

19-1 Securing Workstations and IoT Devices on a Network

Core 2 Objectives

- 1.4
Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
- 1.6
Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- 2.5
Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- 2.7
Explain common methods for securing mobile and embedded devices.
- 2.10
Given a scenario, install and configure browsers and relevant security settings.
- 4.9
Given a scenario, use remote access technologies.

In this section of the module, we focus on securing a workstation that is connected to a local network. You learn how to secure Windows Microsoft Edge and other browsers, how to set up a VPN connection so a computer can securely connect to resources on a remote network, and how to configure a personal firewall for optimum security. You also learn about securing IoT devices connected to the Internet.

19-1a Secure a Browser

Core 2 Objectives

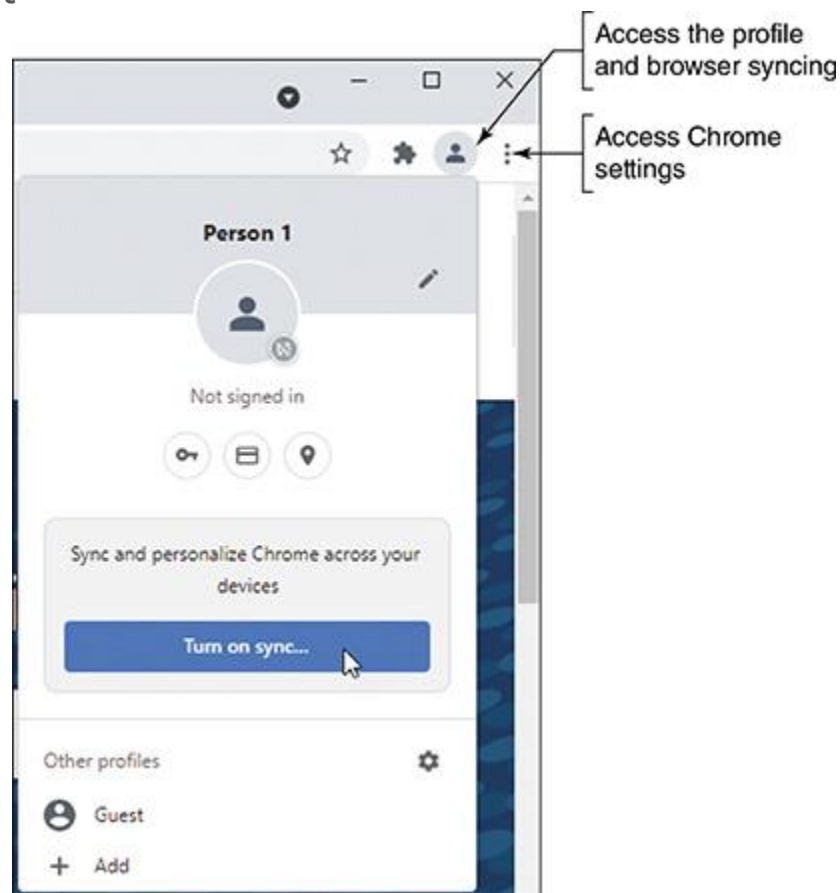
- 1.4
Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
- 2.10
Given a scenario, install and configure browsers and relevant security settings.
In the discussion about securing browsers that follows, we show examples of either Google Chrome, currently the most popular browser, or Microsoft Edge, the default browser in Windows 10/11. However, know that each

browser supports all the functions listed, as do most popular browsers. Do the following to secure Chrome or Edge browsers:

- **Sign in to a browser and sync data across devices.** Browser syncing is a service offered by Google, Microsoft, and other browser developers to sync browser settings and data across each installation of the browser on multiple devices. For Google Chrome, in the Chrome browser, click the profile icon in the upper-right corner (see [Figure 19-1](#)). When you click **Turn on sync**, you will be prompted to sign in to your Google account.

Figure 19-1

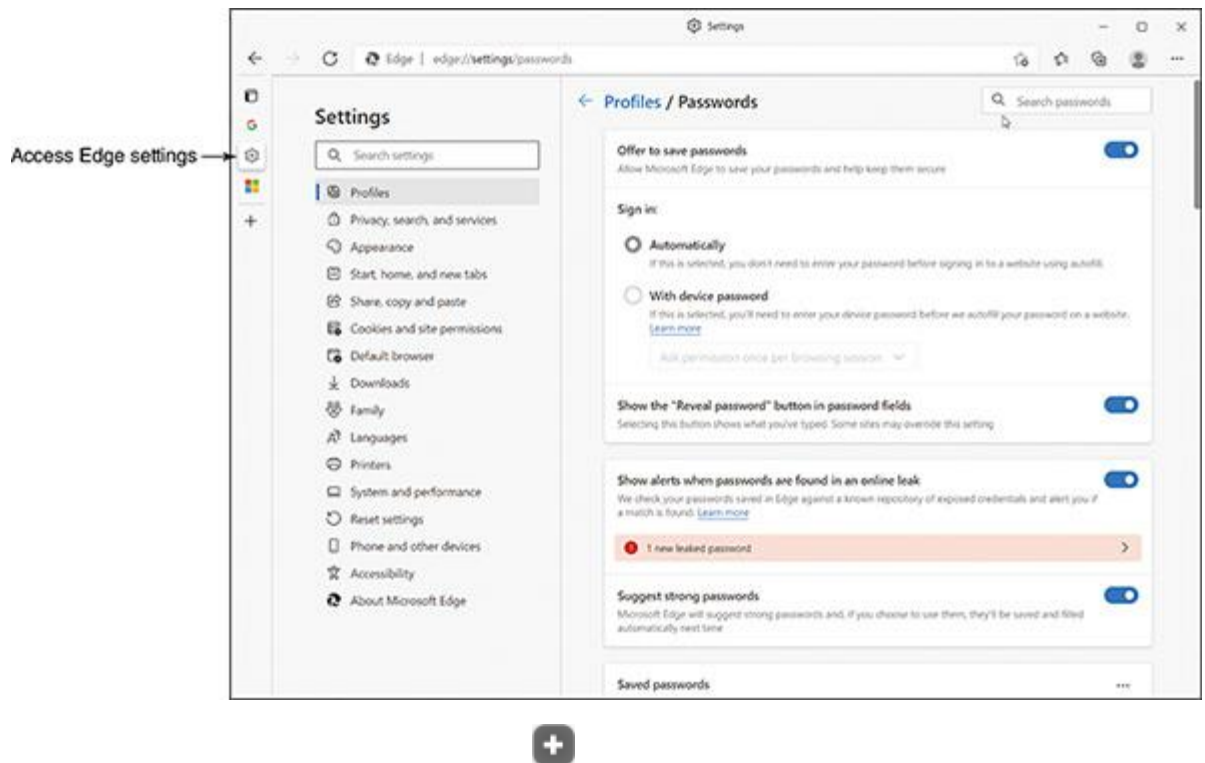
To turn on browser syncing, you must sign in to your Google account



For Edge syncing, go to Edge settings by clicking the settings clog in the left panel of the Edge window (see [Figure 19-2](#)). Select **Profiles**, and sign in to the browser. Edge will ask if you want to sync across all your signed-in devices.

Figure 19-2

Use Microsoft Edge settings to manage Edge profile settings, including passwords



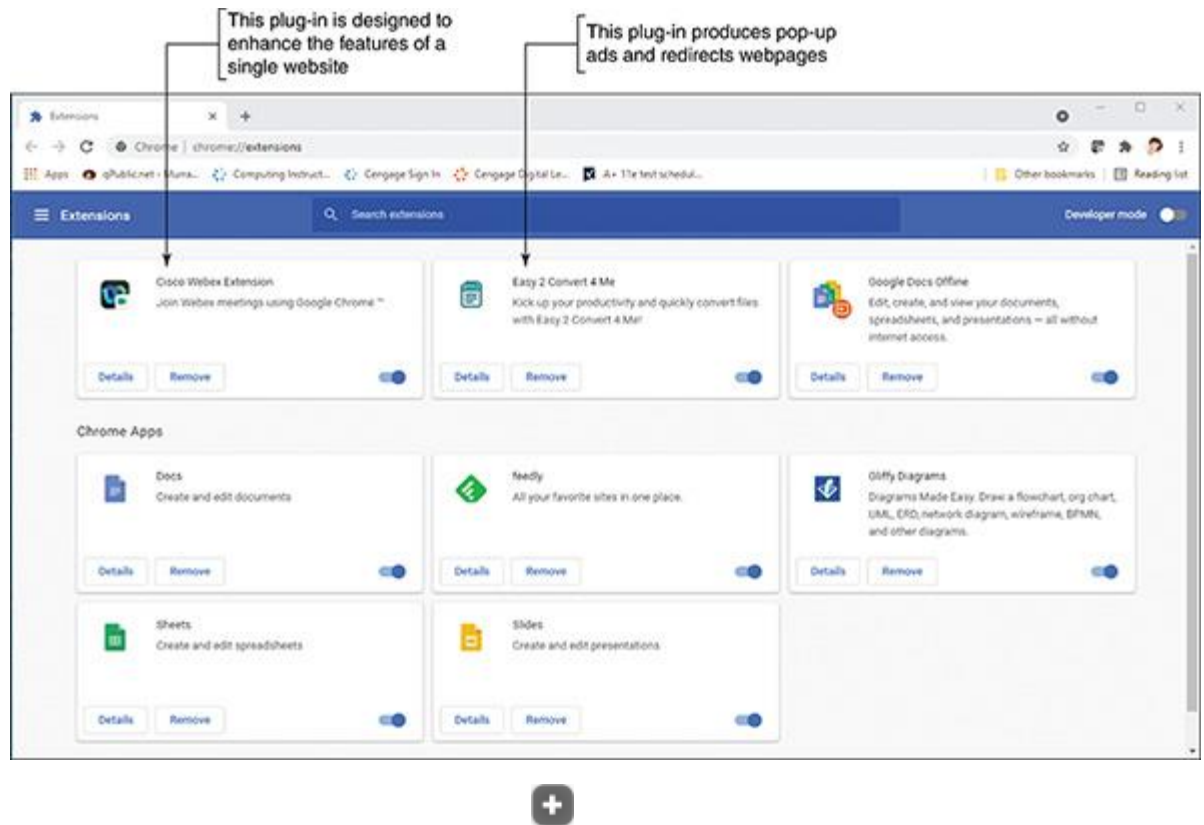
Note 1

Although browser syncing is a convenience and might be appropriate in some situations, best practice for security is to not sign in to a browser and not turn on browser syncing.

- **Manage extensions and plug-ins.** Browser **plug-ins** and **extensions** are small programs that install in a browser to change the way the browser functions or to enhance the features of a single website, such as the Cisco Webex Extension shown in [Figure 19-3](#). A user might unintentionally install an extension or plug-in into their browser. For example, the Easy 2 Convert 4 Me plug-in shown in [Figure 19-3](#) was accidentally installed in Google Chrome and works to display pop-up ads and redirect webpages. To remove the extension, go to Chrome settings by clicking the three-dot menu icon in the upper-right corner of the Chrome window (as shown in [Figure 19-1](#)). In settings, click **Extensions** in the left pane. A list of extensions appears, as shown in [Figure 19-3](#). Click **Remove** in the extensions box to delete it.

Figure 19-3

Manage extensions installed in Google Chrome

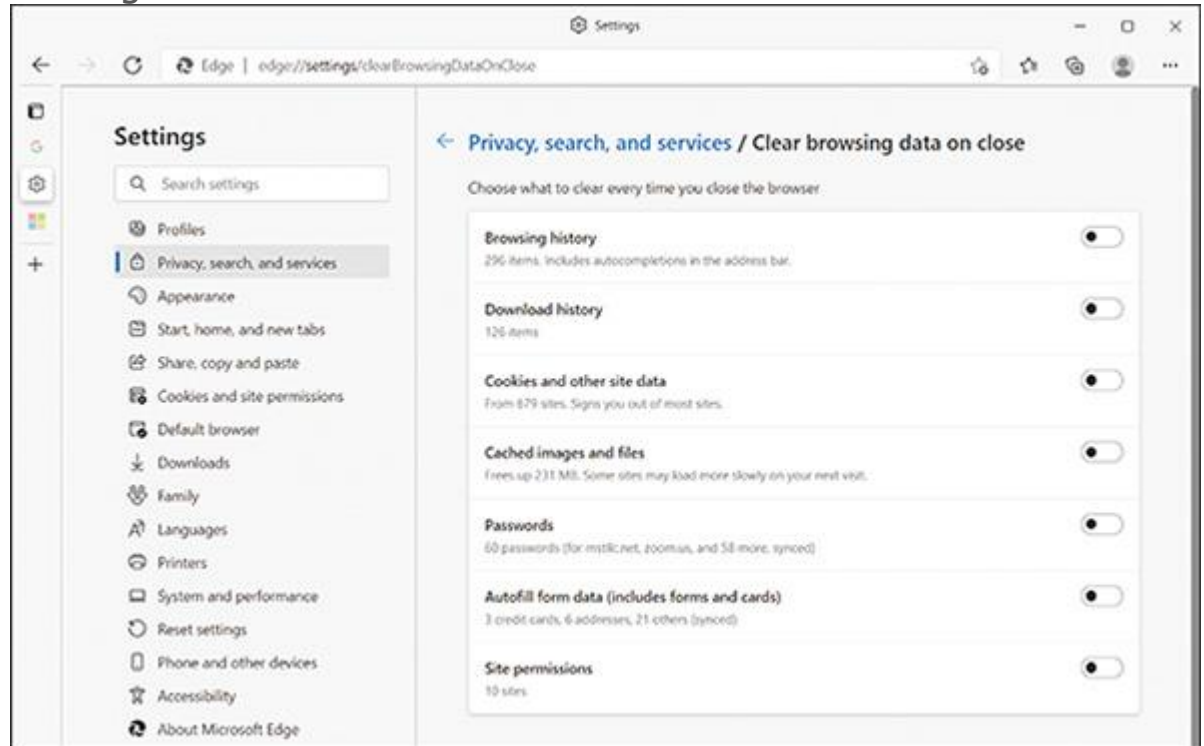


Before installing an extension or plug-in, verify it comes from a trusted source. Read reviews about it, and install it only from the trusted source website, not from other untrusted sources on the web that might have altered the original software or embedded malware in the download.

- **Password manager.** To control how Edge manages passwords, in Edge settings, select **Profiles** and **Passwords**. (Refer back to [Figure 19-2](#).) In the Passwords pane you can turn on or off saving passwords, decide how passwords are managed, and copy, edit, or delete passwords saved by Edge.
- **Pop-up blocker and ad blockers.** In Edge settings, select **Cookies and site permissions** and then **Ads or Pop-ups and redirects** to turn on or off pop-ups, redirects, and intrusive or misleading ads.
- **Clear the cache and all browsing data.** In Edge settings, select **Privacy, search, and services**. Use the Tracking prevention area on this page to manage trackers used by Microsoft and other websites that collect and use information about your browsing habits. In the *Clear browsing data* area of the page, you can choose to clear your browsing data at any time. Select **Choose what to clear every time you close the browser** to see the page shown in [Figure 19-4](#), where you can decide to clear cached images and files and all other browser data each time you close the browser. Clearing all data about you each time you close the browser is a suggested best practice to secure a browser.

Figure 19-4

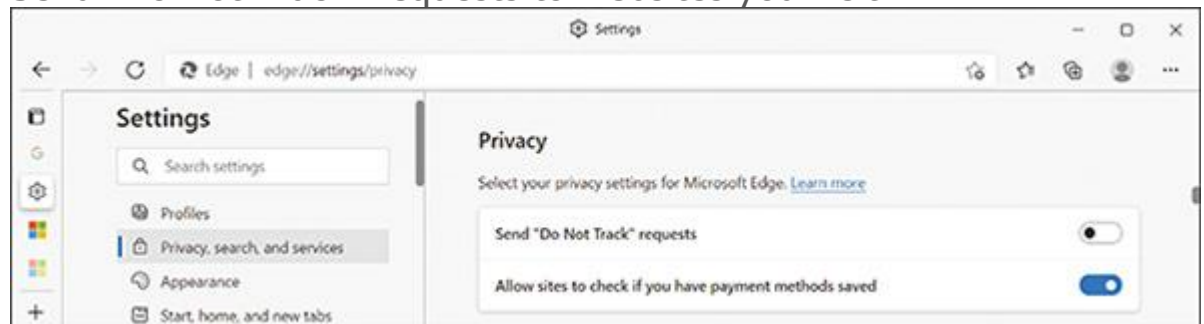
Configure Edge to clear all browsing data each time you close the Edge browser



- **Privacy browsing.** In Edge settings, select **Privacy, search, and services** and use options in the Privacy area (see [Figure 19-5](#)) to send “Do Not Track” requests to websites you visit. Microsoft and Google say that even though you might send this request to a website, it does not guarantee that the website will honor the request.

Figure 19-5

Send “Do Not Track” requests to websites you visit

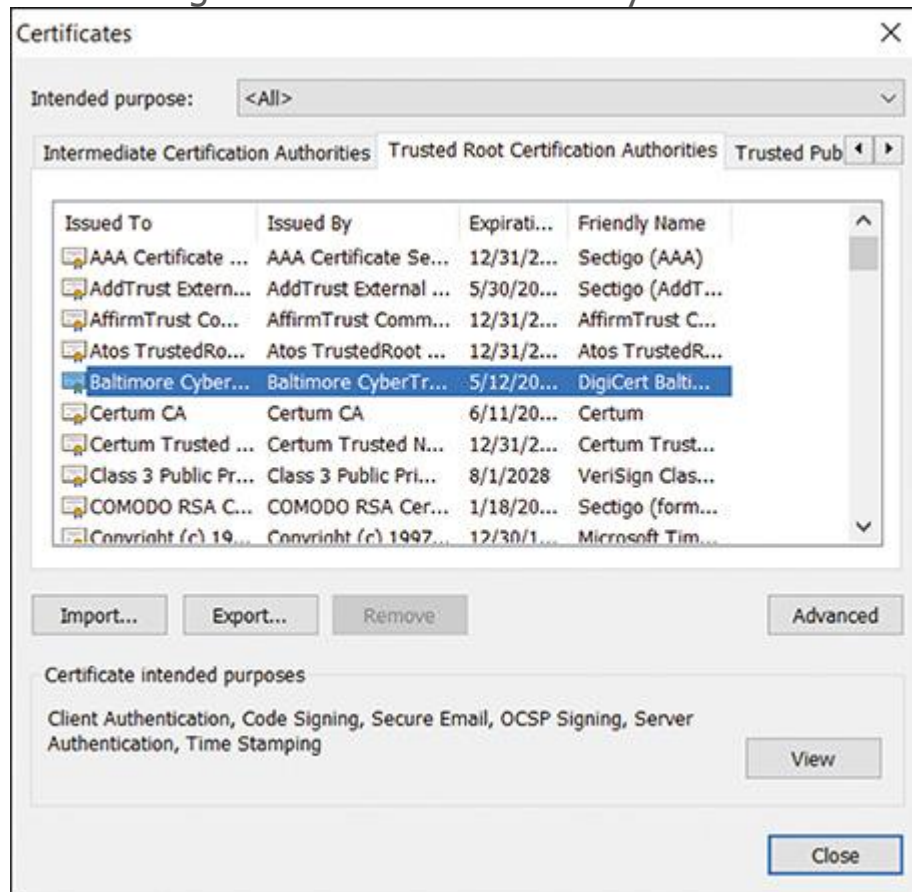


- **Secure connections and sites and valid certificates.** When browsers use HTTPS and SSL encryption protocols to communicate with secured websites, they validate a website’s digital certificate. To

view and manage these certificates, in Chrome settings, select **Privacy and security**, and click **Manage certificates**. In Edge settings, click **Privacy, search, and services** and then click **Manage certificates**. In both cases, the Windows Certificate dialog box appears where you can view, remove, import, and export certificates. See [Figure 19-6](#).

Figure 19-6

View and manage certificates validated by Windows



- **Update or repair Edge.** If you have a problem with Microsoft Edge, to update it, in Edge settings, click **About Microsoft Edge**. The update begins immediately. To repair Edge, use the **Apps & features** page in the Windows Settings app.



Exam Tip

The A+ Core 2 exam expects you to know how to secure browsers, including how to manage passwords, pop-up blockers, clearing the cache, private-browsing modes, browser data synchronization, and ad blockers. You also need to know how to download browsers from only trusted sources using hashing techniques (described later in this module) and how to configure proxy servers using the Windows Internet Options dialog box.

Internet Options and Proxy Settings

Windows 10 offers two browsers: the newer Edge and the older Internet Explorer browsers. Windows 11 offers only the Edge browser, but for legacy websites that require Internet Explorer, you can enable IE Mode in Edge. Internet Explorer in Windows 10 is configured via the **Internet Options** applet in Control Panel. For both Windows 10 and Windows 11, a few settings in Internet Options also affect Edge and other browsers installed in the system, including proxy settings.

Many large corporations and ISPs use proxy servers to speed up Internet access. A web browser does not have to be aware that a proxy server is in use. However, one reason you might need to configure Internet Options and use a proxy server is when you are on a corporate network and are having a problem connecting to a secured website (one using HTTP over SSL or another encryption protocol). The problem might be caused by Windows trying to connect using the wrong proxy server on the network. Check with your network administrator to find out if a specific proxy server should be used to manage secure website connections.

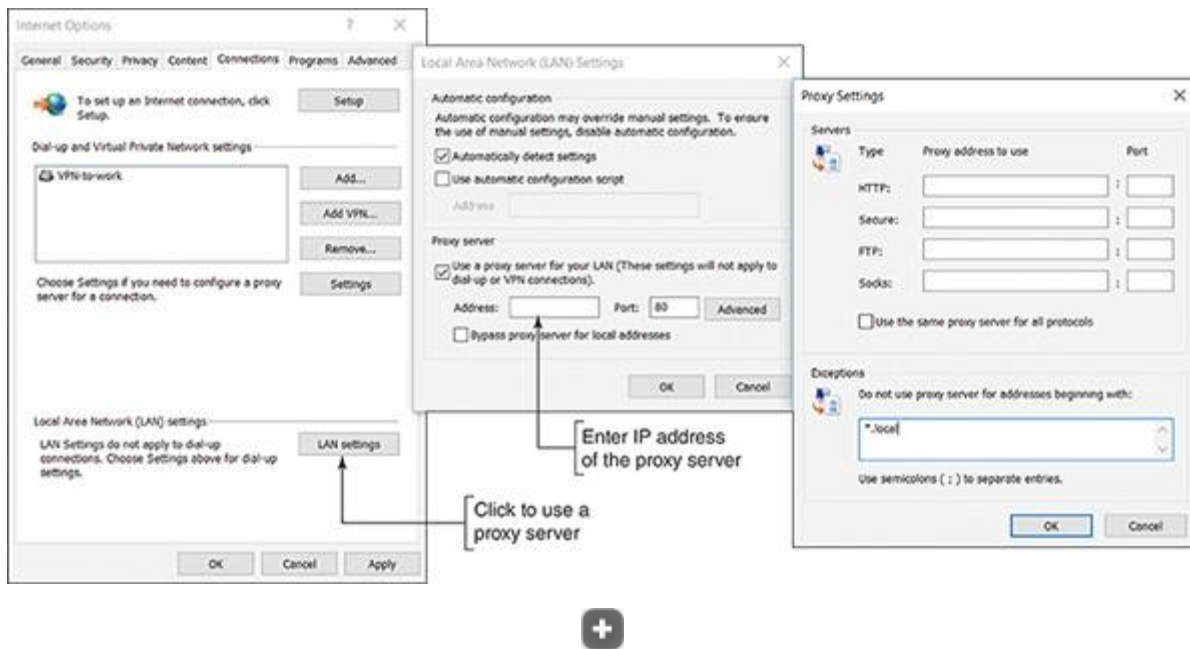
Exam Tip

The A+ Core 2 exam expects you to know how to configure proxy settings on a client desktop. For Windows 10/11, this is done with Internet Options.

If you need to configure Internet Options to use a specific proxy server, open **Control Panel** in classic view, and then open **Internet Options**. On the **Connections** tab, click **LAN settings**. In the settings dialog box, check **Use a proxy server for your LAN**, and enter the IP address of the proxy server (see [Figure 19-7](#)). If your organization uses more than one proxy server, click **Advanced**, and enter IP addresses for each type of proxy server on your network (see the right side of [Figure 19-7](#)). You can also enter a port address for each server, if necessary. If you are trying to solve a problem of connecting to a server using HTTP over SSL or another secured protocol, use the **Secure** field to enter the IP address of the proxy server that is used to manage secure connections.

Figure 19-7

Configure Microsoft Edge and other installed browsers to use one or more proxy servers



When you configure a proxy server in Internet Options, the setting applies to the entire Windows system, including Edge, Chrome, and other browsers and apps that can use a proxy server. If you want to use a proxy server just for a particular browser, know that Chrome, Edge, and Windows 10 Internet Explorer don't support customizing a proxy setting, but the Firefox browser ([mozilla.org](https://www.mozilla.org)) can use either proxy servers set up in Internet Options for the entire system or a customized proxy configured in Firefox.

Downloading Browsers Securely

When you download a new browser, such as Firefox or Chrome, be sure to download only from a trusted source. To verify the download is genuine, the software to install it that downloads with the browser file might be digitally signed. In addition, you can verify the download is error-free by comparing hashes. A **hash**, sometimes called a checksum, is a value generated by applying a specific algorithm to a file or text string. If the browser developer provides a hash value for the file before it is downloaded, you can compare the two values. If the two hash values match, you know the download happened without errors.

