for transporting packets through an otherwise public network by encapsulating (or tunneling) the packets. GRE tunneling is accomplished through tunnel endpoints that encapsulate or de-encapsulate traffic.
* **Gigabit Passive Optical Network (GPON)** A last mile technology that uses fiber optic cable.
* **Internet Key Exchange version 2 (IKEv2)** An enhancement to IPSec that provides VPN tunneling with faster speeds compared to L2TP. It uses 256-bit encryption keys and requires that remote access clients and servers authenticate to each other using an IPSec encryption certificate or preshared key.
* **IP Security (IPSec)** A secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.
* **last mile technology** A technology that spans the “last mile” between the Internet and the organization.
* **Layer Two Tunneling Protocol (L2TP)** A VPN protocol developed by Microsoft and Cisco. It provides for tunneling only and relies on IP Security (IPSec) for the encryption of data packets using encryption keys varying in length from 56 to 256 bits. To participate in an L2TP VPN, the remote access client and server must authenticate to each other. To do this, you can configure the same preshared key (password) or install an IPSec encryption certificate on both the remote access client and server.
* **long-range Wi-Fi** A last mile technology that uses radio wireless, often using wireless transmitters positioned in a line of sight.
* **Microsoft Point-to-Point Encryption (MPPE)** An encryption technique used in PPTP. Although MPPE supports encryption keys varying in length from 40 to 128 bits, modern Windows operating systems such as Windows 10 and Windows Server 2019 contain a registry key that prevents the use of MPPE keys less than 128 bits by default.
* **Network Connectivity Assistant** A DirectAccess service that probes a network location server using HTTPS each time a client network interface is activated on a network to determine whether the client is located on a network outside the organization.
* **network location server** A website that is used to detect whether DirectAccess clients are located in the corporate network. Clients in the corporate network do not use DirectAccess to reach internal resources, but instead, they connect directly.
* **Network Policy and Access Services** A component of Windows Server. It replaces the Internet Authentication Service (IAS) from Windows Server 2003. NPAS helps an administrator safeguard the health and security of a network.
* **Network Policy Server** NPS is installed when you install the Network Policy and Access Services (NPAS) feature in Windows Server 2016 and Server 2019. NPS allows you to create and enforce organization-wide network access policies for connection request authentication and authorization.
* **Next Generation Firewall (NGFW) A** network security device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.
* **overlay network** The virtual network that is created by a VPN.
* **Point-to-Point Protocol** A data link layer communications protocol between two routers directly without any host or any other networking in between. It can provide connection authentication, transmission encryption, and compression.
* **Point-to-Point Protocol over Ethernet (PPPoE)** A network protocol for encapsulating PPP frames inside Ethernet frames.
* **Point-to-Point Tunneling Protocol (PPTP)** One of the oldest and most widely supported VPN protocols. It was developed by a consortium of vendors including Microsoft and encrypts data using Microsoft Point-to-Point Encryption (MPPE). Although MPPE supports encryption keys varying in length from 40 to 128 bits, modern Windows operating systems such as Windows 10 and Windows Server 2019 contain a registry key that prevents the use of MPPE keys less than 128 bits by default.
* **port forwarding** An application of network address translation that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.
* **RADIUS client** A RADIUS-enabled device at the network perimeter that enforces access control for users attempting to access network resources.
* **remote access** The process of connecting to server resources within a DMZ from a location outside of the organization hosting the DMZ.
* **Remote Access** A service used to access a network remotely.
* **remote access client** An Internet user that requests access to a server in the DMZ.
* **Remote Access Dial-In User Authentication Service (RADIUS)** A client/server protocol and software that enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
* **Remote Access Management Console** Tool used to configure and manage DirectAccess.
* **remote access policy** A policy that contains conditions that must be met for the policy to apply to the remote access client.
* **remote access server** A server thataccepts requests from remote access clients on the Internet.
* **Remote Desktop** A remote access technology that uses a different method to achieve remote access compared to VPNs and DirectAccess. Instead of relaying network traffic through an encrypted tunnel to a DMZ, remote access clients use a Remote Desktop app to log into a remote access server to obtain a graphical desktop session on the remote access server itself (called session-based desktop deployment), or a graphical desktop session from a Hyper-V virtual machine running on the remote access server (called virtual machine-based desktop deployment).
* **Remote Desktop app** An app used by remote access clients to log into a remote access server to obtain a graphical desktop session on the remote access server itself.
* **Remote Desktop Connection** The default Remote Desktop app, available by default on Windows systems.
* **Remote Desktop Protocol (RDP)** A proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
* **Remote Desktop Services** One of the components of Microsoft Windows that allows a user to take control of a remote computer or virtual machine over a network connection.
* **RemoteApp** A virtual application solution that allows users to run Windows-based applications regardless of what operating system they are using. It allows users to launch virtual applications from a server that appear on their computer as if they are installed locally, but in reality are running on a remote server.
* **RemoteApp and Desktop Connections** A tool that helps in taking control of remote Windows computers and troubleshooting them remotely.
* **reverse proxy** A type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client, appearing as if they originated from the proxy server itself.
* **Routing and Remote Access** A Microsoft API and server software that make it possible to create applications to administer the routing and remote access service capabilities of the operating system to function as a network router. Developers can also use RRAS to implement routing protocols.
* **Secure Socket Tunneling Protocol (SSTP)** A VPN technology that tunnels data through HTTPS packets on a network. It originally used Secure Sockets Layer (SSL) encryption with 128-bit keys. However, modern SSTP implementations use 256-bit keys alongside Transport Layer Security (TLS) encryption. To use SSTP, the remote access server must contain an HTTPS encryption certificate.
* **Secure Sockets Layer (SSL)** A networking protocol designed for securing connections between Web clients and Web servers over an insecure network, such as the Internet. After being formally introduced in 1995, SSL made it possible for a Web server to securely enable online transactions between consumers and businesses. Due to numerous protocol and implementation flaws and vulnerabilities, SSL was deprecated for use on the Internet by the Internet Engineering Task Force (IETF) in 2015 and has been replaced by the Transport Layer Security (TLS) protocol.
* **service forwarding** Allows requests for a particular port or service to be forwarded to an internal server in the DMZ.
* **session-based desktop deployment** An individual session running inside a server operating system on either a virtual machine or a physical server. There can be multiple user sessions per virtual/physical machine; i.e., each virtual/physical machine is shared by multiple users.
* **split tunneling** A concept that allows a user to access dissimilar security domains like a public network and a local LAN or WAN at the same time, using the same or different network connections.
* **Transport Layer Security (TLS)** A protocol used to provide privacy and data integrity between two or more communicating computer applications.
* **virtual machine-based desktop deployment** An individual virtual machine running a desktop operating system. Each user connects to their own virtual desktop client system.
* **virtual private networks (VPNs)** Networks thatextend a private network across a public network and enable users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
* **VPN protocol** A set of rules that are used to negotiate a connection between the VPN client and the VPN server. At the moment, these are the VPN protocols you are most likely to see being used by VPN providers: PPTP, SSTP, and L2TP/IPSec.
* **VPN tunnel** An encrypted link between your computer or mobile device and an outside network. A VPN tunnel—short for virtual private network tunnel—can provide a way to cloak some of your online activity.