Types of hashing algorithms are MD5, which is mostly used for small files and produces a 128-bit hash value, and SHA-1 and SHA-2, used for larger files. SHA-2 hashing produces a 224-, 256-, 384-, or 512-bit hash value. Here are the general steps to use hashing to verify that a file downloads with no errors:

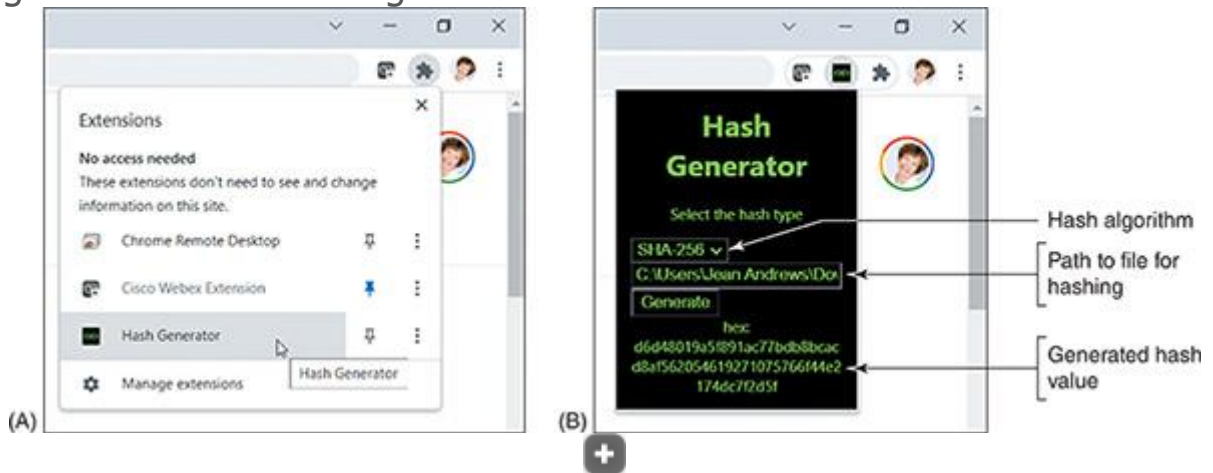
1. 1

You need a hash generator program, which can install as an extension in your browser. For example, for Google Chrome, go to the Chrome Web Store (chrome.google.com/webstore), and search for a hash generator. Select your generator,

and add it as a Chrome extension. It creates a tab in the browser menu bar, as shown in [Figure 19-8A](#).

Figure 19-8

(A) Hash Generator installed as a Chrome extension, and (B) Hashing a file using the SHA-256 hash algorithm



2. **2** Download the file, and obtain the hash value provided by the file developer.
3. **3** Copy the path to the file. (In **Explorer**, select the file, click **Home**, and then click **Copy path**.) For the Hash Generator extension in Google Chrome, open the extension box, paste the path to the file in the box, select the hash algorithm (be sure to select the same algorithm the developer used), and click **Generate**. The hash displays (see [Figure 19-8B](#)), and you can then select and copy it.
4. **4** Compare the hash value you generated to the one the developer provided. If they match, the download was without errors.



Exam Tip

The A+ Core 2 exam expects you to be able to use hashing when verifying that a browser download was successful. However, in practice, very few browser developers provide hash values for their browser installation files. Other types of software developers do routinely provide hash values to verify their downloaded files, and you can use hashing to verify these downloads. When a developer provides a hash value for a file, you might see the value displayed beside the download link on the download page. See [Figure 19-9](#).

Figure 19-9

Developer provides a hash value for its download using the SHA-1 hash algorithm

Download (3.3 GB)	Sha 1 hash — 0xD76AD96773615E8C504F63564AF749469CFCCD57
Download (2.5 GB)	Sha 1 hash — 0x8BED436F0959E7120A448F7C29FF0AA962BDEFC9

19-1b Create a VPN Connection

Core 2 Objectives

- 1.6

Given a scenario, configure Microsoft Windows networking features on a client/desktop.

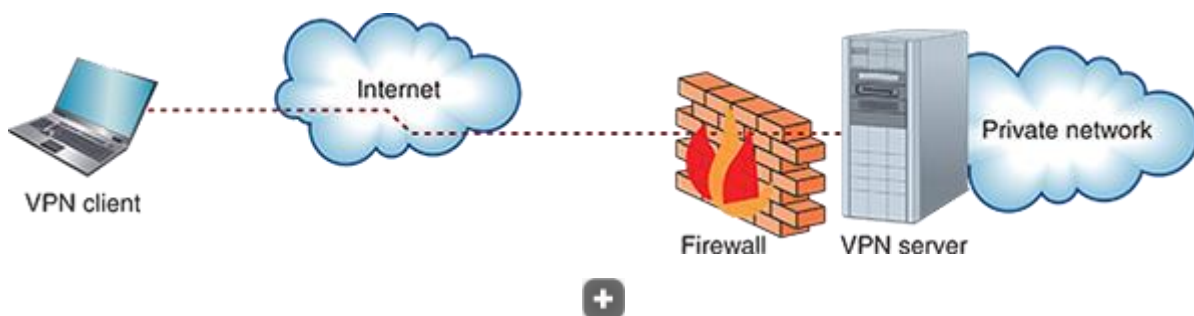
- 4.9

Given a scenario, use remote access technologies.

A virtual private network (VPN) is often used by telecommuting employees to connect to the corporate network by way of the Internet. A VPN protects data by encrypting it from the time it leaves the remote computer until it reaches a server on the corporate network, and vice versa. The encryption technique is called a tunnel or **tunneling** (see [Figure 19-10](#)). Encryption protocols used with a VPN include SSL, TLS, OpenVPN, IKEv2/IPsec, L2TP/IPsec, SSTP, and WireGuard. Managed switches, which you learned about in the Core 1 module “[Network Infrastructure and Cloud Computing](#),” sometimes provide VPN servers embedded in their firmware so they can support VPN connections for remote users of the private network to which they belong.

Figure 19-10

A VPN connection secures all traffic between the VPN client and the VPN server on the private network



A VPN can be managed by operating systems, routers, or third-party software such as OpenVPN (openvpn.net) or NordVPN (nordvpn.com). A VPN connection is a virtual connection, which means you are setting up the tunnel over an existing connection to the Internet. When creating a VPN connection on a personal computer, always follow directions given by the network administrator who hosts the VPN. The company website might provide VPN client software to download and install on your computer. For example, NordVPN provides an app to install on the client computer. Then you might be expected to double-click a configuration file to complete the VPN connection. OpenVPN uses an .ovpn file for this purpose.

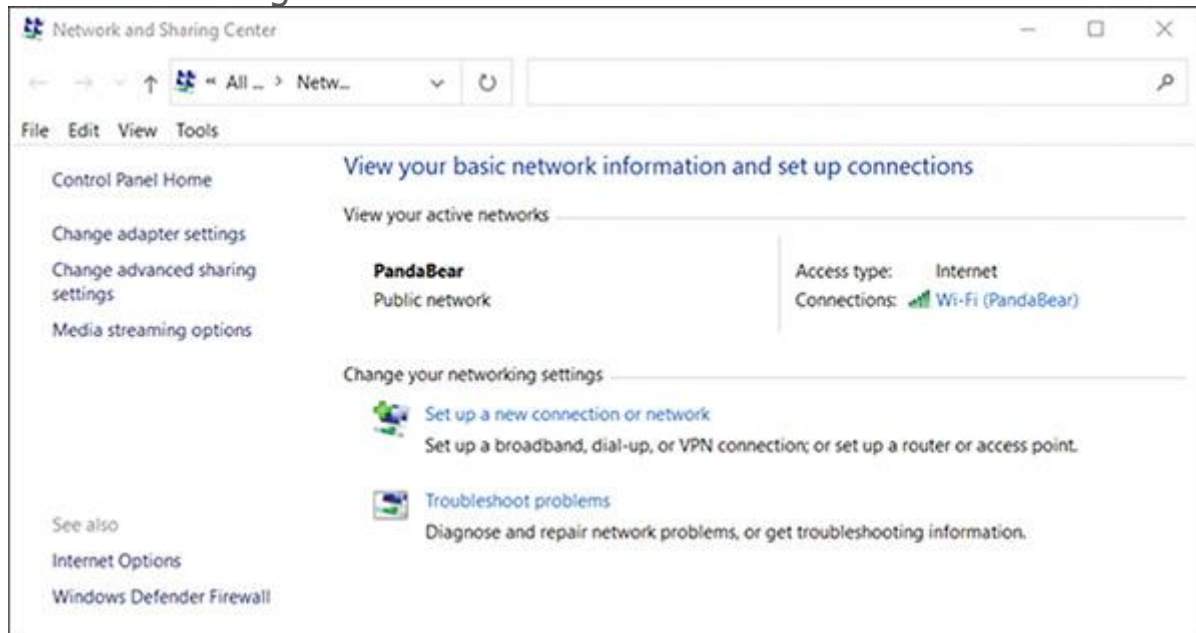
Here are the general steps using Windows 10/11 to connect to a VPN:

1. **1**

You can set up a VPN connection beginning from the Internet Options dialog box or from the Network and Sharing Center. To open the Network and Sharing Center, open **Control Panel** in classic view and then click **Network and Sharing Center** (see [Figure 19-11](#)).

Figure 19-11

Network and Sharing Center



2. **2**

Click **Set up a new connection or network**. Then select **Connect to a workplace** and click **Next**.

3. **3**

In the Connect to a Workplace dialog box, click **Use my Internet connection (VPN)**. In the next dialog box, enter the IP address or domain name of the network (see [Figure 19-12](#)). Your network administrator can provide this information. Name the VPN connection, and click **Create**.

Figure 19-12

Enter connection information to the VPN

← Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

☐ Use a smart card

☒ Remember my credentials

☐ Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

Create Cancel

Whenever you want to use the VPN connection, click the **Network** icon in the taskbar. In the list of available networks, click the **VPN connection**, and then click **Connect**. Enter your user name and password (see [Figure 19-13](#)), and click **OK**. Your user name and password are likely to be the same network ID and password to your user account on the Windows domain on the corporate network.

Figure 19-13

Enter your user name and password to connect to your VPN

Windows Security

Sign in

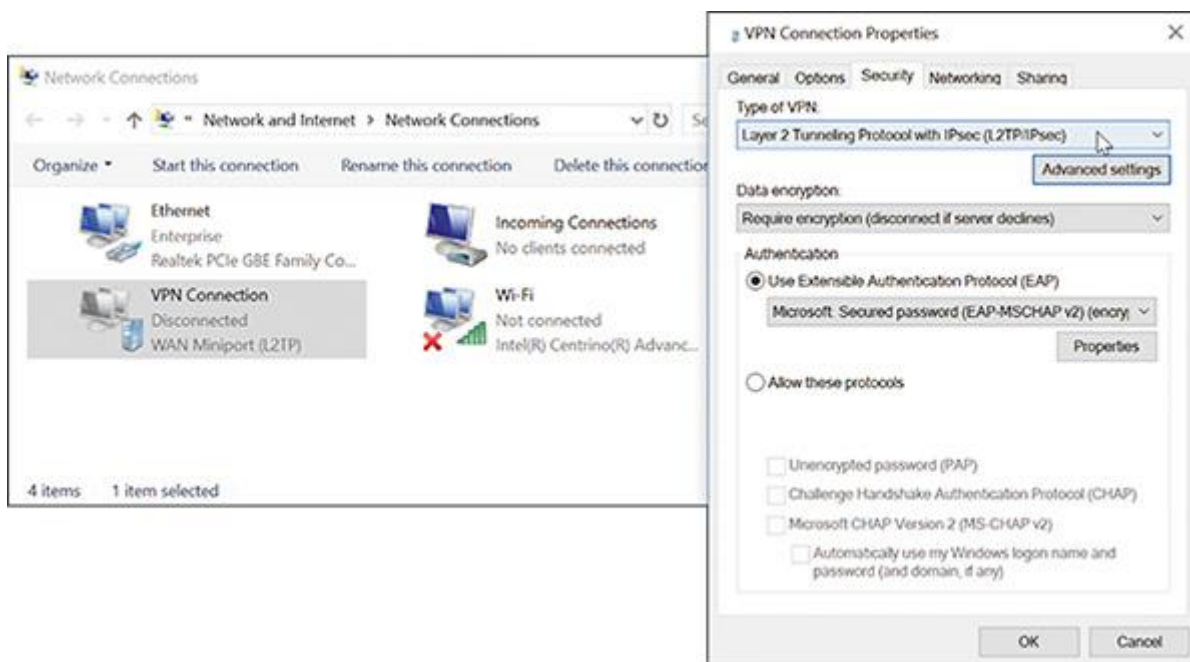
OK Cancel

After the connection is made, you can use your browser to access the corporate secured intranet websites or other resources. The resources you can access depend on the permissions assigned to your user account.

Problems connecting to a VPN can be caused by the wrong authentication protocols being used when passing the user name and password to the VPN. To configure these settings, return to the Network and Sharing Center, and click **Change adapter settings**. In the Network Connections window, right-click **VPN Connection** and click **Properties**. In the Properties dialog box, select the **Security** tab (see [Figure 19-14](#)). Here you can select security settings for the type of VPN, encryption requirements, and authentication protocols given to you by the network administrator.

Figure 19-14

Configure the VPN's security settings



Exam Tip

The A+ Core 2 exam expects you to know how to create VPN and WWAN connections and how to configure an alert when you have neared a data usage limit on a metered connection.

19-1c Create a WWAN Connection

Core 2 Objective

- 1.6

Given a scenario, configure Microsoft Windows networking features on a client/desktop.

A WWAN (Wireless Wide Area Network) connection requires a contract with a cellular carrier and a USB broadband device (see [Figure 19-15](#)) or a SIM slot on a laptop. Install the SIM card in the slot on the laptop, or install the card in the USB device and then insert the device in the USB slot. When the device installs, it automatically launches a program for you to connect to the carrier with a user name and password. Alternately, for a laptop with a SIM slot, you can use the utility provided by the laptop manufacturer, such as the HP Connection Manager, to connect to the cellular network, or you can allow Windows to manage the connection. To allow Windows to manage the connection, in the Settings app, click **Network & Internet, Cellular, and Let Windows manage this connection**. You'll need the user name and password for the mobile account with the cellular carrier.

Figure 19-15

A USB broadband modem by Sierra Wireless



19-1d Metered Connections

Core 2 Objective

- 1.6

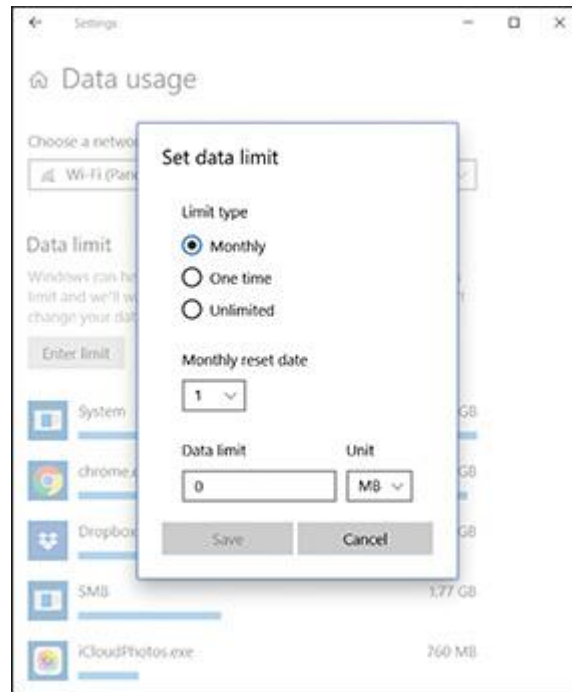
Given a scenario, configure Microsoft Windows networking features on a client/desktop.

To set an alert when you have almost reached a data limit for a metered connection in Windows 10, in the **Settings** app, click **Network & Internet**, and **Status**. On the Status page, click **Data usage**. On the Data usage window,

click **Enter limit**, and set a limit in MB or GB (see [Figure 19-16](#)). For Windows 11, in the **Settings** app, click **Network & internet**, click **Data usage**, click **Enter limit**, and set your limit. After you set the alert, you will be warned when the data usage nears the limit.

Figure 19-16

Set a data limit for a metered connection



19-1e Windows Defender Firewall

Core 2 Objectives

- 1.4

Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

- 1.6

Given a scenario, configure Microsoft Windows networking features on a client/desktop.

- 2.5

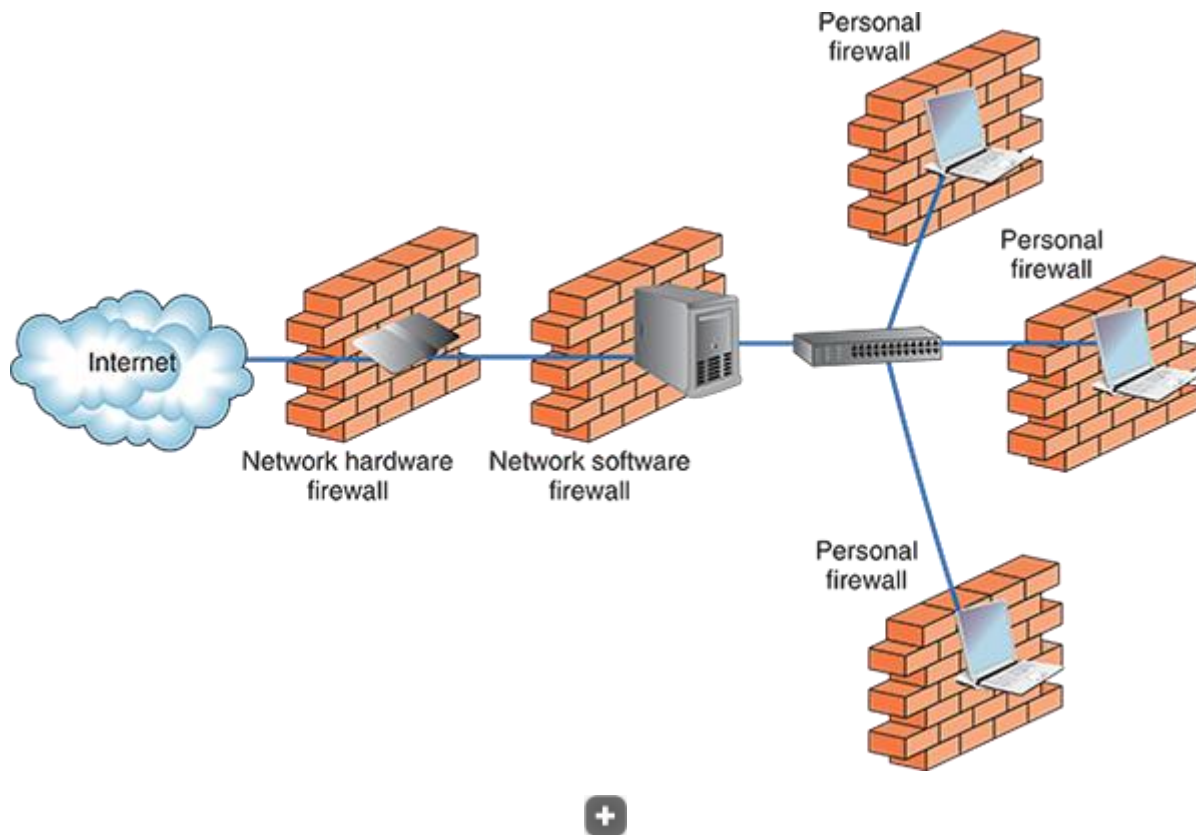
Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Recall from the Core 1 module “[Networking Fundamentals](#)” that a SOHO router can serve as a hardware firewall to protect its network from attack over the Internet, and the best protection from attack is layered protection (see [Figure 19-17](#)). In addition to a network hardware firewall, a large

corporation might use a software firewall, also called a corporate firewall, installed on a computer that stands between the Internet and the network to protect the network. This computer has two network cards installed, and the installed software firewall filters the traffic between the two cards.

Figure 19-17

Three types of firewalls used to protect a network and individual computers on the network



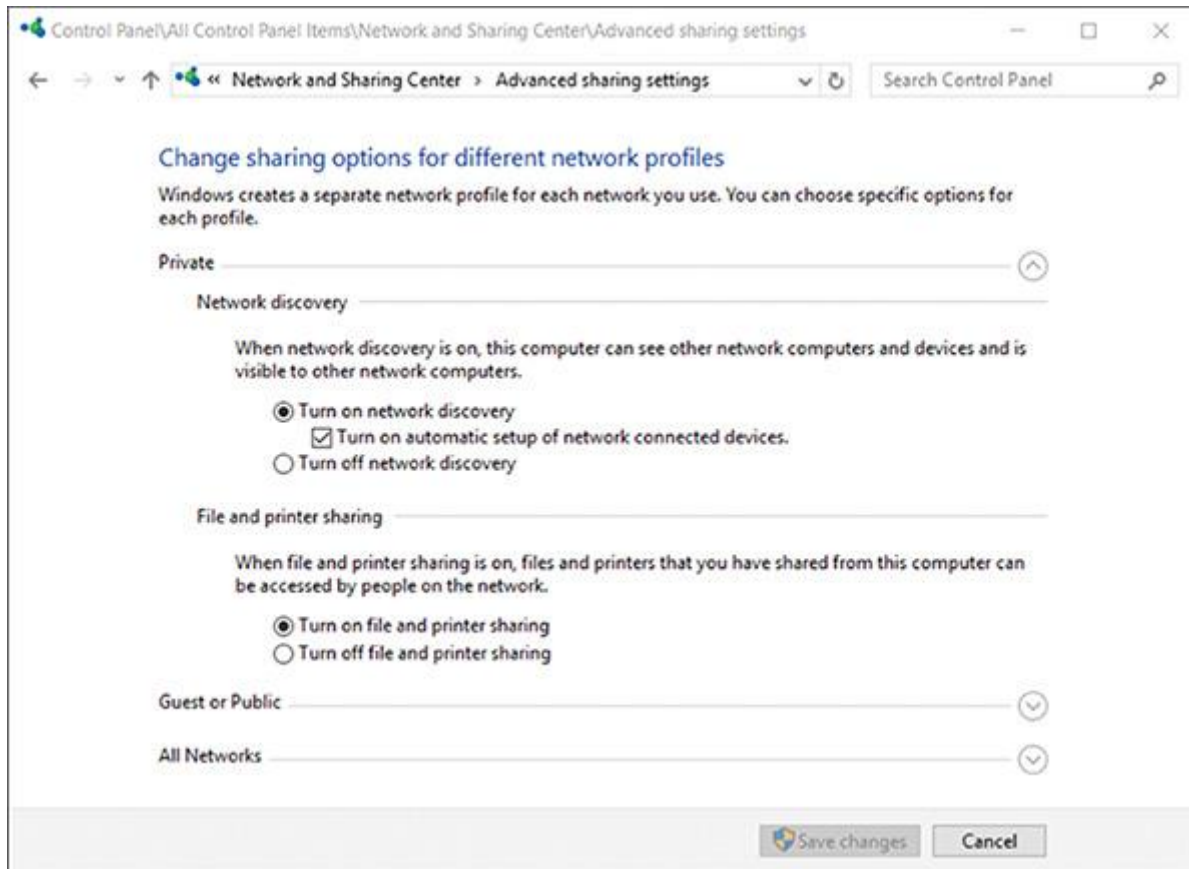
A personal firewall, also called a host firewall or application firewall, is software installed on a personal computer to protect it. A personal firewall provides redundant protection from attacks over the Internet, filters inbound traffic to protect a computer from attack from other computers on the same network, and filters outbound traffic to prevent attacks on other computers on the same network. When setting up a SOHO network or a personal computer, configure a personal firewall on each computer.

Windows Defender Firewall is a personal firewall that protects a computer from intrusion and from attacking other computers; it is automatically configured when you set up your security level for a new network connection. To set the security for a network connection, open the **Network and Sharing Center** in Control Panel, and click **Change advanced sharing settings**. In the Windows 10/11 Advanced sharing settings window (see [Figure 19-18](#)), you can choose private or public security levels and set

other security options for the network connection. All these settings affect settings in Windows Defender Firewall.

Figure 19-18

Configure the security level for network connections



Applying Concepts

Configuring Windows Defender Firewall

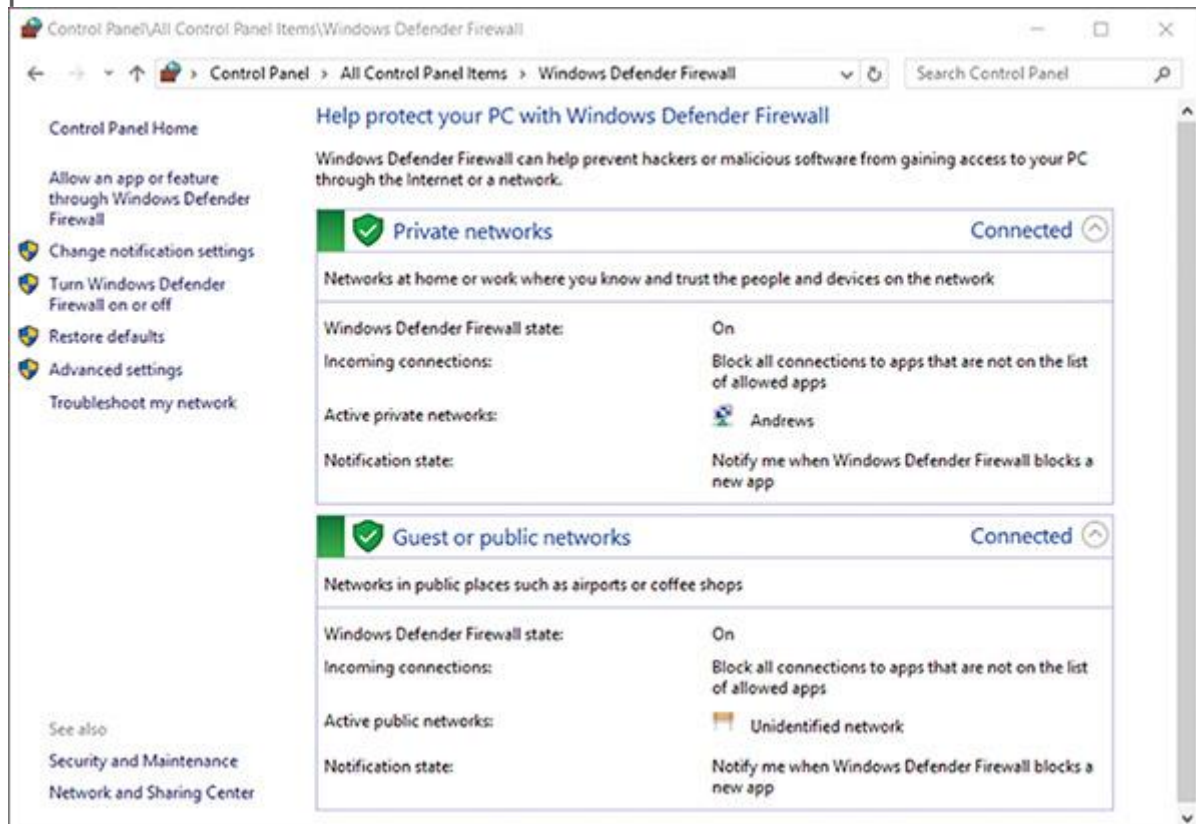
- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.4

You can use the Windows Defender Firewall window in Windows 10/11 to configure even more firewall settings. As you work, be careful that you don't accidentally change a setting that leaves your computer open to attack. Follow these steps to find out more:

1. **1**
Open **Control Panel** in classic view, and click **Windows Defender Firewall**. See [Figure 19-19](#).

Figure 19-19

Windows Defender Firewall shows the firewall is turned on to protect private and public network connections



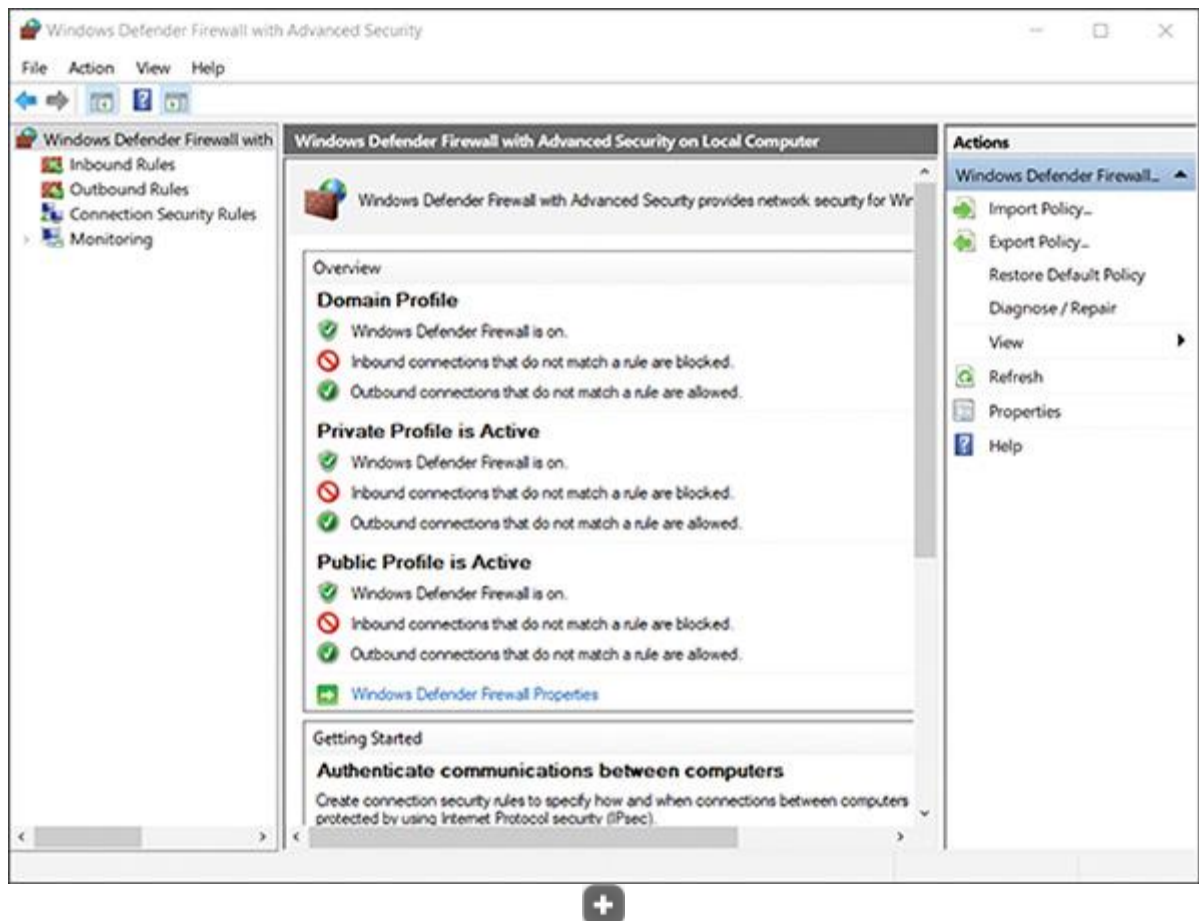
2. 2

In general, Windows Defender Firewall works by allowing or denying network traffic on incoming or outgoing ports. Recall that a port is a number an application on the computer uses to connect to another application on the network or Internet. Here are some basic settings you can configure in Windows Defender Firewall:

1. Use the left pane to turn Windows Defender Firewall on or off. When the firewall is disabled (not a good idea), all traffic is allowed to pass, and your computer is unprotected.
2. When the firewall is enabled, all traffic is stopped unless you have specified an exception. To allow or deny a specific app access to the computer, click **Allow an app or feature through Windows Defender Firewall**. You can then select the app from a list of apps and decide how it can use the network connection.
3. To allow or deny all other types of traffic, not just those related to apps, click **Advanced settings**. On the Advanced Security window (see [Figure 19-20](#)), you can click Inbound Rules or Outbound Rules to create or edit an inbound or outbound rule and control traffic. A rule can specify how port numbers, TCP/IP protocols, programs, services, computers, and remote users can use the network connection. A rule can apply to public, private, and domain networks.

Figure 19-20

Customize an inbound or outbound rule to control exactly what incoming or outgoing traffic is allowed through the firewall



Now let's turn our attention to securing other devices, including the Internet of Things devices.

19-1f Secure Internet of Things Devices

Core 2 Objective

- 2.7

Explain common methods for securing mobile and embedded devices.

For a device, such as a refrigerator or doorbell, to be considered part of the Internet of Things (IoT), the device or its controller or bridge must have an IP address. After all, a node can't connect to the Internet without an IP address. In most cases, IoT devices are monitored and controlled by wireless connections. Besides Wi-Fi and Bluetooth, Z-Wave and Zigbee are two other wireless communication protocols commonly used by smart locks, smart light bulbs, and other IoT devices. Here are the primary facts about Z-Wave and Zigbee:

- **Z-Wave** transmits around the 900 MHz band and requires less power than Wi-Fi. It has a larger range than Bluetooth, reaching a range of up to 100 meters in open air (although significantly less inside buildings).
- **Zigbee** operates in either the 2.4 GHz band or the 900 MHz band, requires less power than Wi-Fi, and generally reaches a range of about 20 meters inside, but it can reach much farther.
- Z-Wave and Zigbee are not compatible. Zigbee is faster than Z-Wave. Z-Wave and Zigbee both use encryption and are considered safe from hackers.
- Both Z-Wave and Zigbee devices can connect in a mesh network, which means that devices can “hop” through other devices to reach the destination device. Z-Wave and Zigbee devices are not normally assigned IP addresses unless another protocol, such as Z/IP or Zigbee IP, is working to manage TCP/IP networking.
- Typically, Zigbee and Z-Wave compete about equally for the wireless standard of choice for IoT devices in the residential market. Zigbee is the choice for large-scale commercial or industrial use because it is more robust.

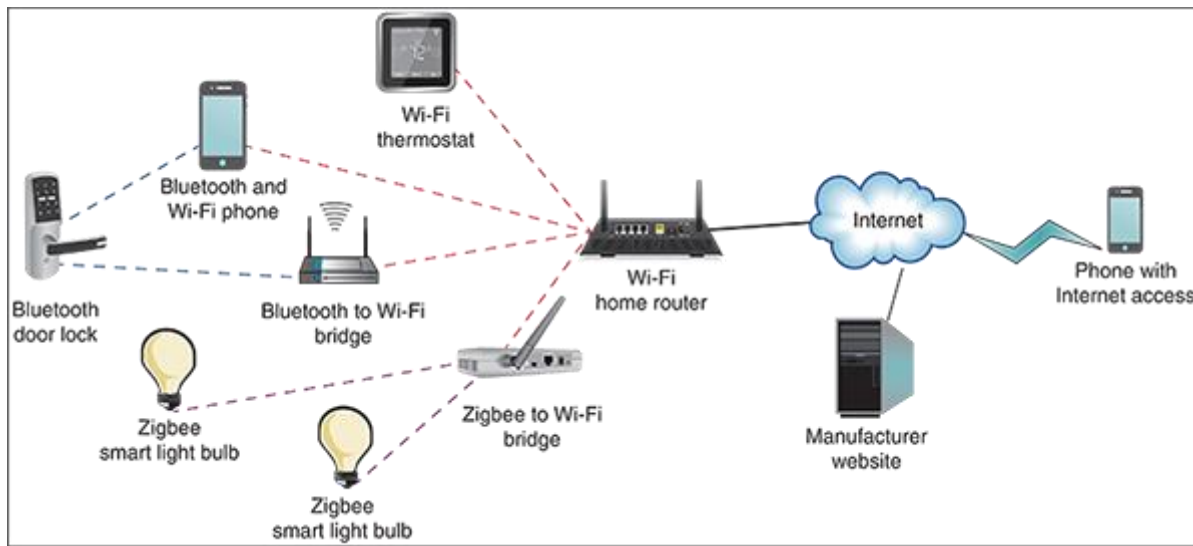
Note 2

When worker honeybees return to their nest, they do a dance that looks like a zig-zag pattern. Zigbee was named after this phenomenon: *zig bee*.

Some smart devices, such as a smart thermostat by Nest (nest.com), can connect directly to a Wi-Fi network via an embedded Wi-Fi radio (see [Figure 19-21](#)). Alternately, devices such as a door lock or thermostat might use Bluetooth to communicate with a phone or tablet within Bluetooth range or might use a bridge to connect to the Wi-Fi network. Other devices, such as smart light bulbs or a door lock, might use Zigbee, Z-Wave, or another wireless technology that the phone or tablet does not use. Such devices require a bridge device to connect them to the Wi-Fi network, as shown in [Figure 19-21](#).

Figure 19-21

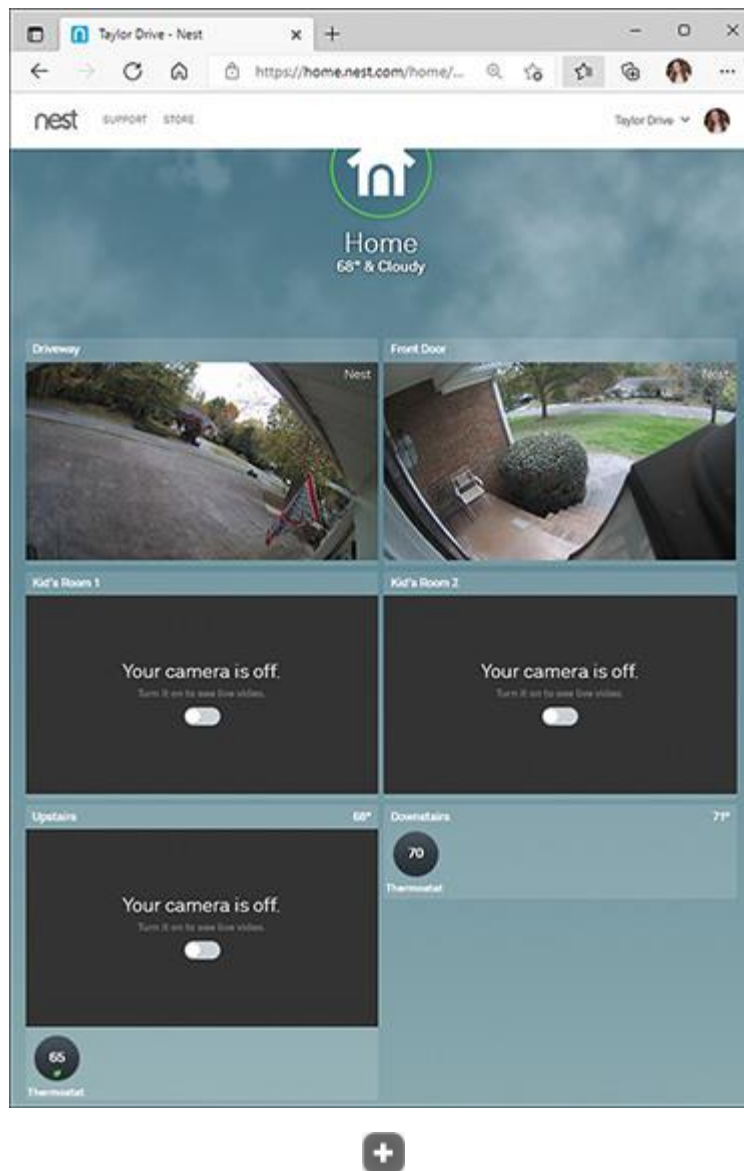
IoT devices connected to a smart home network may use a variety of wireless technologies



For smart devices to truly be IoT devices, you must be able to control them over the Internet. For that to happen, they must connect directly or through a bridge to a home or business Wi-Fi network that has Internet access. Notice in [Figure 19-21](#) that the manufacturer's website is involved when managing many IoT devices. For example, [Figure 19-22](#) shows the webpage where two exterior webcams, three interior webcams, and two thermostats by Nest (nest.com) can be monitored and managed from anywhere on the web.

Figure 19-22

IoT device manufacturers provide websites to manage their devices



Source: Nest

Here are some tips to secure IoT devices:

- Avoid using public networks on the Internet when you're monitoring or controlling IoT devices. If you must use public networks, consider using a VPN connection.
- Set up guest networks for your guests to use in your home or small business so your IoT devices are not exposed.
- For all IoT devices that have default user names and passwords, change the user names and create strong passwords.
- Don't connect locks and security cameras to your voice assistant. You don't want an intruder to yell through the window, "Alexa, open the front door!"
- Frequently purge the data kept by Amazon for Alexa and by Google for Google Assistant. You can use your phone app to delete.
- Keep software and firmware up to date to make sure security patches are current.

- Implement the wireless security methods for your wireless router covered next.

19-2 Securing a Multifunction Router for a SOHO Network

Core 2 Objectives

- 2.2
Compare and contrast wireless security protocols and authentication methods.
- 2.5
Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- 2.9
Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

An IT support technician is likely to be called on to set up a small office or home office (SOHO) network. As part of setting up a small network, you need to know how to set up and secure a multipurpose router to stand between the network and the Internet. A **router** (see [Figure 19-23](#)) is a device that manages traffic between two or more networks and can help find the best path for traffic to get from one network to another.

Figure 19-23

Cisco Catalyst 8200 Series Edge Platform router is suited for small and medium-sized enterprise branch offices



Source: Cisco

Exam Tip

The A+ Core 1 and A+ Core 2 exams both require you to be able to install and configure a SOHO wired and wireless router. The A+ Core 2 exam expects you to be able to secure the router and SOHO network.



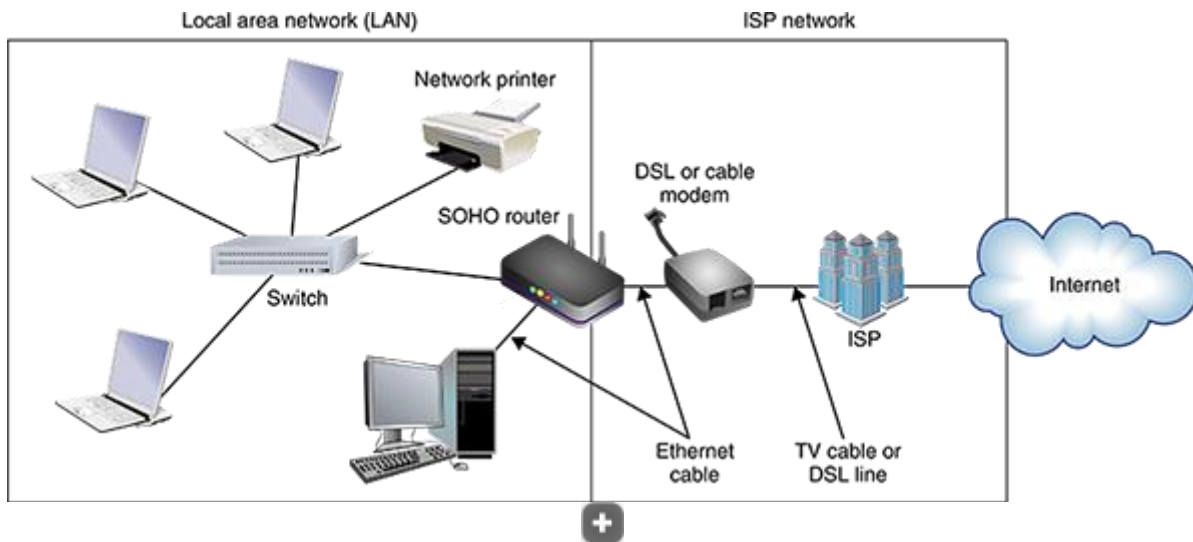
Core to Core

In the Core 1 module “[Networking Fundamentals](#),” you learned to install and set up a SOHO router. This module takes you one step further to learn how to secure the router and the local network it supports. If you have not yet read the module “[Networking Fundamentals](#),” now would be a good time to work your way through it and then turn back to this module.

A SOHO router stands between the Internet and a small local network (LAN) to connect the LAN to a network that belongs to an ISP, which connects to the Internet. See [Figure 19-24](#).

Figure 19-24

A SOHO router stands between the local network and the IPS’s network, which connects to the Internet



Here is a brief review of the functions of a SOHO router you learned about in the module “[Networking Fundamentals](#)”:

- As a router, it stands between two networks—the ISP network and the local network—and routes traffic between the two networks.
- As a **switch**, it manages several network ports that can be connected to wired devices on the local network.
- As a DHCP server, it can provide IP addresses to computers and other devices on the local network.
- As a **wireless access point (WAP)**, it enables wireless devices to connect to the network. These wireless connections can be secured using wireless security features.
- As a firewall, it blocks unwanted traffic from the Internet and can restrict Internet access for local devices behind the firewall.
- If an external storage device, such as a USB flash drive or external hard drive, connects to the router via the USB port, the router can be used as a file server for network users.

An example of a multifunction router is the Nighthawk AC1900 by NETGEAR, shown in [Figures 19-25](#) and [19-26](#). It has one Internet port (also called the WAN or wide-area-network port) to connect to the ISP by way of a modem or ONT and four ports for devices on the network. The USB port can be used to plug in a USB external hard drive for file sharing on the network. The router is also a wireless access point with multiple antennas to increase speed and range.

Figure 19-25

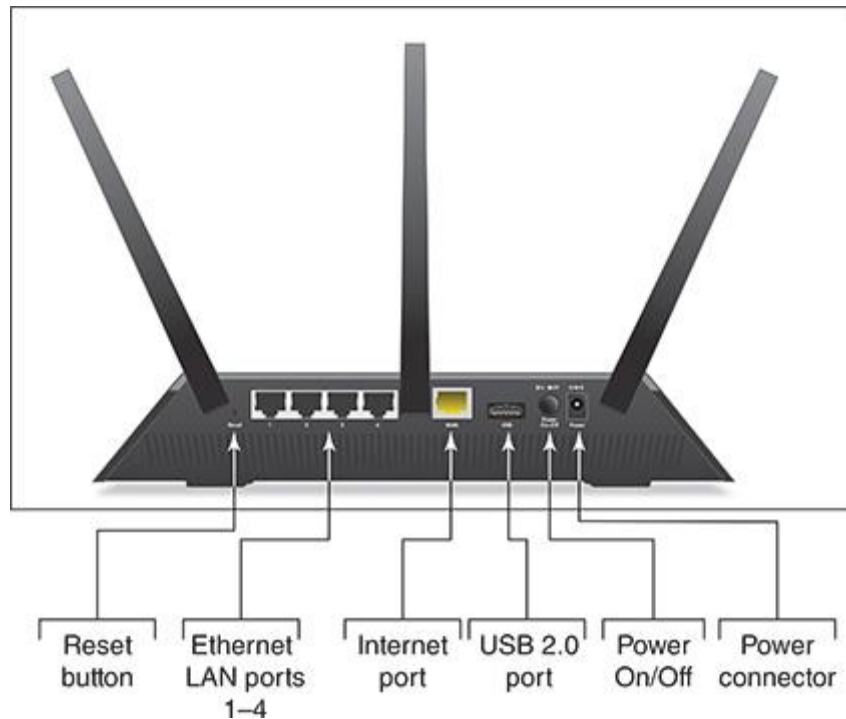
The NETGEAR Nighthawk AC1900 dual-band Wi-Fi Gigabit router



Source: [Amazon.com](https://www.amazon.com), Inc.

Figure 19-26

Connections and ports on the back of the NETGEAR router



Source: Netgear

Next, let's step through the process of securing a SOHO router and the network it supports.

19-2a Router Placement for Best Security

Core 2 Objective

- 2.9

Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

When securing a router, consider its physical security. If the router will be used as a wireless access point, make sure it is centrally located to create the best Wi-Fi hotspot for users. For physical security in a small business, don't place the router in a public location, such as the lobby. For best security, place the router behind a locked door accessible only to authorized personnel in a location with access to network cabling. The indoor range for a Wi-Fi hotspot is up to 70 meters; this range is affected by many factors, including interference from walls, furniture, electrical equipment, and other nearby hotspots. For the best Wi-Fi strength, position your router or a stand-alone wireless access point in the center of where you want your hotspot, and know that a higher position (near the ceiling) works better than a lower position (on the floor).

For routers that have external antennas, raise the antennas to vertical positions. Plug in the router and connect network cables to devices on the local network. Connect the network cable from the ISP modem or other device to the uplink port on the router.

19-2b Basic Security Features of a Router

Core 2 Objectives

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

- 2.9

Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

To configure a router for the first time or change its configuration, always follow the directions of the manufacturer. You can use any computer on the network that uses a wired connection (it doesn't matter which computer) to configure the firmware on the router. You'll need the IP address of the router and the default user name and password to the router setup. To find this information, look in the router documentation or search online for your model and brand of router.

Here are the general steps for one router, the ASUS RT-AX55. The setup screens for your router may be different:

1. **1**

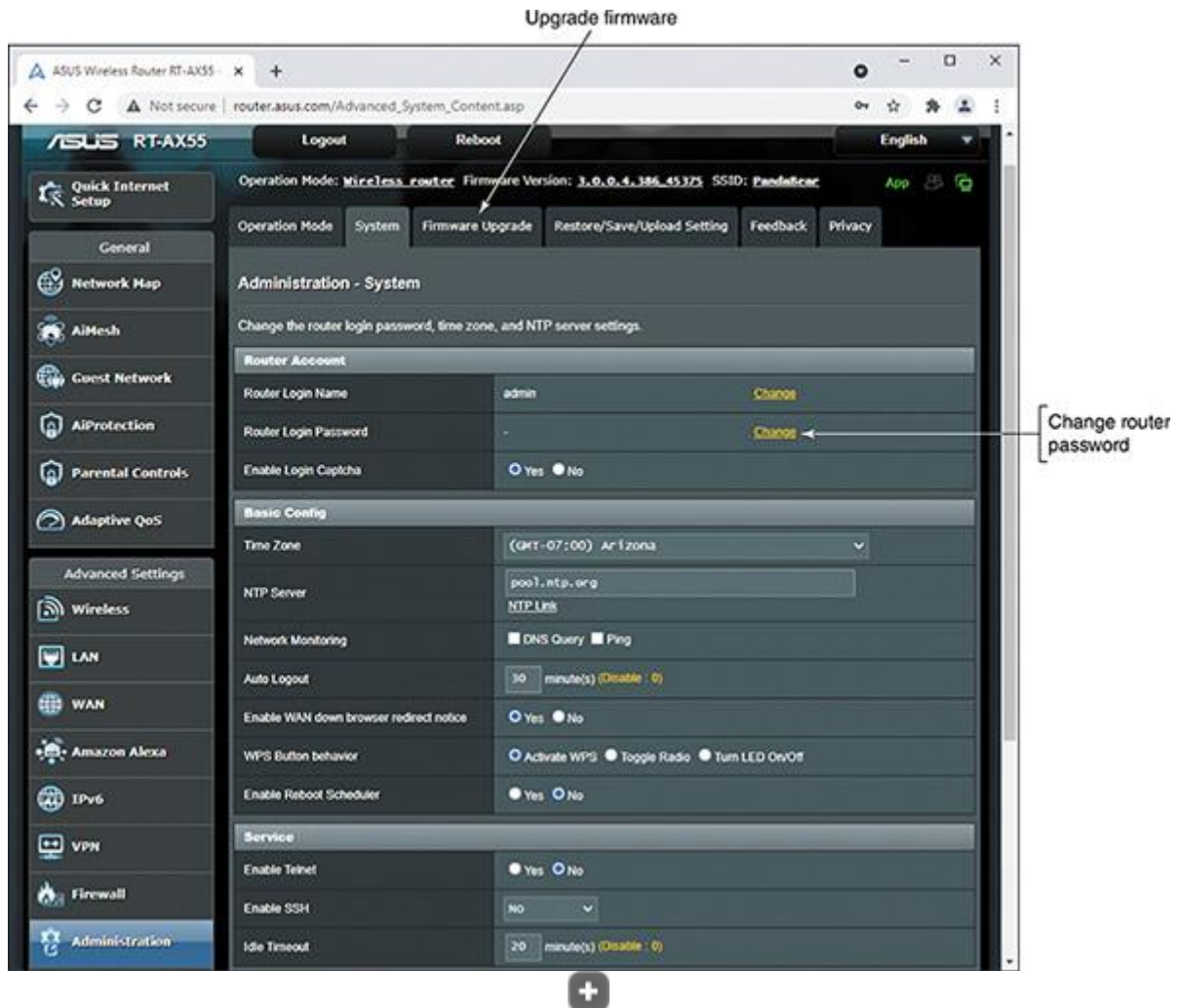
Sign in to router. Open your browser, and enter the IP address of the router in the address box. In our example, the address is 192.168.1.1. Enter the user name and password to the router firmware. The router firmware main menu screen appears.

2. **2**

Change the default password. One important security setting is to change the default password to the router firmware. For the ASUS router, click **Administration** in the left pane, and then click the **System** tab to change the router name and password. See [Figure 19-27](#).

Figure 19-27

Change the password to the router firmware configuration



! Caution

Changing the router password is especially important if the router is a wireless router. Unless you have disabled or secured the wireless access point, anyone within its range—even outside your building—can use your wireless network. If they guess the default password to the router, they can change the password to hijack your router. Also, your wireless network could be used for criminal activity.

1. **3**

Update firmware. Also notice in [Figure 19-27](#) the Firmware Upgrade tab in the Administration group. On this tab, you can check online for a firmware update and then download and install the update. If the update fails while it is installing, you can manually download and install the ASUS Firmware Restoration utility to undo the update.

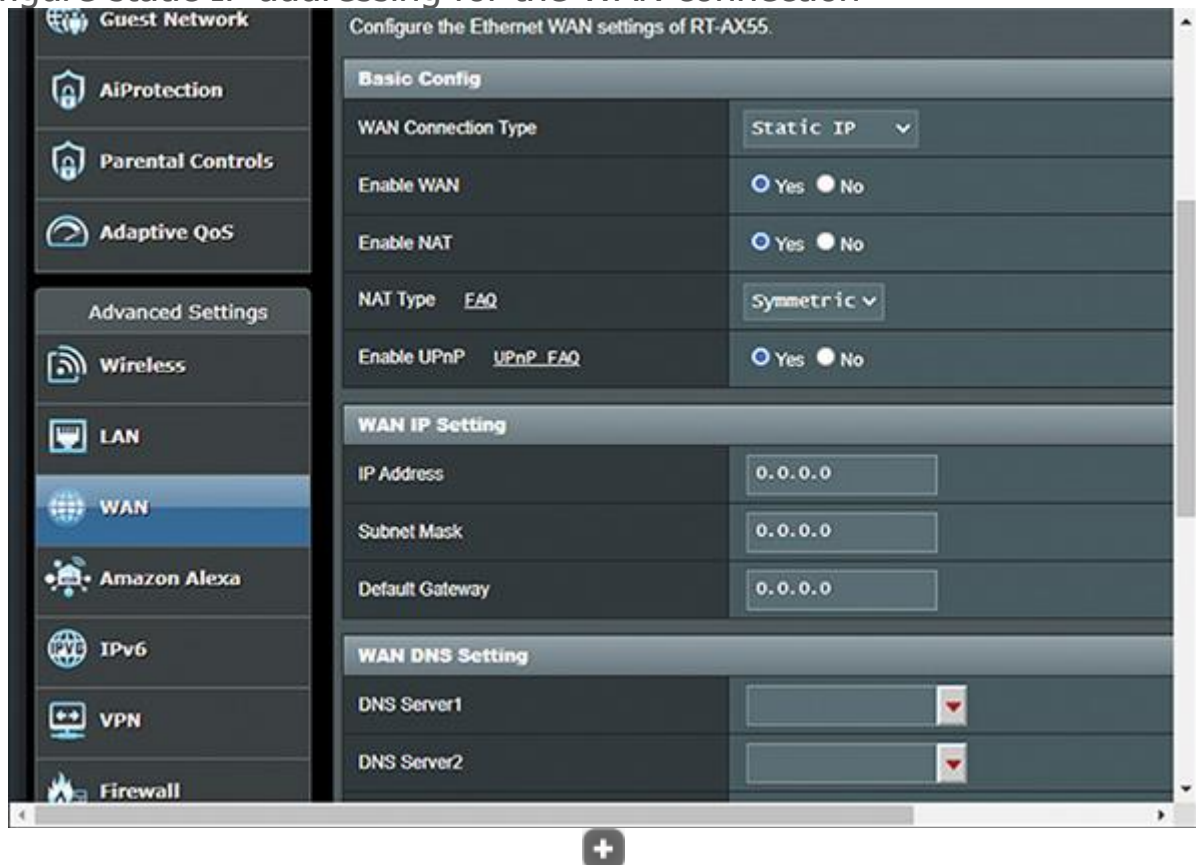
2. **4**

Static wide-area network (WAN) IP address. Normally, the ISP serves up a dynamic IP address, subnet mask, default gateway, and DNS server addresses to the router for its connection to the ISP network. However, if your local network publishes a website, email service, or other service on the Internet, the router will need a static IP address configuration on the WAN so computers on the Internet can find your network. For this purpose, you can lease a public IP address from the ISP or other source and configure

the router to use this static IP address. To configure this connection, for the ASUS router, click **WAN** in the left pane, and in the **Basic Config** section, select **Static IP** as the WAN Connection Type (see [Figure 19-28](#)). Enter the IP address, subnet mask, default gateway, and DNS server addresses for the WAN configuration.

Figure 19-28

Configure static IP addressing for the WAN connection



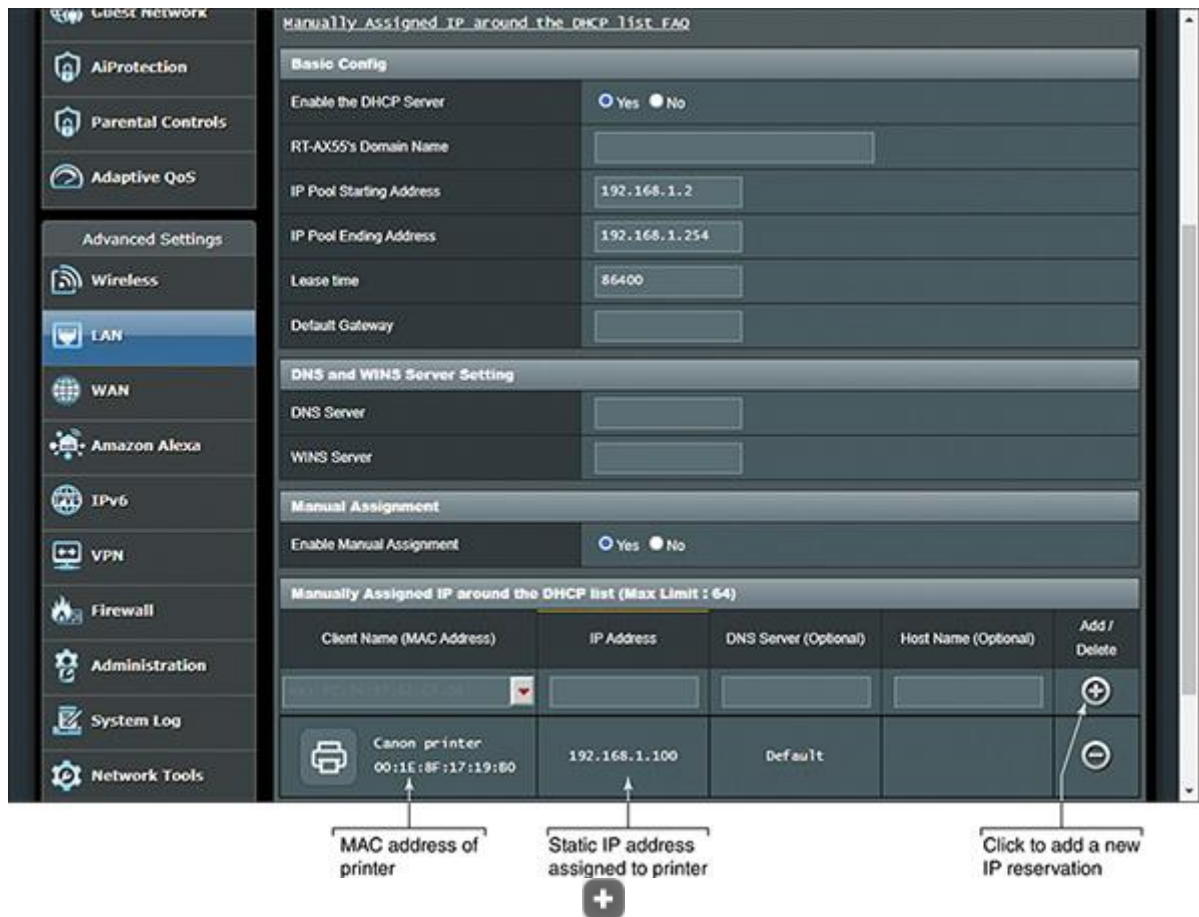
! Caution

After you make a change to the router firmware, be sure to click **Apply** at the bottom of the screen to save your changes before you move on to another firmware screen.

- 5 DHCP reservations.** Recall from the module “[Networking Fundamentals](#)” that you can set the local IP address for the router, the subnet mask, and the range of IP addresses that the router’s DHCP server can serve up to local hosts on the network. See [Figure 19-29](#). In addition, you can reserve an IP address for a host on the network, such as a printer, that requires a static IP address so other hosts on the network can find it. In [Figure 19-29](#), notice the Canon printer is assigned the static IP address 192.168.1.100. The printer was initially identified by its MAC address, also shown in the figure.

Figure 19-29

Configure the DHCP server and reserve a static IP address for a host



Exam Tip

The A+ Core 1 and A+ Core 2 exams both require you to know about DHCP servers and how to reserve an IP address for a host that requires a static IP address on the network.

1. **6**

Universal Plug and Play (UPnP). Some devices—such as printers, mobile devices, and some smart home IoT appliances—might be enabled for **Universal Plug and Play (UPnP)**, which allows them to discover and communicate with each other on the network. Enable UPnP if devices on your network are having a problem establishing communication. Basically, a device can then use the router to advertise its service and automatically communicate with other devices on the network. UPnP is considered a security risk because shields between devices are dropped, which hackers might exploit. Also, UPnP increases chatter on the network and can affect performance. Therefore, use UPnP with caution. For our sample router, UPnP is enabled in the WAN group, in the Basic Config section (refer back to [Figure 19-28](#)).

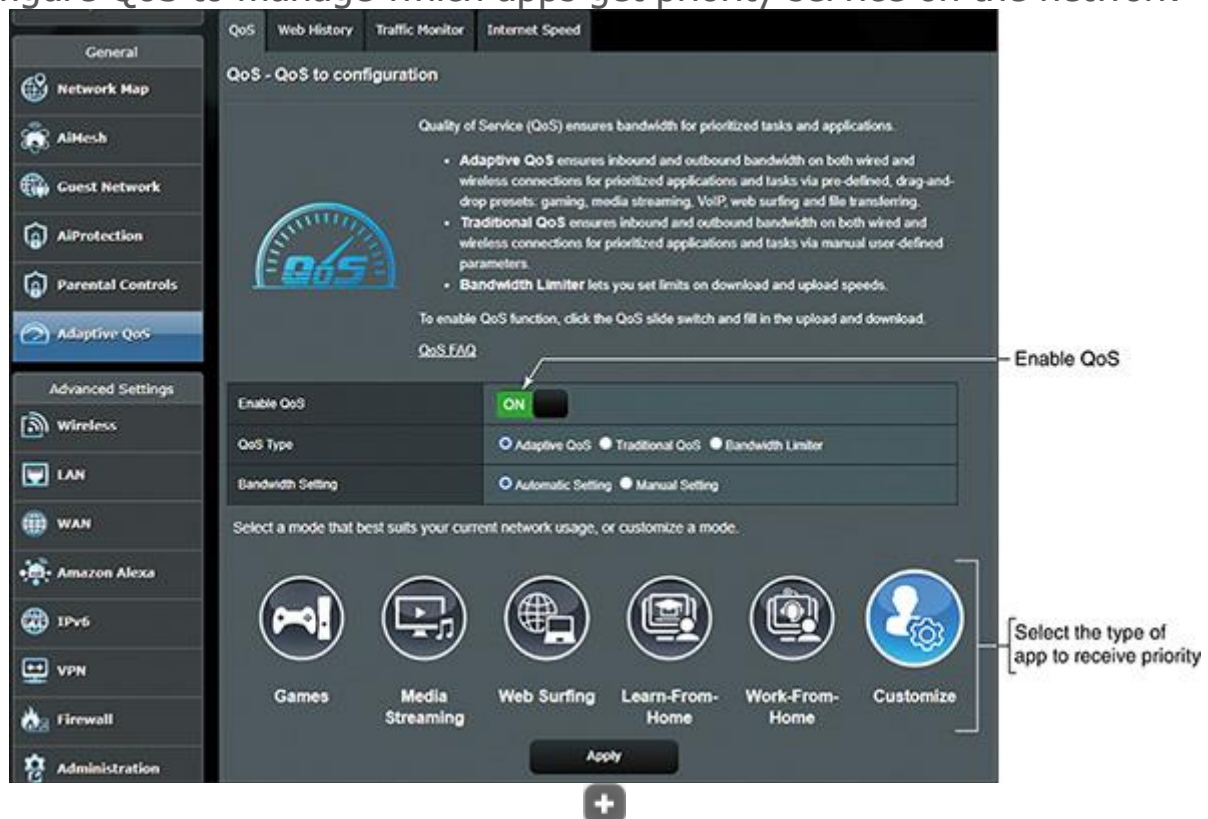
2. **7**

QoS for an application. As you use your network and notice that one application, such as VoIP, gaming, or media streaming, is not getting the best service, you can improve its network performance using the Quality of Service (QoS) feature discussed in earlier modules. For our sample router, click **Adaptive QoS** in the left pane and the **QoS** tab in the right pane. Then turn on **Enable QoS**. See [Figure 19-30](#). You can then use the

buttons near the bottom of this window to promote a type of application or click **Customize** to further fine-tune which apps get priority with network bandwidth.

Figure 19-30

Configure QoS to manage which apps get priority service on the network



Now let's look at the concepts and steps to put up a firewall to control traffic to and from your network and the Internet. Then we'll look at how to set up a wireless network.

19-2c Firewall Settings

Core 2 Objectives

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

- 2.9

Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

To protect resources on the network, a router's firewall can examine each message coming from the Internet and decide if the message is allowed onto the local network. When a message arrives at the router, it is directed to a particular computer (identified by its IP address) and to a particular

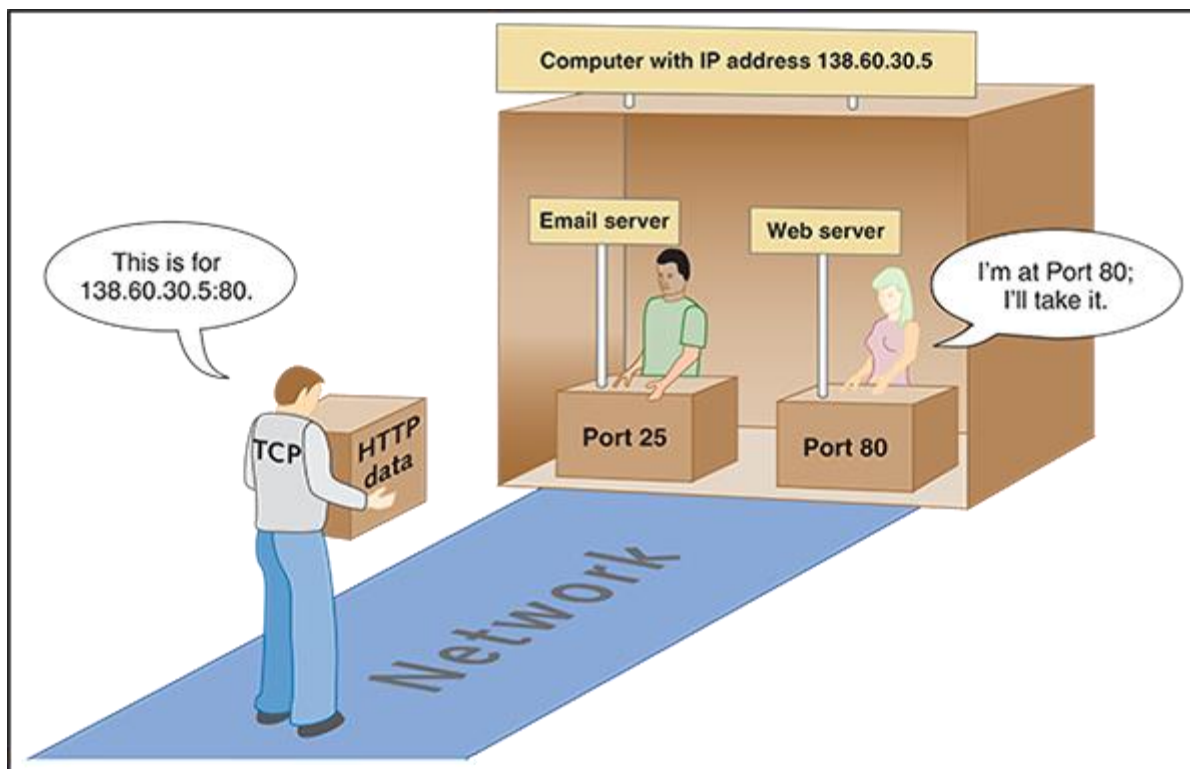
application running on that computer (identified by a port number, also called a port or **port address**.)

Recall that most applications used on the Internet or a local network are client/server applications. Client applications—such as Microsoft Edge, Google Chrome, or Outlook—communicate with server applications such as a web server or email server. Each client and server application installed on a computer listens at a predetermined port that uniquely identifies the application on the computer.

Suppose a computer with an IP address of 138.60.30.5 is running an email server listening at port 25 and a web server application listening at port 80. If a client computer sends a request to 138.60.30.5:25 (IP address and port 25), the email server listening at that port responds. On the other hand, if a request is sent to 138.60.30.5:80 (IP address and port 80), the web server listening at port 80 responds (see [Figure 19-31](#)).

Figure 19-31

Each server application running on a computer is addressed by a unique port number



Core to Core

For a refresher on how client/server applications use port addresses and the common ports they use, see the Core 1 module "[Networking Fundamentals](#)."

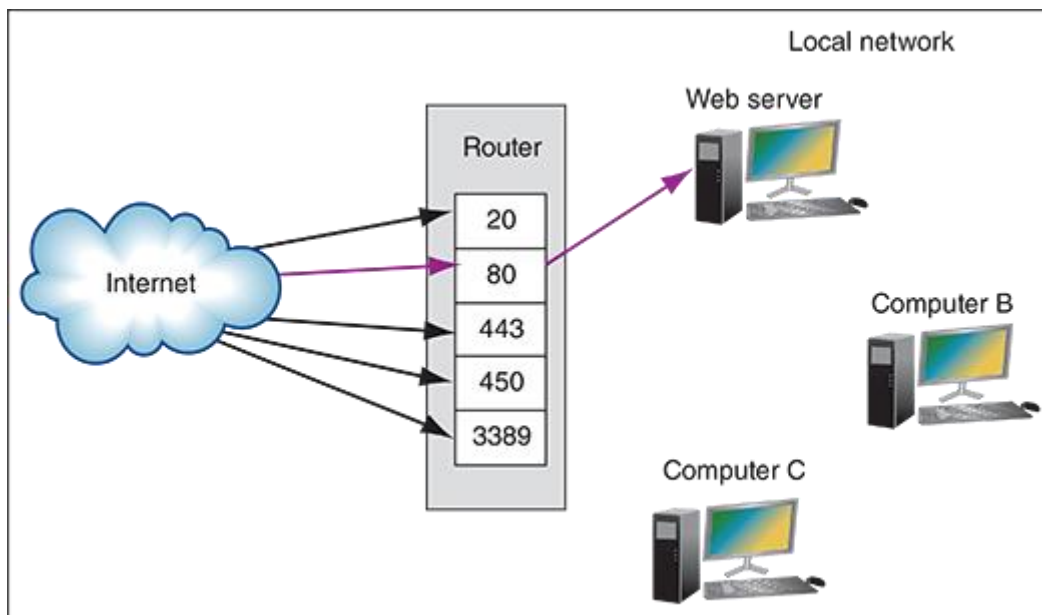
Firewalls on routers offer the option to disable (close) all ports, which means that no activity initiated from the Internet can get in. For some routers, you must explicitly disable all ports. For the ASUS router in our example, all ports are disabled (closed) by default. You must specify exceptions to this firewall rule in order to allow unsolicited traffic from the Internet. Exceptions are allowed using port forwarding or a DMZ (described later in this module). In addition to managing ports, you can also limit Internet traffic by filtering content. All these techniques are discussed next.

Port Forwarding

Suppose you're hosting an Internet game or website or you want to use Remote Desktop to access your home computer from the Internet. In these situations, you need to enable (open) certain ports to certain computers so that activity initiated from the Internet can get past your firewall. This technique, called **port forwarding** or port mapping, means that when the firewall receives a request for communication from the Internet to the specific computer and port, the request will be allowed and forwarded to that computer on the network. The computer is defined to the router by its static IP address. For example, in [Figure 19-32](#), port 80 is open and requests to port 80 are forwarded to the web server listening at that port. This one computer on the network is the only one allowed to receive requests at port 80.

Figure 19-32

Port forwarding allows a port to receive incoming traffic to a specific host on the network



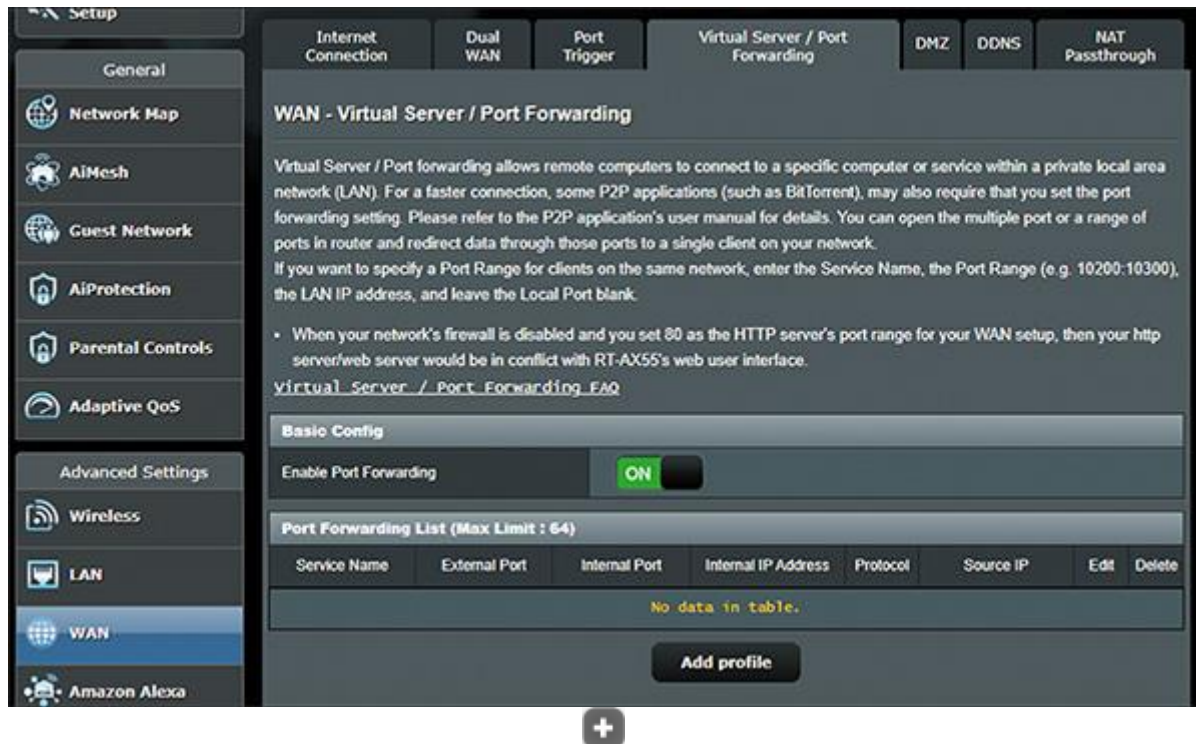
To configure port forwarding for our sample router, follow these steps:

1. **1**

In the router firmware, click **WAN** in the left pane, select the **Virtual Server/Port Forwarding** tab, and turn on **Enable Port Forwarding** (see [Figure 19-33](#)).

Figure 19-33

Enable port forwarding to allow unsolicited Internet traffic through your firewall

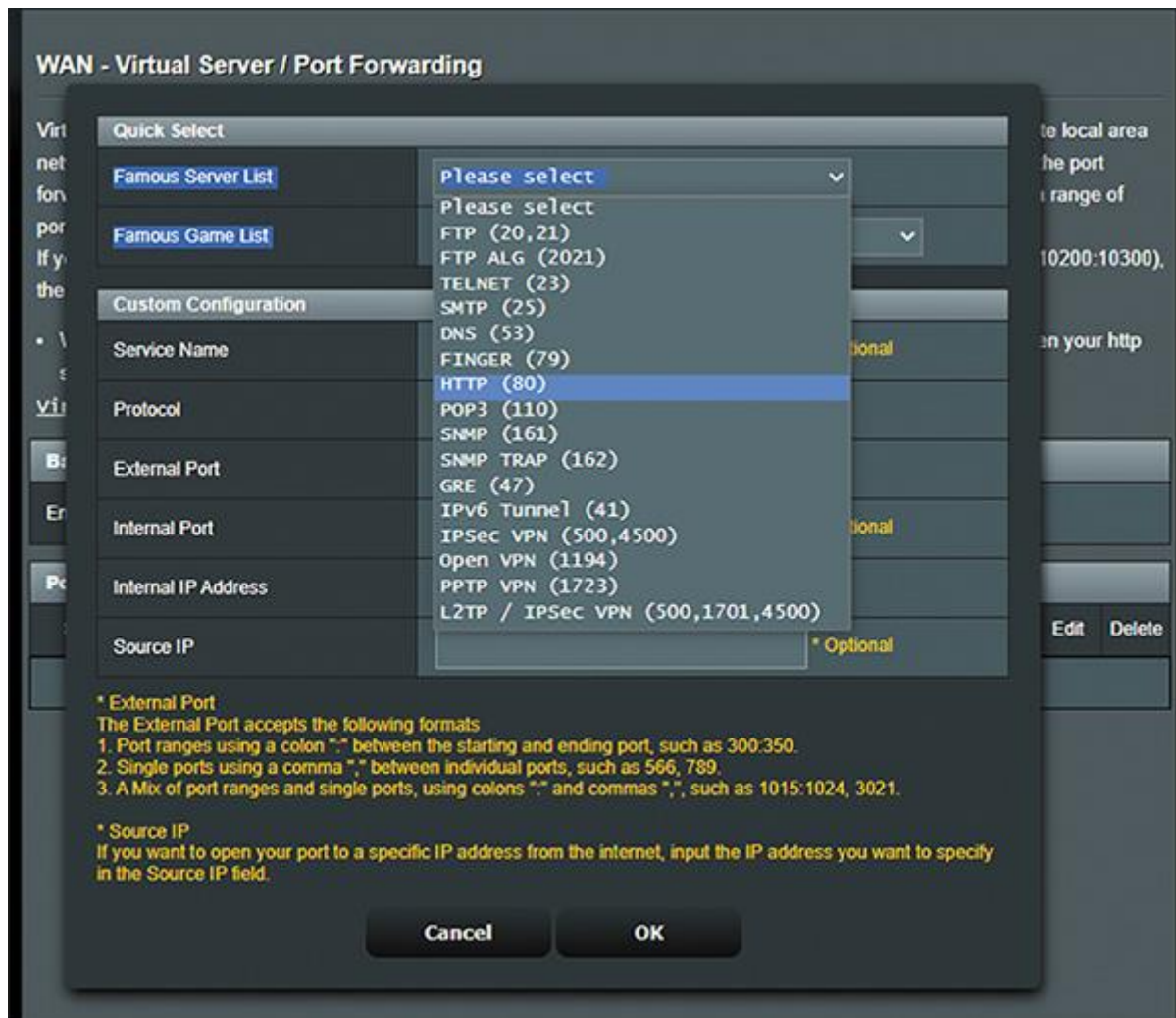


2. **2**

To add a port forwarding rule, click **Add profile**. For a web server, in the box that appears, select **HTTP (80)** as shown in [Figure 19-34](#). The TCP protocol is selected automatically.

Figure 19-34

Select the service that is to receive traffic from the Internet



3. **3** In the dropdown list of internal IP addresses, select the IP address of the web server. Click **OK**.
4. **4** Be sure to test your port forwarding rule by using a device connected to the Internet but not connected to your LAN or router. Can the device reach your website?

Note 3

If you want to use a domain name rather than an IP address to access a computer on your network from the Internet, you'll need to purchase the domain name and register it in the Internet namespace to associate it with your public static IP address. Assign this public IP address to your router, which forwards requests to the web server behind the firewall. Several websites on the Internet let you lease domain names and public IP addresses; one such site is by Network Solutions (networksolutions.com).

Here are some tips to keep in mind when using port forwarding:

- You must have a static IP address for the WAN side of your router so people on the Internet can find you. Most ISPs will provide you a static

IP address for an additional monthly fee, or you can lease one from another source and inform your ISP about it.

- For port forwarding to work, the computer on your network must have a static IP address so the router knows where to send the communication.
- Using port forwarding, your computer and network are more vulnerable because you are allowing external users directly into your private network. For better security, turn on port forwarding only when you know it's being used and be sure to disable any unused ports you don't need open.

DMZ and Screened Subnet

A **DMZ (demilitarized zone)** in networking is a computer or network that is not protected by a firewall or has limited protection. You can drop all your shields protecting a computer by putting it in a DMZ, and the firewall will no longer protect it. If you are having problems getting port forwarding to work, putting a computer in a DMZ can free it to receive any communication from the Internet. All unsolicited traffic from the Internet that the router would normally drop is forwarded to the computer designated as the DMZ server.



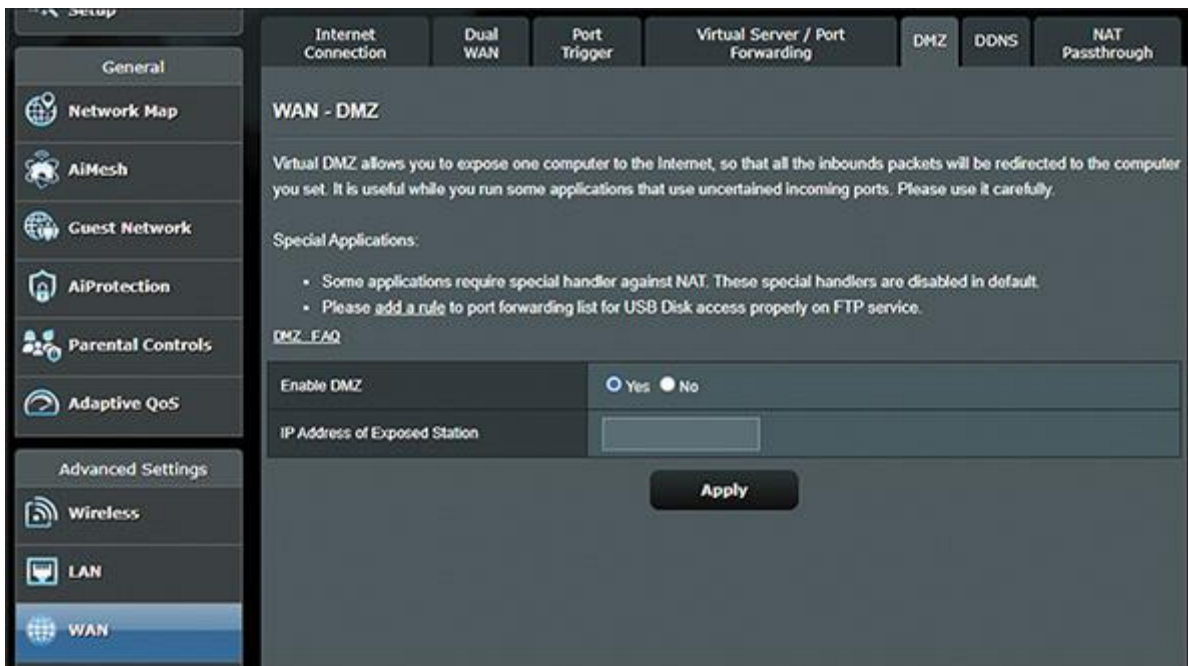
Caution

If a DMZ computer is compromised, it can be used to attack other computers on the network. Use it only as a last resort when you cannot get port forwarding to work. It goes without saying you should not leave the DMZ enabled unless you are using it.

To set up a DMZ server for our sample router, click **WAN** in the left pane, click the **DMZ** tab, and enable the DMZ. You can then enter the static IP address of the one computer you want to put in the DMZ. See [Figure 19-35](#).

Figure 19-35

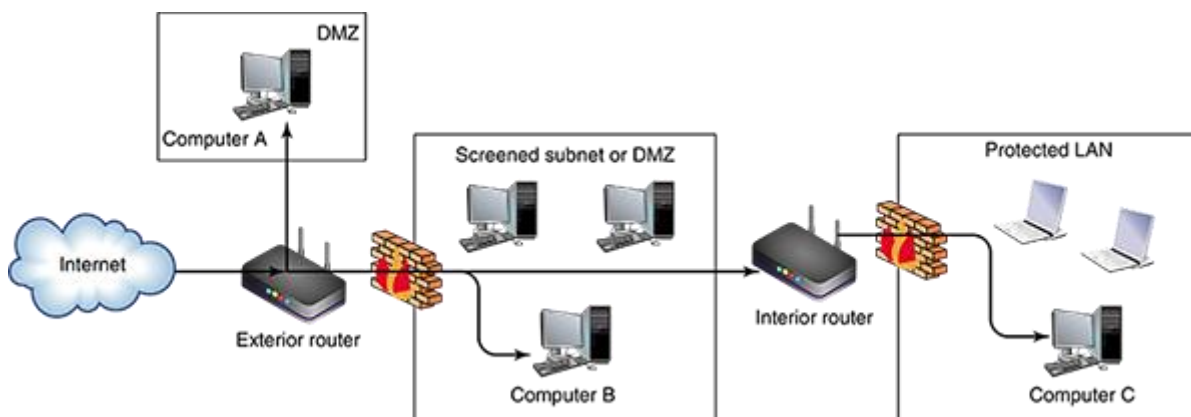
Configure an unprotected DMZ computer exposed to the Internet



A **screened subnet** is a variation of a DMZ, and the two terms are often used interchangeably. As in the previous example, the computer labeled as computer A in [Figure 19-36](#) is in the DMZ and is exposed to all Internet traffic. Computer B is in the screened subnet and is partially protected by a firewall provided by the exterior router, sometimes called an access router. A second router, the interior router, protects another subnet containing computer C, which is the most protected of all. In an organization, web servers and other servers that are exposed to unsolicited Internet traffic are put in the screened subnet, which offers some protection, and all other computers are put in the highly protected LAN. To reach these computers, traffic must make its way through two firewalls.

Figure 19-36

A screened subnet offers some protection for computers behind the first firewall



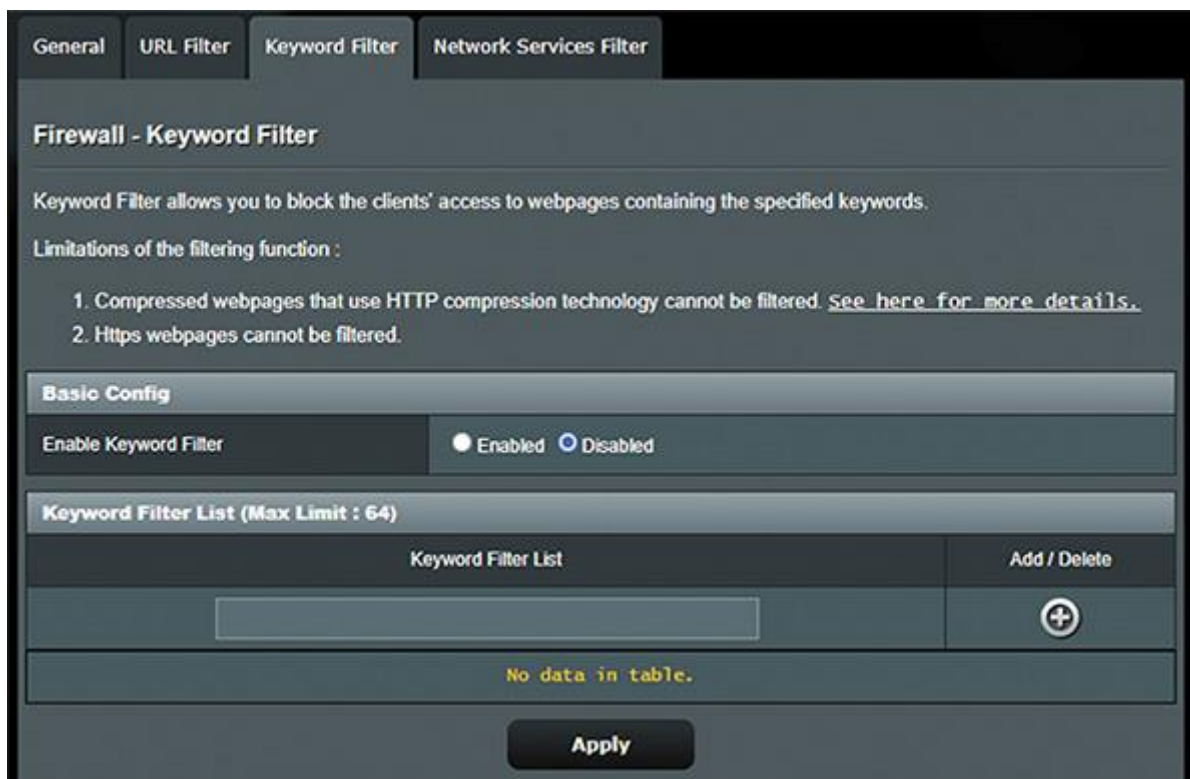
Content Filtering

Routers normally provide a way for employers or parents to limit the content that computers on the local network can access on the Internet. Filtering can apply to specific computers, users, websites, categories of websites, keywords, services, time of day, and day of the week. Criteria for filtering can draw from **blacklists** (lists of what cannot be accessed) or **whitelists** (lists of what can be accessed).

For our sample ASUS router, to manage content filtering, click **Firewall** in the left pane and the **Keyword Filter** tab. In this window, you can enable keyword filtering, and then enter a list of key words. Unsecured webpages that contain these key words will be blocked. Webpages that use HTTPS will not be filtered. See [Figure 19-37](#).

Figure 19-37

Content filtering blocks unsecured web pages that contain specified key words



Application and Port Security and IP Filtering

Firewalls block specific applications or network services, ports, and IP addresses. For the ASUS router, all this is done in the Firewall group, on the Network Services Filter page (see [Figure 19-38](#).) First enable network service filtering, and then you can either deny or allow (deactivate or activate) the activity you specify. You can filter well-known applications by

name or filter other apps by the ports they use. For example, you can block Internet gaming services, email services, or web services, or you can allow a service based on a schedule. You can also specify the IP addresses of computers to which the block applies.

Figure 19-38

Deny or allow applications, ports, and IP address activities

Firewall - Network Services Filter

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked). Leave the source IP field blank to apply this rule to all LAN devices.

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network.

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter: ☒ Yes ☐ No

Filter table type:

Well-Known Applications:

Date to Enable LAN to WAN Filter: ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri

Time of Day to Enable LAN to WAN Filter: : - :

Date to Enable LAN to WAN Filter: ☒ Sat ☒ Sun

Time of Day to Enable LAN to WAN Filter: : - :

Filtered ICMP packet types:

Network Services Filter Table (Max Limit : 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="button" value="+"/>
No data in table.					



Exam Tip

The A+ Core 1 and A+ Core 2 exams may give a scenario that expects you to resolve a problem by implementing port forwarding (mapping), whitelists, blacklists, content filtering, DMZ, screened subnets, application and port security, and IP filtering.

Now let's turn our attention to configuring a wireless access point provided by a router.

19-2dSecuring a Wireless Network

Core 2 Objectives

- 2.2

Compare and contrast wireless security protocols and authentication methods.

- 2.9

Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

A wireless network is created by a wireless access point using the Wi-Fi standards. These Wi-Fi standards are technically the IEEE 802.11 standards—collectively known as the 802.11 a/b/g/n/ac/ax standards—and have evolved over the years. [Table 19-1](#) lists older and current standards.

Table 19-1

Wi-Fi Technologies

Standard	Maximum Speed	Description
802.11a	Up to 54 Mbps	No longer used. Used 5 GHz frequency with a range up to 50 meters.
802.11b	Up to 11 Mbps	Experiences interference from cordless phones and microwaves. Used 2.4 GHz frequency and a range up to 100 meters.
802.11g	Up to 54 Mbps	Compatible with and has replaced 802.11b. Uses 2.4 GHz frequency and range up to 100 meters.
802.11n (Wi-Fi 4)	Up to 600 Mbps	An access point can have up to four antennas to improve performance. Uses both 2.4 and 5 GHz frequencies, with an indoor range up to 70 meters and outdoor range up to 250 meters.
802.11ac (Wi-Fi 5)	Theoretically up to 7 Gbps, but currently limited to 1.3 Gbps	Supports up to eight antennas and beamforming to increase signal strength toward connected devices. Uses 5 GHz frequency only and has the same ranges as 802.11n.
802.11ax (Wi-Fi 6)	Up to 10 Gbps	This throughput is possible when using the 160 MHz channel spacing and eight antennas. (Each antenna provides one spatial stream.) Uses both 2.4 and 5 GHz frequencies and has a range a bit better than 802.11n/ac.



Wireless computers and other devices on the wireless LAN (WLAN) must support the latest wireless standard for that standard to be used. If they do not, the connection uses the latest standard supported by both the WAP and the client. [Figure 19-39](#) shows a wireless adapter that has two antennas and supports the 802.11ax standard. Most new adapters, wireless computers,

and mobile devices support 802.11ax and are backward compatible with older standards.

Figure 19-39

A wireless network adapter with two antennas supports 802.11a/b/g/n/ac/ax Wi-Fi standards



Source: [Amazon.com](https://www.amazon.com), Inc.

Now let's look at the various features and settings of a wireless access point needed to secure the wireless network.

Note 4

When configuring your wireless access point, it's important you are connected to the router using a wired connection. If you change a wireless setting and you are connected wirelessly, your wireless connection will be dropped immediately, and you will not be able to continue configuring the router until you connect again.

Require a Security Key

The most common and effective method of securing a wireless network is to require a security key before a client can connect to the network. By default, a network that uses a security key encrypts data traversing the network. Use the router firmware to set the security key. For best security, enter a security key that is different from the password for the router's firmware utility.

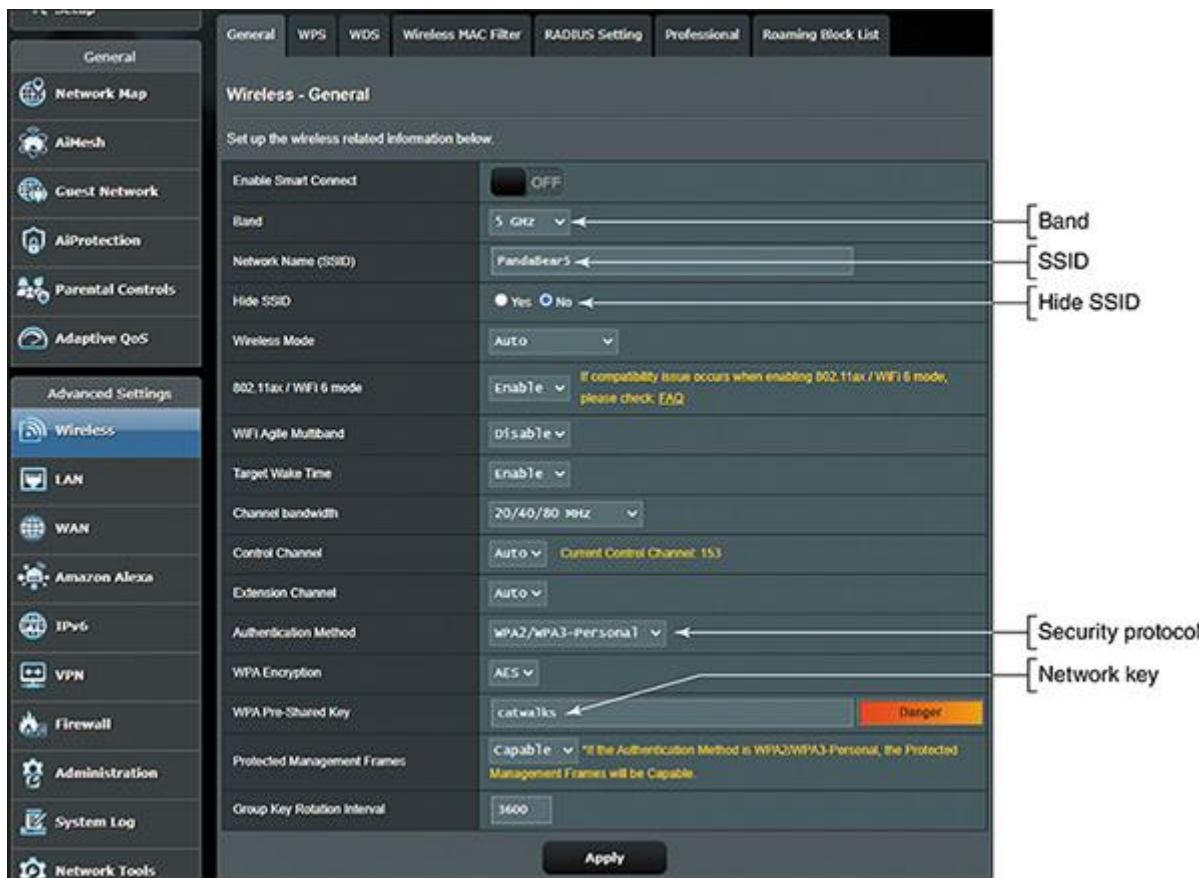
Note 5

When it comes to making secure passwords and passphrases, longer is better and randomness is crucial. To make the strongest passphrase or security key, use a random group of numbers, uppercase and lowercase letters and, if allowed, at least one symbol. At the bare minimum, use at least eight characters in the passphrase.

For our sample router, to set the security keys, click **Wireless** in the left pane. On the **General** tab, notice the key must be set for each Wi-Fi band, 2.4 GHz and 5 GHz (see [Figure 19-40](#)). Here, the security key is called the WPA Pre-Shared Key. Click **Apply** to save your changes.

Figure 19-40

Configure the router's wireless access point



Change the Default SSID and Disable SSID Broadcasting

The **Service Set Identifier (SSID)** is the name of a wireless network. Referring back to [Figure 19-40](#), you can see that each frequency band has its own SSID, and you can change that name. Each band is its own wireless network, which is connected by the access point (router) to the local wired network. When you assign an SSID that includes 2.4 or 5 in the name

(PandaBear5 in [Figure 19-40](#)), a user can more easily select the network using the 5 GHz band in order to get the faster speeds.

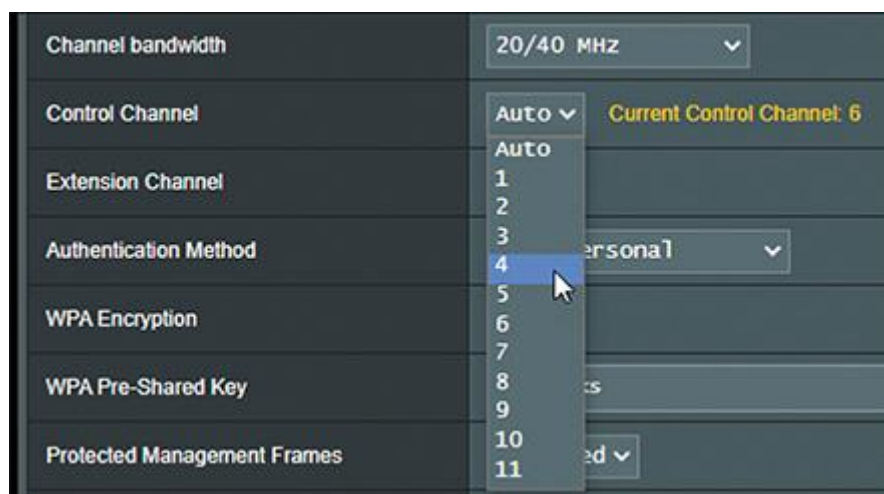
Also notice in [Figure 19-40](#) the option to Hide SSID, which disables SSID broadcasting. Doing so causes the wireless network to appear as Unnamed or Unknown Network on an end user's device. When a user selects this network, they are given the opportunity to enter the SSID. If they don't enter the name correctly, they will not be able to connect. This security method is not considered strong because software can be used to discover an SSID that is not being broadcast.

Select Channels for the WLAN

A **channel** is a specific radio frequency within a broader frequency. For example, two channels in the 2.4 GHz band are 2.412 GHz and 2.437 GHz. In the United States, eleven channels are available for wireless communication in the 2.4 GHz band. In order to avoid channel overlap, however, devices in the 2.4 GHz band select channels 1, 6, or 11, resulting in three nonoverlapping channels available for use. The 5 GHz band offers up to 24 nonoverlapping channels in the United States, but some of those channels are restricted in certain areas, such as near an airport. For most networks, you can allow auto channel selection so the device scans for the least busy channel. However, if you are trying to solve a problem with interference from a nearby wireless network, you can manually set each network to a different channel and make the channels far apart to reduce interference. For example, in the 2.4 GHz band, set the network on one WAP to channel 1 and set a nearby WAP's network to channel 11. For our sample router, the dropdown menu for channel selection in the 2.4 GHz band is shown in [Figure 19-41](#). To allow the router to automatically select the least busy channel, select **Auto**.

Figure 19-41

Select Auto or a specific channel in the 2.4 GHz range

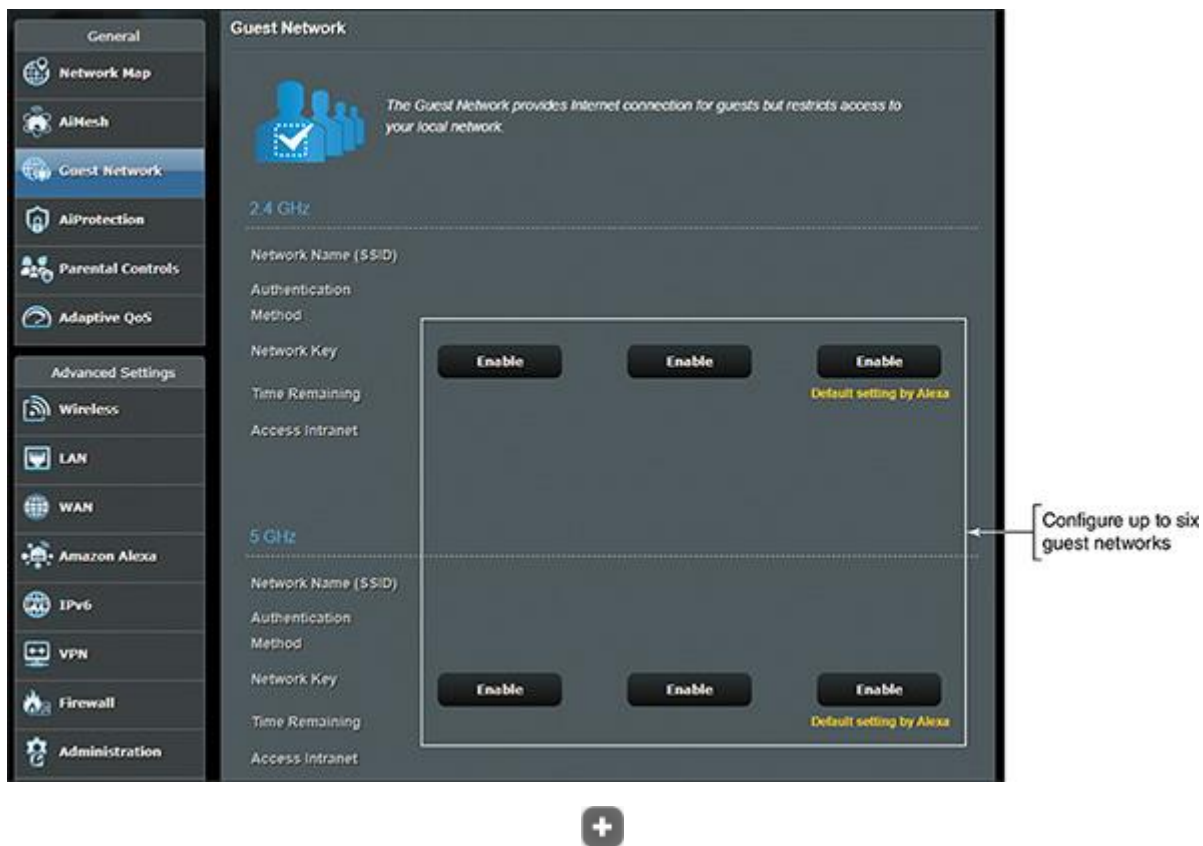


Disable Guest Access

A SOHO router is likely to offer the option to set up guest networks. A guest network provides access to the Internet but does not allow access to the local network. For our sample router, click **Guest Network** in the left pane to see the setup shown in [Figure 19-42](#). Using this window, you can configure up to three 2.4 GHz and three 5 GHz guest networks. Best security practices recommend you not allow guest access and disable these guest networks.

Figure 19-42

Configure up to six guest networks to allow Internet access but not access to the LAN



Set Encryption

When you set a security key, routers by default encrypt wireless transmissions. You can change the encryption protocols used or disable encryption. (Encrypting transmissions increases security but slows down the network; disabling encryption can improve performance and might be appropriate when you are not concerned about transmissions being hacked.) The three main security standards for 802.11 wireless networks are as follows:

- **WPA. WPA (Wi-Fi Protected Access)** is an older encryption standard and typically uses **TKIP (Temporal Key Integrity Protocol**, pronounced “tee-kip”) for encryption. TKIP generates a different key for every transmission; however, the encryption algorithm used for its calculations is no longer considered secure.
- **WPA2. WPA2 (Wi-Fi Protected Access 2)** typically uses **AES (Advanced Encryption Standard)** for encryption, which provides faster and more secure encryption than TKIP. All wireless devices sold today support the WPA2 standard.
- **WPA3. WPA3 (Wi-Fi Protected Access 3)** offers better encryption and additional features over WPA2. For example, you can securely configure a nearby wireless device, such as a wireless webcam or motion sensor, over the wireless network, eliminating the need to connect the device with a wired connection to configure it. Another feature is Individual Data Encryption, which allows a secure connection for your laptop or other wireless device over a public, unsecured Wi-Fi network.

To configure Wi-Fi encryption for our sample router, first know that each band (2.4 GHz and 5 GHz) is assigned its own encryption type. For the most flexibility, set both bands to the highest encryption standards the router and wireless devices support. By selecting WPA2/WPA3-Personal (see [Figure 19-43](#)), a wireless connection will use WPA3 unless an older device does not support it, in which case the connection reverts to WPA2 encryption. Click **Apply** to save your changes.

Figure 19-43

Select the highest encryption standards the network supports



Note 6

Looking back at [Figure 19-40](#), you can see that WPA2/WPA3-Personal is selected as the authentication method. A Personal method relies on a passphrase shared with all network users, which could be compromised. An Enterprise method relies on an authentication server to manage authenticating all users to the network. Very few SOHO networks, however, have the resources to set up and host an authentication server. In most cases, when setting up a SOHO network, your most secure option is Personal.



Exam Tip

The A+ Core 2 exam may give you a scenario that requires you to install and configure a wireless network—including Wi-Fi 802.11 standards, frequencies, channels (1–11)—and encryption protocols including WPA2, WPA3, TKIP encryption, and AES encryption.

Authentication Services in an Enterprise

If you are called on to configure a SOHO router in an enterprise environment, you might need to configure the security protocol with an Enterprise standard, for example, WPA3-Enterprise. In this situation, authentication to the wireless network is done using an authentication server in cooperation with Active Directory on a Windows domain. Three well-known security protocols to provide authentication services for large networks are RADIUS, TACACS+, and Kerberos:

- **RADIUS (Remote Access Dial-In User Service)** protocol was originally designed just for authentication, but it has evolved to include authentication, authorization, and accounting (AAA) services. It works with dial-up, wired and wireless networking, and VPNs. RADIUS uses the UDP protocol and port 1812 for authentication and authorization and port 1813 for accounting.
- **TACACS+ (Terminal Access Controller Access Control System Plus)** is a proprietary Cisco protocol for AAA services, specifically designed for network administrators and technicians to remotely connect to a network to configure and manage Cisco network devices, such as routers, switches, and firewalls. TACACS+ uses TCP protocol and port 49.
- **Kerberos** is strictly an authentication protocol and is used when a Windows computer authenticates a user to Active Directory in a Windows domain. It uses AES encryption, UDP protocol, and port 88. Kerberos supports two-factor authentication, whereas RADIUS and TACACS+ do not.

RADIUS, TACACS+, and Kerberos can each authenticate a user to resources on a network using an authentication server, and that server will most likely turn to Active Directory to authenticate user credentials. The key differences among the three protocols are when and where they are used:

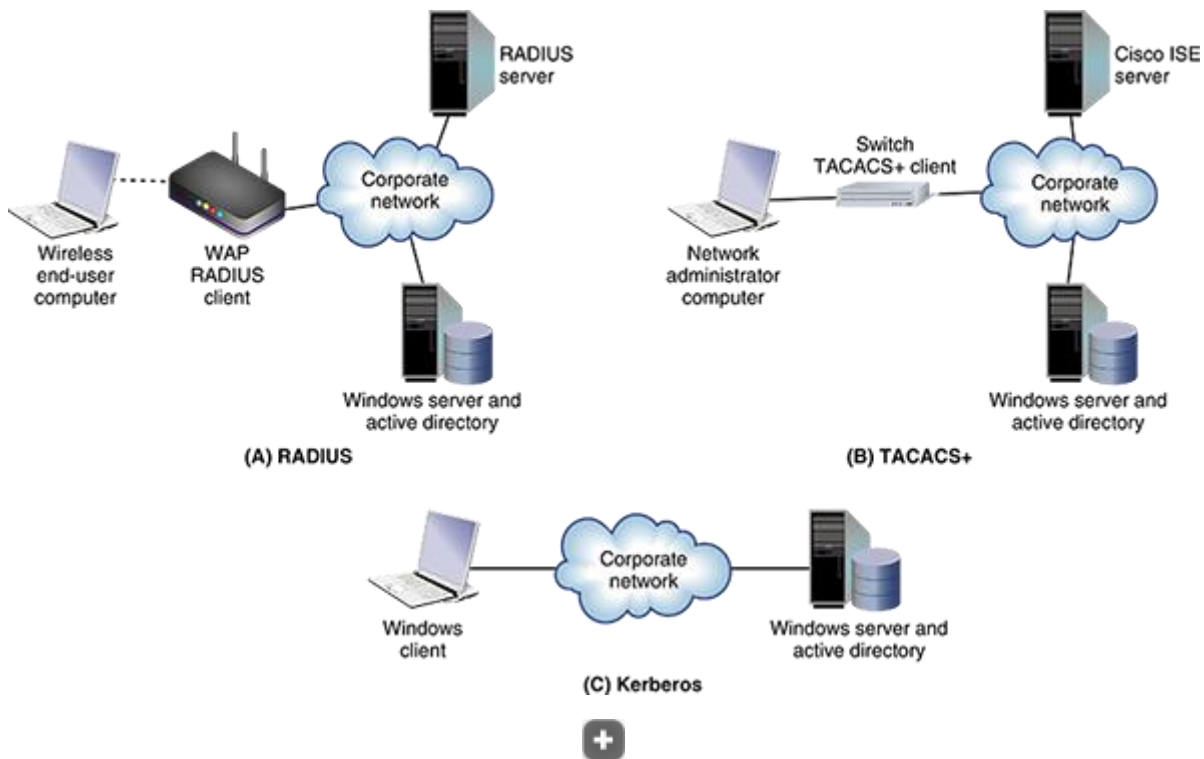
- RADIUS and TACACS+ extend authentication out to non-Windows devices—such as a switch, router, or WAP—to connect a device to the network.
- For a wireless network, RADIUS or TACACS+ is used to authenticate via an authentication server rather than using a network security key.
- TACACS+ is used on Cisco switches, routers, and other networking devices. RADIUS is used on non-Cisco devices, such as an ASUS wireless router.

- Kerberos is used on Windows computers already connected to the network to authenticate to a Windows domain.

Notice in [Figure 19-44](#) that either the WAP using RADIUS or the switch using TACACS+ acts as the client, which is responsible for querying the authentication server before allowing the device on the network. The authentication server interfaces with Active Directory as part of the authentication process. (Cisco calls its TACACS+ server the Identify Service Engine server or ISE server.)

Figure 19-44

Authentication services provided by (A) RADIUS, (B) TACACS+, and (C) Kerberos



To configure RADIUS for wireless authentication using our sample ASUS router, click **Wireless** in the left pane, and click the **RADIUS Setting** tab. See [Figure 19-45](#). Select the wireless band, and enter the IP address of the RADIUS authentication server and the Connection Secret, which is used to generate encrypted messages to the server. Notice in the figure the RADIUS port on the server is 1812, which is the default RADIUS port.

Figure 19-45

Configure RADIUS for network authentication in an enterprise

Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	2.4 GHz
Server IP Address	
Server Port	1812
Connection Secret	

Apply



Note 7

Often, a basic WAP isn't smart enough to act as the RADIUS or TACACS+ client. In an enterprise environment, many WAPs are connected to a wireless controller device in the data closet, which in turn does the work of managing client requests to the RADIUS or ISE server.



Exam Tip

The A+ Core 2 exam expects you to be able to compare and contrast RADIUS, TACACS+, and Kerberos, including identifying which authentication protocol supports multifactor authentication.

19-3 Using Remote Access Technologies

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

An IT technician often finds it necessary to remotely access systems they support and use. You might need to remotely transfer files, access your Windows desktop or a corporate server, access monitoring and management software that you are using to oversee critical systems, assist users by accessing their systems with screen sharing, or support corporate video conferencing.

Several methods and tools to help with these tasks have already been covered in previous modules. In this section of this module, we summarize

tools already covered, look at some new ones, and consider security issues when using these tools. Let's begin with file transfers.

19-3a File Transfers over the Internet

Core 2 Objective

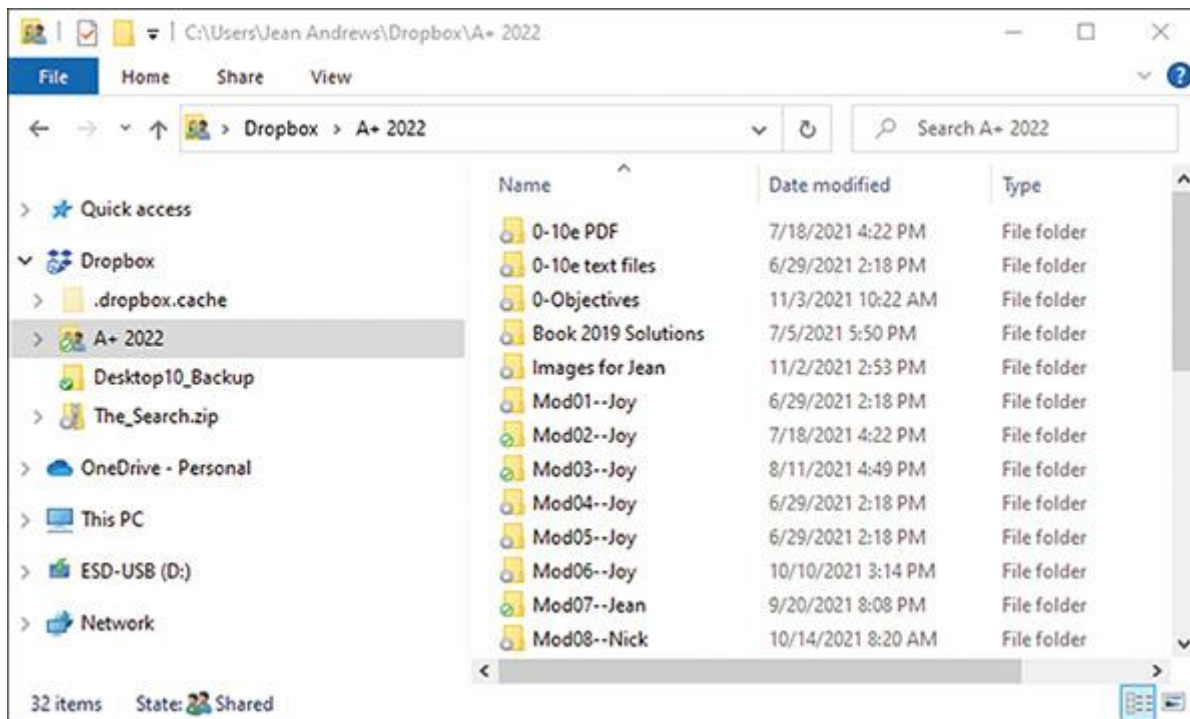
- 4.9

sGiven a scenario, use remote access technologies.

In previous modules, you learned about FTP, the tried-and-true tool to transfer files over a network or the Internet. FTP software is free and easy to install, but it has some limitations. Services on the web that have slowly replaced FTP as the file transfer tool of choice include OneDrive (onedrive.live.com), Dropbox (dropbox.com), Box (box.com), Google Drive (drive.google.com), and other web-based solutions. [Figure 19-46](#) shows OneDrive and Dropbox embedded in Explorer in Windows 10.

Figure 19-46

The author team keeps files for this text in Dropbox



Comparing Dropbox to FTP, Dropbox is faster, more secure, and easier to use. FTP uses the FTP protocol and incoming and outgoing ports 20 and 21. With FTP, several commands pass back and forth before a file can be

transferred, causing a slower transfer process. Dropbox uses a single HTTPS connection for both uploads and downloads, and it can compress files before transferring. In addition, Dropbox is able to upload only the parts of a file (call the diff or difference) that have changed since the last upload, and it can upload a file in segments to multiple IP addresses, further speeding up the process.

19-3b Windows 10/11 Remote Control Tools

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

Windows 10/11 offers two solutions to remotely access a computer: Remote Desktop Connection and Microsoft Remote Assistance. Both tools use the RDP protocol and port 3389 and require a little setup to use. Let's see how each works.

Remote Desktop Connection (RDC)

Remote Desktop Connection (RDC), commonly called Remote Desktop, gives a user access to a Windows desktop from anywhere on the Internet. As a software developer, I find Remote Desktop extremely useful when I work from a remote location (my home office) and need to access a corporate network to support software on that network. Using the Internet, I can access a file server on these secured networks to make my software changes. Remote Desktop is easy to use and relatively safe for the corporate network. To use Remote Desktop, the computer you want to remotely access (the server) must be running business or professional editions of Windows 10/11, but the computer you're using to access it (the client) can be running any version of Windows.



Exam Tip

The A+ Core 2 exam expects you to know how to use Remote Desktop and Remote Assistance and to know which port and protocol they use and which tool is appropriate in a given scenario.

Applying Concepts

Configuring Remote Desktop on Two Computers

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 4.9

The host or server computer is the computer that serves up Remote Desktop to client computers that can “remote in to” (remotely access) the server. To prepare your host computer, you need to configure it for static IP addressing and then configure the Remote Desktop service. Here are the steps needed:

1. **1**
Configure the computer for static IP addressing.



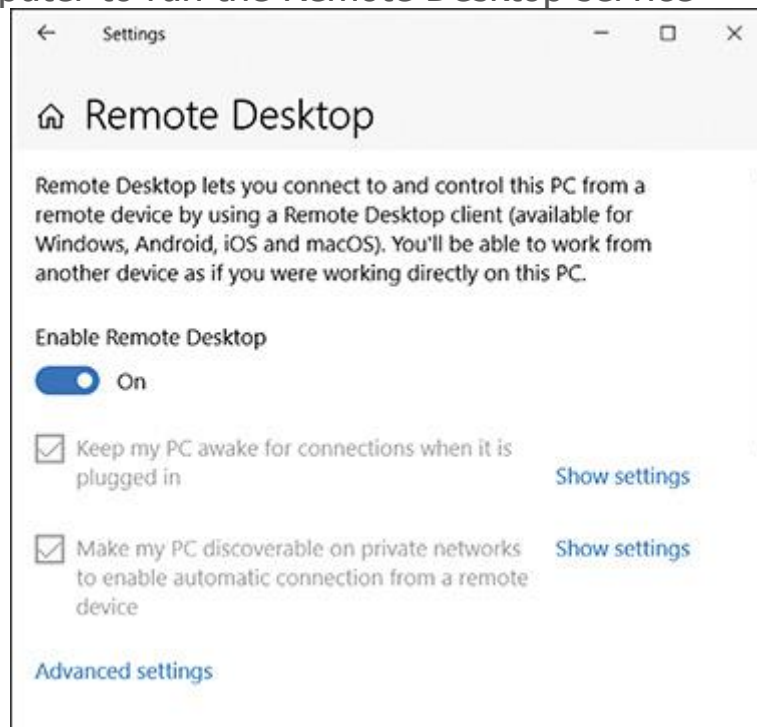
Core to Core

How to assign a static IP address is covered in the Core 1 module “[Networking Fundamentals](#).”

2. **2**
If your computer is behind a firewall, configure the router for port forwarding and allow incoming traffic on port 3389. Forward that traffic to the IP address of your desktop computer.
3. **3**
To turn on the Remote Desktop service, right-click **Start** and click **System**. In the About window, click **Remote desktop**. In the Remote Desktop window (see [Figure 19-47](#)), enable Remote Desktop. You can also control other Remote Desktop settings from this window.

Figure 19-47

Configure a computer to run the Remote Desktop service



Note 8

Server applications such as Remote Desktop listen for network activity from clients. If you want these server applications to be available at all times, you can set your network adapter properties to Wake-on-LAN, which you learned about in the Core 1 module “[Networking Fundamentals](#).”

4. **4**

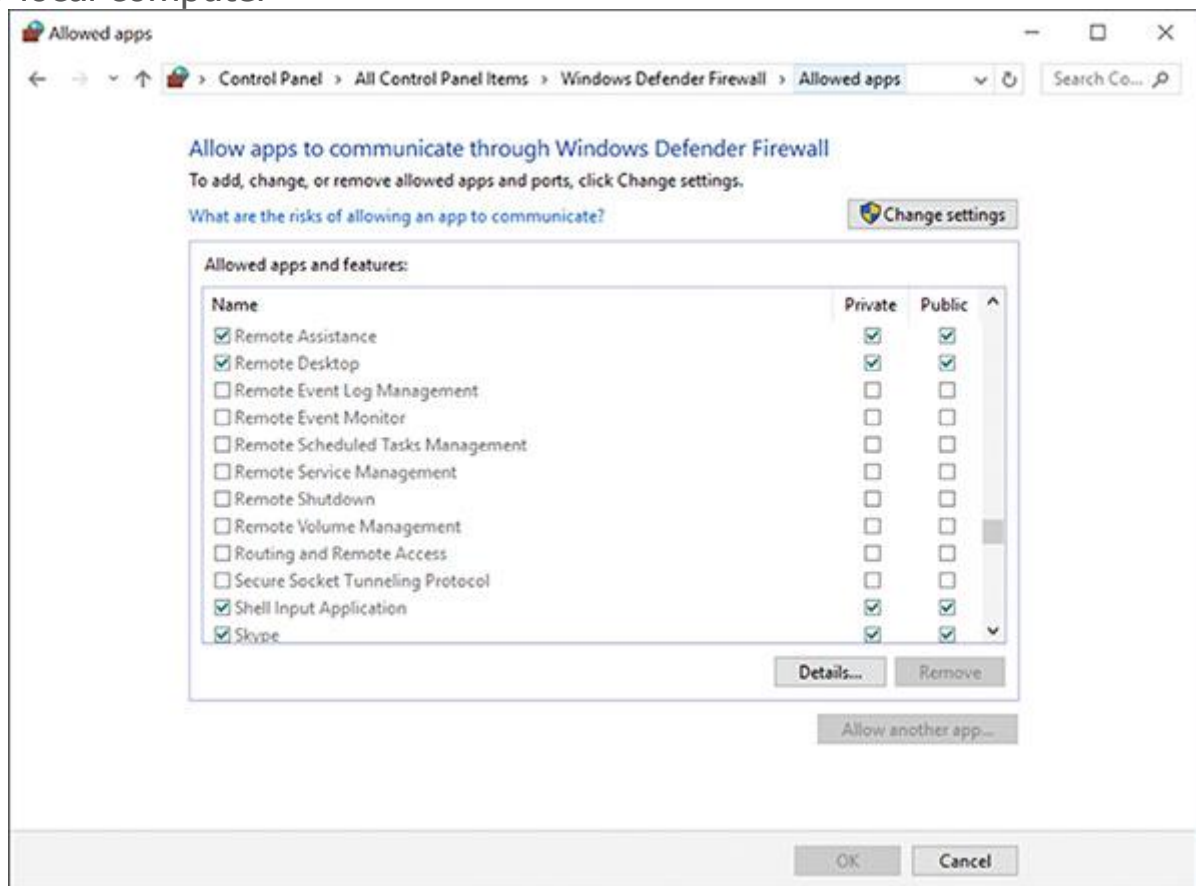
To verify that Windows Defender Firewall is set to allow Remote Desktop activity on this computer, open **Control Panel** in classic view, and click **Windows Defender Firewall**. In the Windows Defender Firewall window, click **Allow an app or feature through Windows Defender Firewall**.

5. **5**

The Allowed apps window appears. Scroll down to Remote Desktop, and adjust the settings as needed (see [Figure 19-48](#)). Click **OK** to apply any changes. You are now ready to test Remote Desktop.

Figure 19-48

Allow Remote Desktop communication through Windows Defender Firewall on your local computer



Try to use Remote Desktop from another computer somewhere on your local network, and make sure it works before testing the Remote Desktop connection from the Internet. On the client computer, you can start Remote Desktop to remote in to your host computer by using **Microsoft Terminal Services Client (mstsc.exe)**.

Follow these steps to use Remote Desktop:

1. **1** Sign in to Windows with an administrator account. Enter **mstsc** in the Windows 10/11 search box. The Remote Desktop Connection box opens (see [Figure 19-49](#)).

Figure 19-49

The IP address of the remote computer can be used to connect to it



2. **2** Enter the IP address or the host name of the computer to which you want to connect. If you decide to use a host name, begin the name with two backslashes, as in `\\CompanyFileServer`.

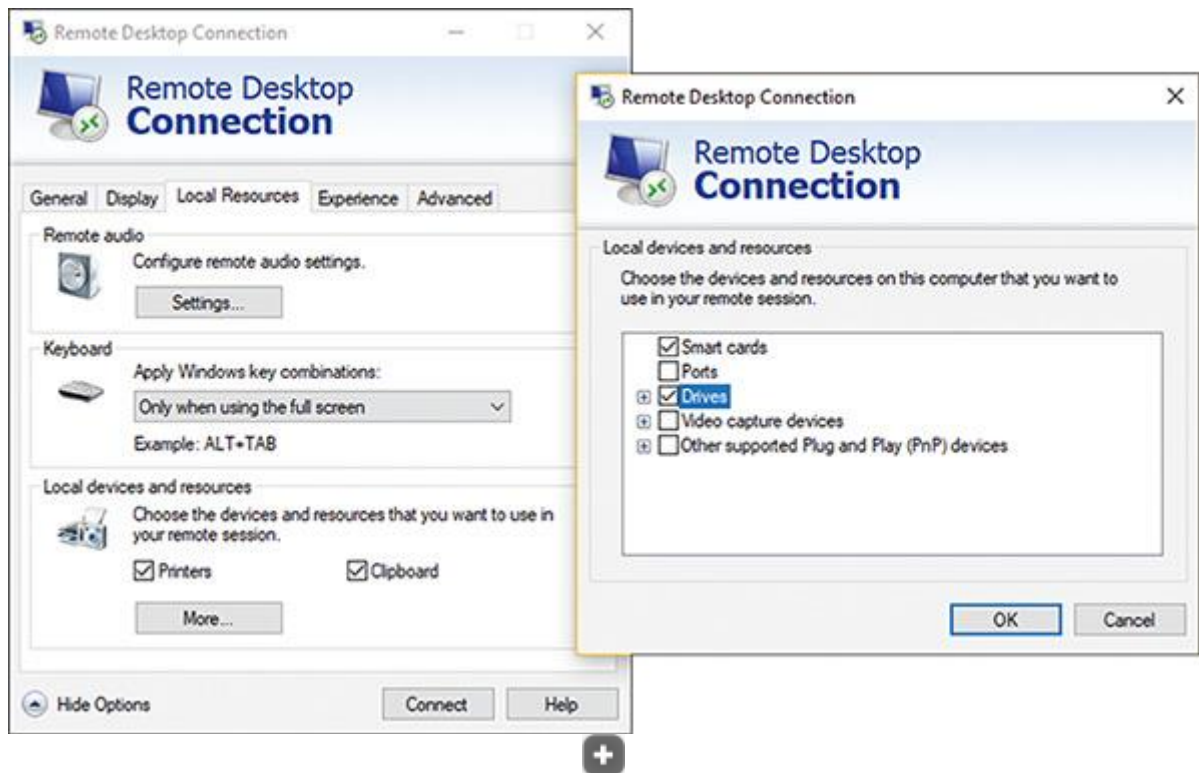
Note 9

If you have trouble using the host name to make a Remote Desktop connection on a local network, try entering the host name and IP address of the remote computer in the hosts file in the C:\Windows\System32\drivers\etc folder of the client computer.

3. **3** If you plan to transfer files from one computer to the other, click **Show Options**, and then click the **Local Resources** tab, as shown on the left side of [Figure 19-50](#). Click **More** to see the dialog box on the right side of the figure. Check **Drives** and click **OK**. Click **Connect** to make the connection. If a warning box appears, click **Connect** again. If another warning box appears, click **Yes**.

Figure 19-50

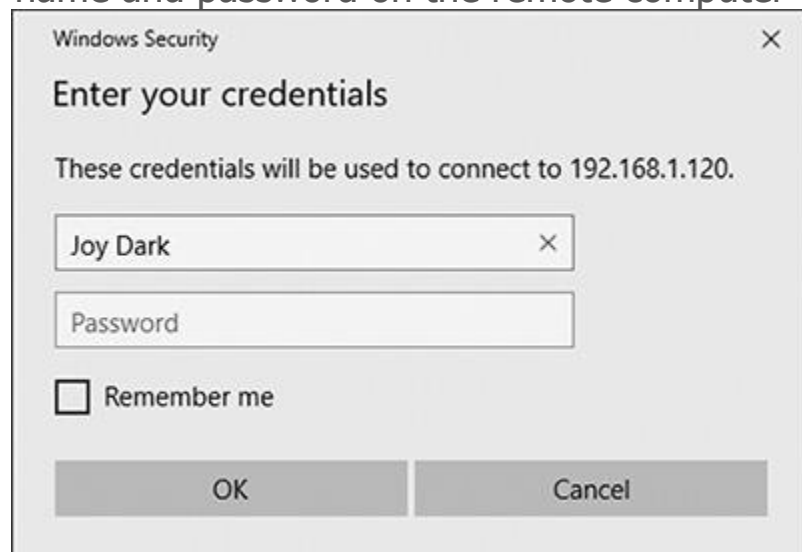
Allow drives and other devices to be shared using the Remote Desktop Connection



4. **4** A Windows Security dialog box is displayed by the remote computer (see [Figure 19-51](#)). Sign in with an administrator user name and password for the remote computer. If a warning box reports that the remote computer might not be secure, click **Yes** to continue the connection.

Figure 19-51

Enter your user name and password on the remote computer



5. **5** The desktop of the remote computer appears with a toolbar at the top of the screen, as shown in [Figure 19-52](#). Click **Restore Down** to show both the remote desktop and the local desktop on the same screen, as shown in [Figure 19-53](#).

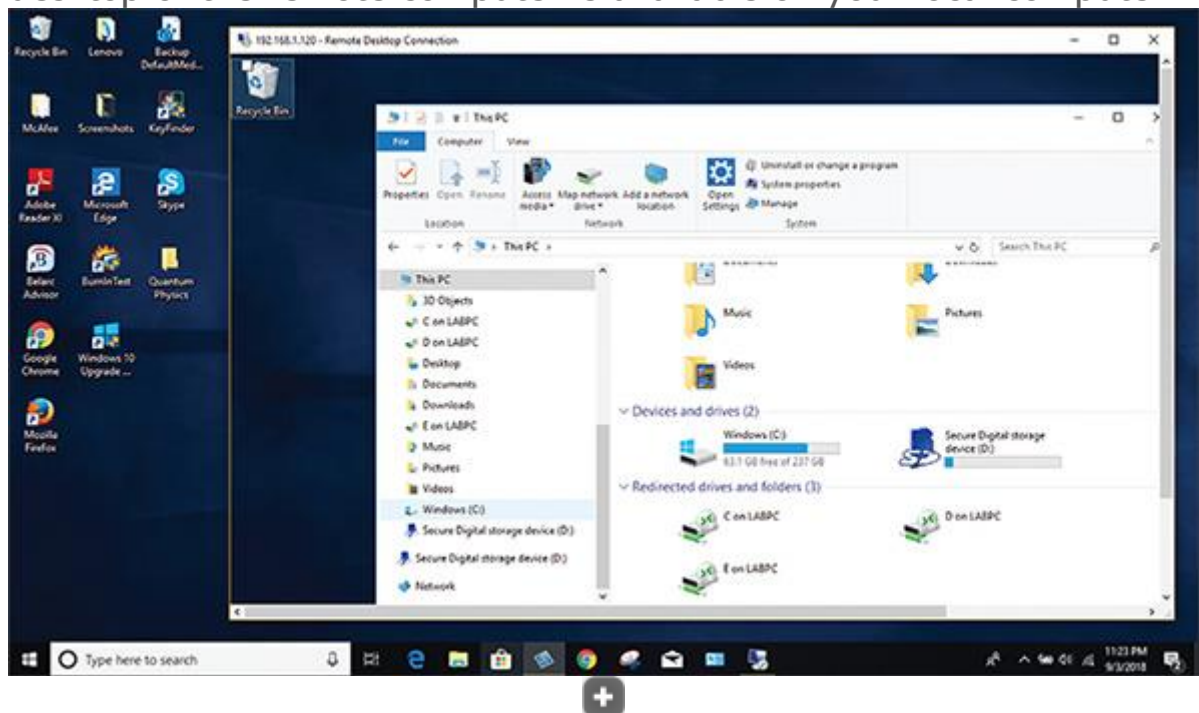
Figure 19-52

The RDC connection toolbar is pinned to the top of the window showing the remote computer's screen



Figure 19-53

The desktop of the remote computer is available on your local computer



Note 10

When a remote desktop connection is made, the user sitting at the remote computer will see it return to the Windows sign-on screen.

When you click in the remote desktop's window, you can work with the remote computer just as if you were sitting in front of it, except response time is slower. To move files back and forth between computers, use Explorer on the remote computer. Files on your local computer and on the remote computer will appear in the Explorer window on the remote computer. For example, you can see drive C: on each computer labeled in [Figure 19-53](#). To close the connection to the remote computer, sign out from the remote computer or close the desktop window.

Note 11

Even though Windows normally allows more than one user to be signed in at the same time, this is not the case with Remote Desktop. When a Remote Desktop session is open, all local users on the remote computer must sign out after receiving a warning.

Is your host computer as safe as it was before you set it to serve up Remote Desktop and enabled port forwarding to it? Actually, no, because a port has been opened, so take this into account when you decide to use Remote Desktop.

Microsoft Remote Assistance (MSRA)

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

Microsoft Remote Assistance (MSRA) differs from Remote Desktop in that a user on the server computer can remain signed in during the remote session, retains control of the session, and can see the screen. This is helpful when troubleshooting problems on a computer. The user who needs your help sends you an invitation by email or chat to connect to their computer using Remote Assistance. When you respond to the invitation, you can see the user's desktop just as they see it; if the user gives you permission, you can take control of their computer to change settings or do whatever else is needed to fix their problem or show them how to perform a task. Think of Remote Assistance as a way to provide virtual desk-side support.

There are several ways to initiate a Remote Assistance session. The first method listed is the most reliable:

- The user saves an invitation file and then sends that file to the technician. The file can be sent by any method, including email, chat, or posting to a shared folder on the network.
- The user can send an automated email through the Remote Assistance app. This option only works if the system is configured with a compatible email program.
- The user can use Easy Connect, which is the easiest method to start a Remote Assistance connection, but it only works if both computers

used for the connection are using Windows. Also know that some routers don't support the Peer Name Resolution Protocol (PNRP), which is the protocol Easy Connect uses to establish a Remote Assistance connection.

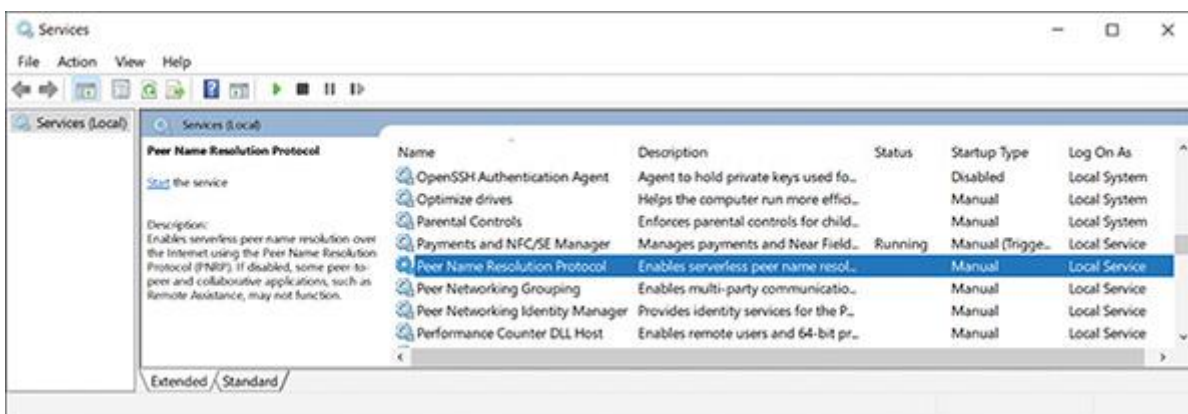
- The technician can initiate a session. This method is the most difficult to use; it requires that Group Policies be applied on the technician's computer.

Note 12

Easy Connect is the easiest method for the user when initiating a Remote Assistance connection, but it can be the most difficult for the technician to set up. If Easy Connect is grayed out when starting a session, chances are that the PNRP service might be down. To start the service, enter the **services.msc** command to open the Services console (see [Figure 19-54](#)). Select **Peer Name Resolution Protocol**, and click **Start**.

Figure 19-54

Use the Services console to start a service

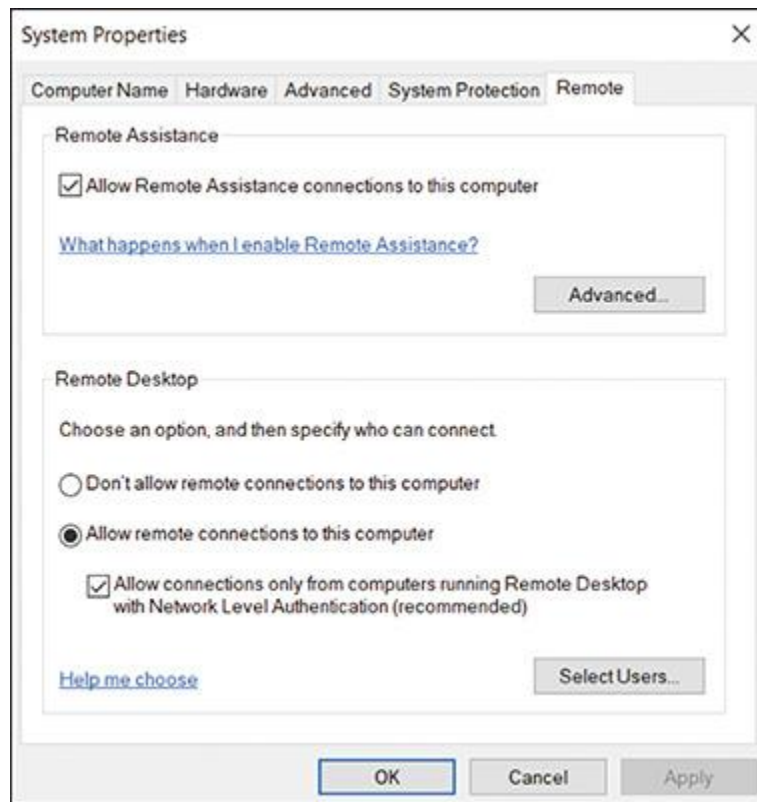


To initiate a Remote Assistance connection when the user sends an invitation to the technician, follow these steps:

1. To allow Remote Assistance sessions on the user's computer, called the host computer, right-click **Start**, and click **System**. In the About window, click **System protection**. In the System Properties dialog box, click the **Remote** tab. See [Figure 19-55](#).

Figure 19-55

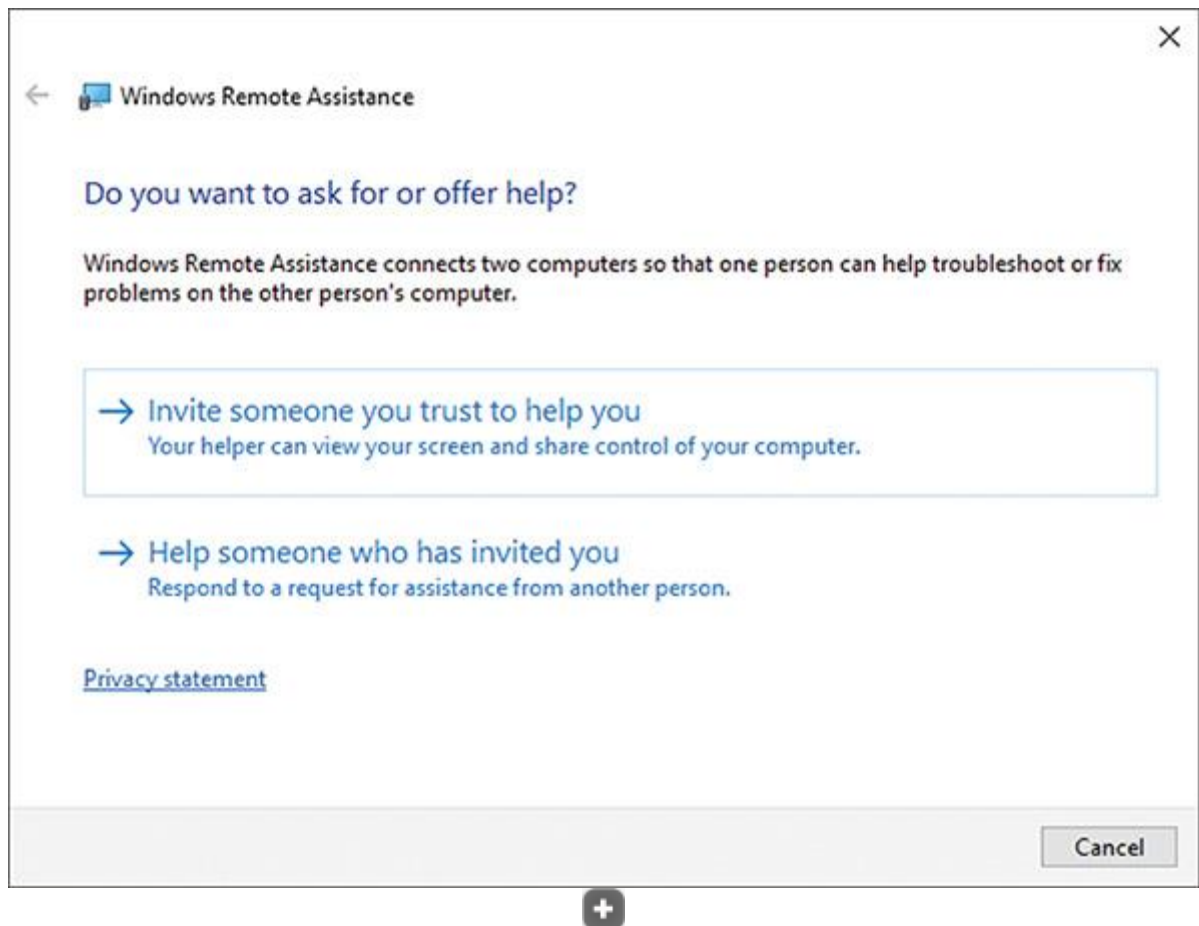
Configure a computer to allow Remote Assistance connections



2. **2** In the Remote Assistance area, check **Allow Remote Assistance connections to this computer**, and then click **OK**.
3. **3** In the search box, type **remote assistance**, and then click **Invite someone to connect to your PC and help you, or offer to help someone else**. The Windows Remote Assistance box appears, as shown in [Figure 19-56](#).

Figure 19-56

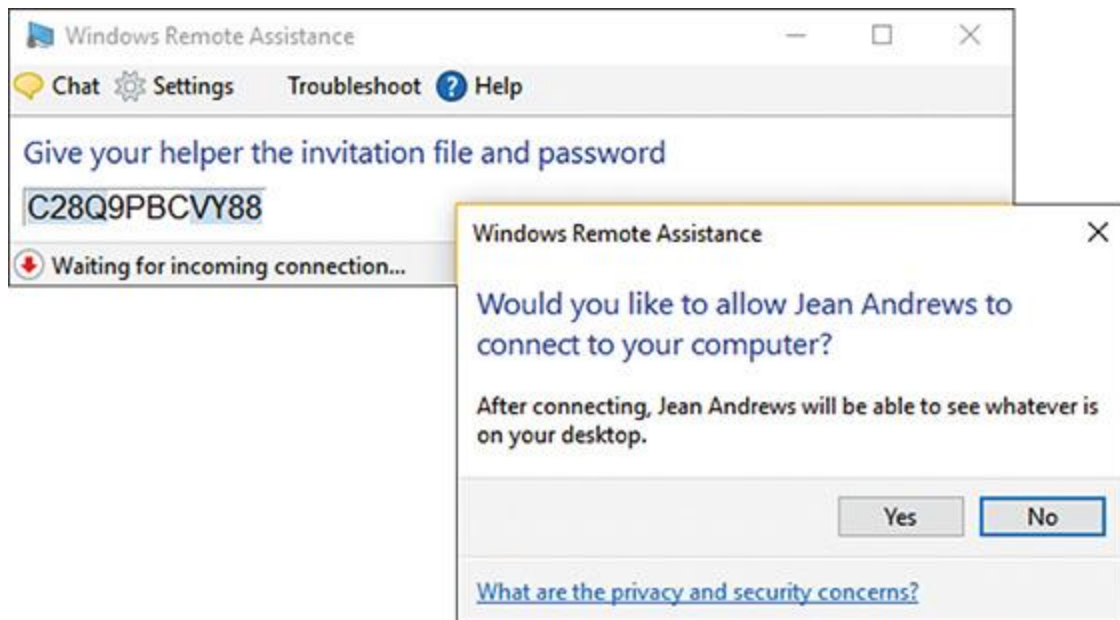
Create or respond to an invitation to connect



4. **4** Click **Invite someone you trust to help you**, and then click **Save this invitation as a file**. Point to a location to save the file, and click **Save**. Remote Assistance provides a password for the user to give the technician in order to create the connection (see the left side of [Figure 19-57](#)). The user can send the invitation file to the technician as an email attachment or by other means.

Figure 19-57

The user's computer shows a password the technician must enter to connect Remote Assistance

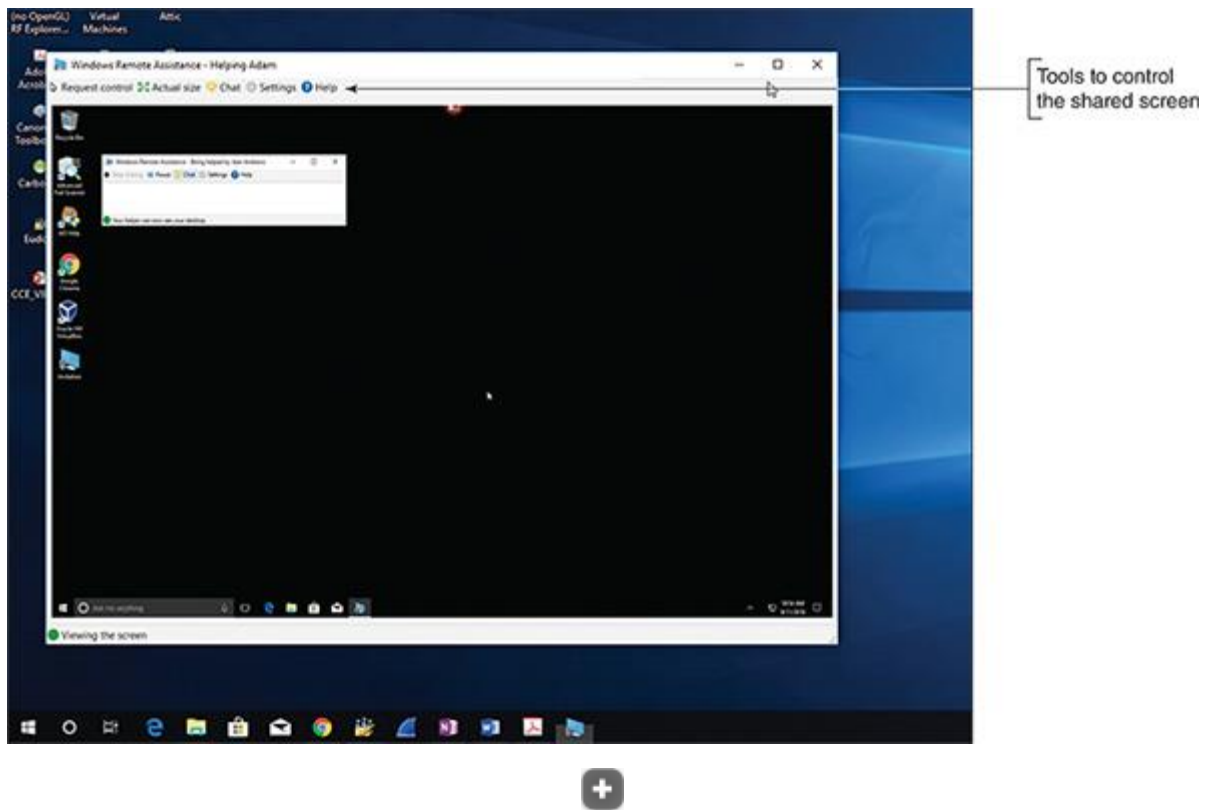


The technician can respond to the invitation into Remote Assistance as follows:

1. On the technician's computer, the technician double-clicks the invitation file they received from the user. In the box that appears, the technician enters the password that appeared on the user's screen, and clicks **OK**. (Most often, the user reads the password to the technician over the phone.)
2. The user's computer generates a warning box requesting permission for the technician's computer to connect (see the right side of [Figure 19-57](#)). The user clicks **Yes** to allow the connection. The user's desktop turns black, and the Remote Assistance management window appears. The technician's computer opens the Windows Remote Assistance window, as shown in [Figure 19-58](#), with a live feed from the user's computer.

Figure 19-58

Control the shared screen using the toolbar options at the top



With Remote Desktop, you can share files between computers, but Remote Assistance does not allow for file sharing. Here are some things you can do during a Remote Assistance session:

- To open a chat session with the user, click the **Chat** icon. A chat pane appears in the Remote Assistance window on both desktops.
- To ask the user if you can take control of their desktop, click **Request control** in the Remote Assistance control window. When the user accepts the request, you can control their computer. The user can stop sharing control by clicking **Stop sharing**.
- The user can hide their desktop from you at any time by clicking **Pause** in the control window.
- Either of you can disconnect the session by closing the control window.
- A log file is kept of every Remote Assistance session in the C:\Users\username\Documents\Remote Assistance Logs folder. The file includes the chat session. If you type instructions during the chat session that will be helpful for the user later, they can use the log file to remind them of what was said and done.
- If an invitation created by a user is not used within six hours, the invitation expires. This time frame can be changed by clicking **Advanced** in the Remote Assistance section on the Remote tab of the System Properties dialog box.

If you have problems making the connection, consider the following:

1. Windows Defender Firewall on the user's computer might be blocking Remote Assistance. Verify that Remote Assistance is checked as an exception to blocked apps in the Windows Defender Firewall window.
2. If you are outside the user's local network, the hardware firewall protecting their network might be blocking Remote Assistance. Verify that port forwarding on that hardware firewall is enabled for Remote Assistance. Remote Assistance uses port 3389, the same RDP port used by Remote Desktop.

Note 13

Because Remote Assistance can be difficult to set up, Windows 10/11 offers Quick Assist, which is more universally compatible with existing network hardware configurations. For Quick Assist to work, both computers must be running Windows 10 or Windows 11, the technician providing assistance must have a Microsoft account, and the person receiving the connection must agree to it by entering a code generated by the technician's client computer.

19-3c Virtual Network Computing (VNC)

Core 2 Objective

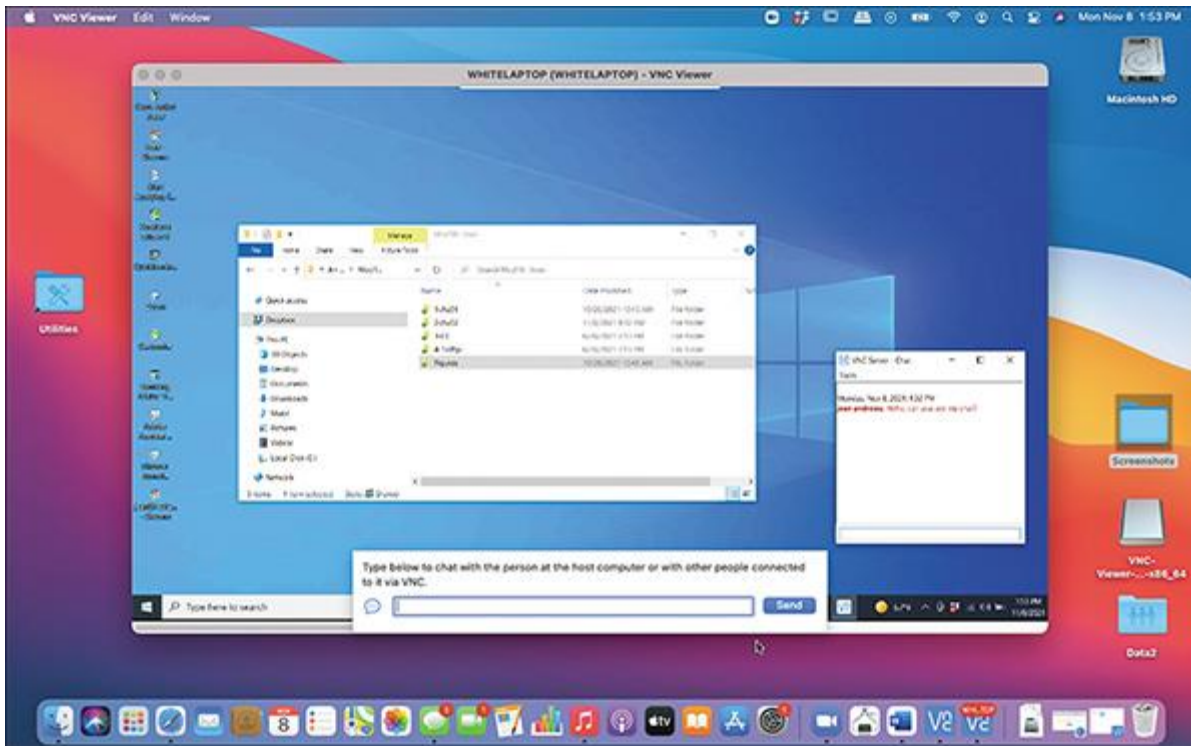
- 4.9

Given a scenario, use remote access technologies.

Virtual Network Computing (VNC) is client/server software used to remotely control a computer, file transfers, and screen sharing. VNC Connect (realvnc.com) by RealVNC is one example of this type of software. See [Figure 19-59](#). It can be used for virtual desktop support and unattended access to a remote computer. When used for virtual desktop support, the person being helped can watch what the technician does with their computer and interact as needed. VNC uses port 5901 and the Remote Framebuffer Protocol, which provides a simple way of communicating where images of the desktop and keystrokes are passed between client and server. The server side of VNC—the computer being controlled—can be installed in Windows, Linux, and macOS. The client side of VNC, called the viewer, controls the other computer and can be installed in Windows, UNIX, Linux, macOS, Android, and iOS.

Figure 19-59

A Mac computer uses a VNC viewer to remotely control a Windows 10 computer acting as the VNC server



Weaknesses of VNC include the large volume of screen data transferred during a session and poor encryption that can be hacked. To secure a VNC session, you can use a VPN connection, which encrypts the session end to end. Alternately, for Linux systems, you can use an SSH tunnel to encrypt the connection. In a project at the end of this module, you practice using a VNC session to remotely control a Windows computer.

19-3d Secure Shell (SSH)

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

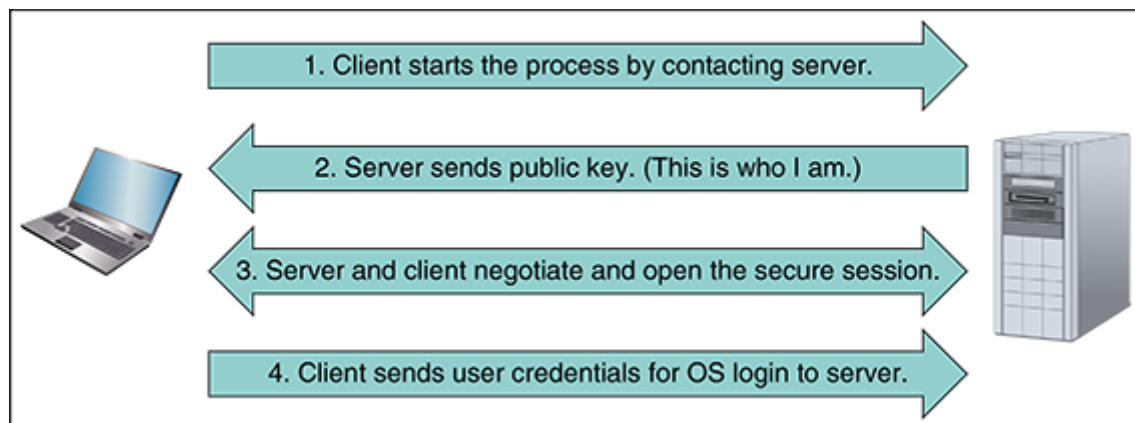
Secure Shell, also called the **SSH protocol**, is open-source software to remotely sign in to and control another computer. It was designed to replace Telnet and FTP on Linux systems. Recall from the Core 1 module [“Networking Fundamentals”](#) that Telnet can remotely control another computer, and FTP is used for file transfers; neither of these programs encrypts transmissions. Secure Shell encrypts the entire session, including the authentication of credentials used to sign in. The server end of Secure Shell is preinstalled in most UNIX and Linux systems. A well-known client program for Secure Shell is PuTTY (putty.org), a file transfer program available in Linux and Windows. You can establish a secure session between a client computer and Linux server using Secure Shell and then run another

program, such as a VNC program, over the Secure Shell connection using tunneling.

Secure Shell uses port 22 and creates an encrypted session using a method called public key encryption with two SSH keys. See [Figure 19-60](#). The SSH client starts the process by contacting the server and requesting its public SSH key. The server sends the public key and starts negotiating the parameters of the secure channel. The client uses the public key to authenticate the server and uses its own private key to encrypt the user's credentials, which are sent to the server for the server to authenticate the user to the server OS. In a project at the end of this module, you learn to use SSH and PuTTY.

Figure 19-60

Public key encryption is used to secure an SSH session



19-3e Remote Monitoring and Management (RMM)

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

Remote Monitoring and Management (RMM) software, such as RMM by Atera (atera.com), is installed on systems to monitor and manage these systems remotely so IT personnel can more easily support these systems. RMM software can be used in-house to help the internal IT department better do its job, or it can be used by a managed services provider (MSP), which is an IT organization that a company contracts with to support its IT needs. RMM software features include the ability to monitor systems in real time, send alerts to management and IT personnel when potential problems arise, automatically run scripts (for example, backup scripts and scripts to

install security patches), and analyze and report system performance and reliability.

19-3f Security Benefits of Third-Party Tools

Core 2 Objective

- 4.9

Given a scenario, use remote access technologies.

You've just learned about several screen-sharing, video-conferencing, file transfer, desktop management, and RMM software suites. When evaluating the security risks of one of these types of programs, consider whether the program requires you to open a port to your network. For example, Remote Desktop and Remote Assistance both require you to open port 3389, which is a security risk. Third-party remote access software executed from a browser window is more secure because the browser initiates communication outside the protected network, and opening listening ports is not required. Examples of this type of software, some of which are free, are TeamViewer ([teamviewer.com](https://www.teamviewer.com)), GoToMyPC by Citrix ([gotomypc.com](https://www.gotomypc.com)), LogMeIn ([logmein.com](https://www.logmein.com)), and Zoom (zoom.us). When evaluating third-party remote access applications, consider the following:

- Where is software installed—on the host, on the client, or on both computers?
- How secure is the connection? Are you required to open incoming ports?
- How are live screens shared? For example, is a live screen shared only by the host computer, or can it be shifted to another computer in the same screen-sharing session?
- Can files be shared in one or both directions during the same screen-sharing session?

19-4 Troubleshooting Network Connections

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

Windows 10/11 includes several utilities you can use to troubleshoot networking problems. In this section of the module, you learn to use ping,

hostname, ipconfig, nslookup, tracert, pathping, two net commands, and netstat. Most of these program files are found in the \Windows\System32 folder.

Exam Tip

The A+ Core 2 exam expects you, when given a scenario, to know when and how to use these network utilities: ping, hostname ipconfig, nslookup, ifconfig, tracert, pathping, net use, net user, and netstat. You should know when and how to use each utility and how to interpret results. In addition, these commands form the foundation you'll need when studying more advanced networking.

Now let's see how to use each utility.

19-4a **ping [-a] [-t] [targetname]**

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **ping** command tests connectivity by sending an echo request to a remote computer. If the remote computer is online, detects the signal, and is configured to respond to a ping, it responds. (Responding to a ping is the default Windows setting, although some companies disable responding to ping, especially on computers that can be reached from the Internet.) Use ping to test for connectivity or to verify that DNS is working. Ping cannot verify other network services on the computer are working. If a ping does not work, after reasonable investigation into the source of the problem, check with a security administrator to determine if the network might be under attack.

Note 14

If a ping to a host using its IP address works, but a ping to the same host using its domain name does not work, DNS is down. Try different DNS servers, such as 8.8.8.8 and 8.8.4.4, the Google public DNS servers.

A few examples of ping are discussed in [Table 19-2](#). Two examples are shown in [Figure 19-61](#).

Table 19-2

Examples of the Ping Command

Ping Command	Description
ping 69.32.208.75	Ping tests for connectivity using an IP address. If the remote computer responds, the round-trip times are displayed.

Ping Command	Description
ping -a 69.32.208.75	The -a parameter tests for name resolution. Use it to display the host name and verify that DNS is working.
ping -t 69.32.208.75	The -t parameter causes pinging to continue until interrupted. To display statistics, press Ctrl+Break. To stop pinging, press Ctrl+C.
ping 127.0.0.1	This is called a loopback address test. The IP address 127.0.0.1 always refers to the local computer. If the local computer does not respond, you can assume there is a problem with the network connection's configuration.
ping cengage.com	Use a host name to find out the IP address of a remote computer. If the computer does not respond, suspect there is a problem with DNS. On the other hand, some computers are not configured to respond to pings.

Figure 19-61

Use ping to test for connectivity and name resolution

```

C:\Users\Jean Andrews>ping 69.32.208.75

Pinging 69.32.208.75 with 32 bytes of data:
Reply from 69.32.208.75: bytes=32 time=23ms TTL=238
Reply from 69.32.208.75: bytes=32 time=23ms TTL=238
Reply from 69.32.208.75: bytes=32 time=24ms TTL=238
Reply from 69.32.208.75: bytes=32 time=22ms TTL=238

Ping statistics for 69.32.208.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 24ms, Average = 23ms

C:\Users\Jean Andrews>ping cengage.com

Pinging cengage.com [69.32.208.75] with 32 bytes of data:
Reply from 69.32.208.75: bytes=32 time=22ms TTL=238
Reply from 69.32.208.75: bytes=32 time=22ms TTL=238
Reply from 69.32.208.75: bytes=32 time=24ms TTL=238
Reply from 69.32.208.75: bytes=32 time=23ms TTL=238

Ping statistics for 69.32.208.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 24ms, Average = 22ms

C:\Users\Jean Andrews>

```

19-4bhostname

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **hostname** command displays the hostname of the computer. The command has no parameters.

19-4c **ipconfig [/all] [/release]** **[/renew] [/displaydns] [/flushdns]**

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **ipconfig (IP configuration)** command can display network configuration information and refresh the TCP/IP assignments for a connection, including its IP address. Some examples of the command are listed in [Table 19-3](#).

Table 19-3

Examples of the Ipconfig Command

Ipconfig Command	Description
ipconfig /all	Displays a network connection's configuration information, including the MAC address.
ipconfig /release	Releases the IP address and other TCP/IP assignments when dynamic IP addressing is being used.
ipconfig /release6	Releases an IPv6 address and other TCP/IP assignments.
ipconfig /renew	Leases a new IP address from a DHCP server. Make sure you release the IP address before you renew it.
ipconfig /renew6	Leases a new IPv6 address from a DHCP IPv6 server. Make sure you release the IPv6 address before you renew it.
ipconfig /displaydns	Displays information about name resolutions that Windows currently holds in the DNS resolver cache.
ipconfig /flushdns	Flushes the name resolver cache, which might solve a problem when the browser cannot find a host on the Internet.

Note 15

Only the more commonly used parameters or switches for each command are discussed in this module. For several of these commands, you can use the `/?` or `/help` parameter to get more information. For even more information about each command, search the docs.microsoft.com site.

19-4d nslookup [computername]

Core 2 Objective

- 1.2

sGiven a scenario, use the appropriate Microsoft command-line tool.

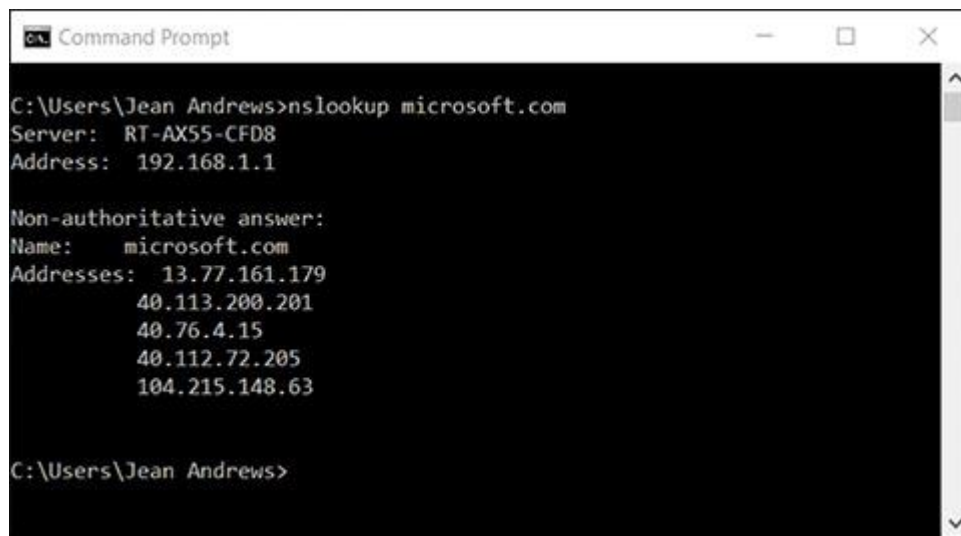
The **nslookup (namespace lookup or name server lookup)** command is used to test name-resolution problems with DNS servers by allowing you to request information from a DNS server's zone data, which is the portion of the DNS namespace that the server knows about. For example, to find out what your DNS server knows about the domain name [microsoft.com](https://www.microsoft.com), enter this command:

```
nslookup microsoft.com
```

[Figure 19-62](#) shows the results. Notice in the figure that the DNS server reports five different IPv4 addresses assigned to [microsoft.com](https://www.microsoft.com). It also reports that this information is nonauthoritative, meaning that it is not the authoritative, or final, name server for the [microsoft.com](https://www.microsoft.com) domain name.

Figure 19-62

The nslookup command reports information about the Internet namespace



```
Command Prompt

C:\Users\Jean Andrews>nslookup microsoft.com
Server: RT-AX55-CFD8
Address: 192.168.1.1

Non-authoritative answer:
Name: microsoft.com
Addresses: 13.77.161.179
           40.113.200.201
           40.76.4.15
           40.112.72.205
           104.215.148.63

C:\Users\Jean Andrews>
```

A **reverse lookup** is when you run the nslookup command to find the host name when you know a computer's IP address, such as:

```
nslookup 69.32.208.75
```

To find out the default DNS server for a network, use the nslookup command with no parameters.

Note 16

The Linux `dig` command gives information similar to the Windows `nslookup` command. You learn to use `dig` in the module “[Linux and Scripting](#).”

19-4e `tracert [targetname]`

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **`tracert (trace route)`** command can be useful when you’re trying to resolve a problem reaching a destination host such as an FTP site or website. The command sends a series of requests to the destination computer and displays each hop to the destination. (A hop happens when a message moves from one router to another.) For example, to trace the route to the *cengage.com* web server, enter this command in a command prompt window:

```
tracert cengage.com
```

The results of this command for one location are shown in [Figure 19-63](#); your results will be different. A message is assigned a Time to Live (TTL), which is the number of hops it can make before a router drops the message and sends an error message back to the host that sent the original message (see [Figure 19-64](#)). The `tracert` command creates its report from these messages. If a router doesn’t respond, the *Request timed out* message appears.

Figure 19-63

The `tracert` command traces a path to a destination computer

```
Command Prompt
C:\Users\Jean Andrews>tracert cengage.com

Tracing route to cengage.com [69.32.208.75]
over a maximum of 30 hops:

 1  2 ms  1 ms  1 ms  RT-AX55-CFD8 [192.168.1.1]
 2  6 ms  2 ms  2 ms  10.2.0.1
 3  *      *      *      Request timed out.
 4  3 ms  3 ms  3 ms  147.253.242.1
 5  7 ms  5 ms  7 ms  te4-2.ar01.dltnga01.bb.ena.net [207.191.191.109]
 6  7 ms  6 ms  7 ms  te0-0-0-6.bb01.atlaga01.bb.ena.net [207.191.191.156]
 7  10 ms 10 ms  9 ms  cinbell.tieatl.telxgroup.net [198.32.132.102]
 8  22 ms 23 ms 23 ms 216.68.14.162
 9  21 ms 21 ms 21 ms 216.68.14.114
10  *      *      *      Request timed out.
11  22 ms 21 ms 21 ms cengage.static.fuse.net [216.68.230.46]
12  22 ms 22 ms 23 ms 69.32.128.159
13  22 ms 24 ms 23 ms puertorico-tienda.cengage.com [69.32.208.75]
14  23 ms 23 ms 23 ms puertorico-tienda.cengage.com [69.32.208.75]

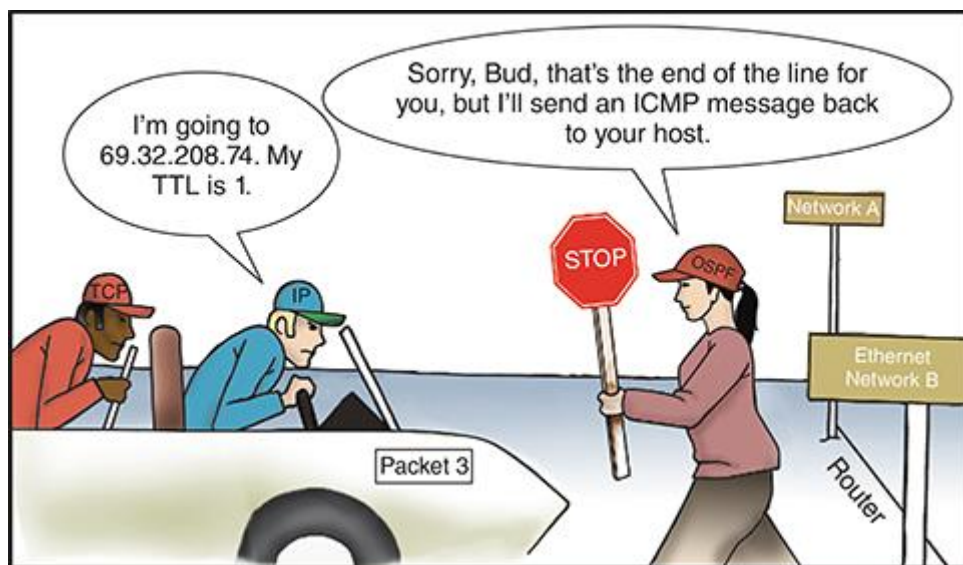
Trace complete.

C:\Users\Jean Andrews>
```



Figure 19-64

A router eliminates a message that has exceeded its TTL



19-4f pathping

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **pathping** command combines the ping and tracert commands into a single command to help identify where on the network path the network might be slow or giving problems. For example, to show problems along the way to the *cengage.com* site, enter this command:

```
pathping cengage.com
```

19-4g The net Commands

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The net command is several commands in one, and most of the net commands require an elevated command prompt window, which allows commands that require administrator privileges in Windows. In this section, you learn about the net use and net user commands. The **net use** command connects or disconnects a computer from a shared resource, or it can display information about connections.

Enter the following commands to pass a user name and password to the \\bluelight remote computer, and then map a network drive to the \Medical folder on that computer:

```
net use \\bluelight\Medical /user:"Jean Andrews"  
mypassword
```

```
net use z: \\bluelight\Medical
```

The double quotation marks are needed in the first command because the user name has a space in it.

A persistent network connection is one that happens at each logon. To make the two commands persistent, add the /persistent parameter like this:

```
net use \\bluelight\Medical /user:"Jean Andrews"  
mypassword /persistent:yes
```

```
net use z: \\bluelight\Medical /persistent:yes
```

To disconnect a network drive, enter this command:

```
net use z: /delete
```

The **net user** command manages user accounts. For example, the built-in administrator account is disabled by default. To activate the account, enter this net user command:

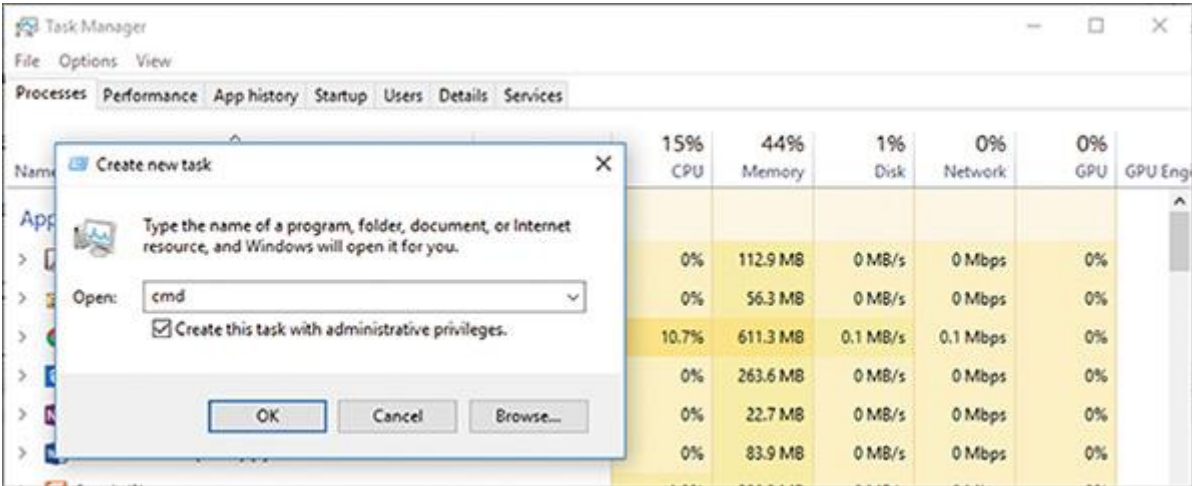
```
net user administrator /active:yes
```

Note 17

One way to get an elevated command prompt window is to open **Task Manager**, click **File**, click **Run new task**, type `cmd`, check **Create this task with administrative privileges**, and then click **OK**. See [Figure 19-65](#). The command prompt window that opens has Administrator in the title bar.

Figure 19-65

Open an elevated command prompt window



19-4hnetstat [-a] [-b] [-o]

Core 2 Objective

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

The **netstat (network statistics)** command gives statistics about network activity, and it includes several parameters. [Table 19-4](#) lists a few netstat commands.

Table 19-4

netstat Commands

netstat Command	Description
netstat	Lists statistics about the network connection, including the IP addresses of active connections.
netstat >>netlog.txt	Directs output to a text file.
netstat -b	Lists programs that are using the connection (see Figure 19-66) and is useful for finding malware that might be using the network. The -b switch requires an elevated command prompt.

netstat Command	Description
netstat -b -o	Includes the process ID of each program listed. When you know the process ID, you can use the taskkill command to end the process.
netstat -a	Lists statistics about all active connections and the ports the computer is listening on.
netstat -na	List all open ports.

Figure 19-66

netstat -b lists programs that are using a network connection

```

C:\WINDOWS\system32>netstat -b

Active Connections

Proto Local Address          Foreign Address        State
TCP    127.0.0.1:668            WHITELAPTOP:1102      ESTABLISHED
[carboniteservice.exe]
TCP    127.0.0.1:668            WHITELAPTOP:1103      ESTABLISHED
[carboniteservice.exe]
TCP    127.0.0.1:1102           WHITELAPTOP:668       ESTABLISHED
[CarboniteUI.exe]
TCP    127.0.0.1:1103           WHITELAPTOP:668       ESTABLISHED
[CarboniteUI.exe]
TCP    127.0.0.1:1198           WHITELAPTOP:1199      ESTABLISHED
[Dropbox.exe]
TCP    127.0.0.1:1199           WHITELAPTOP:1198      ESTABLISHED
[Dropbox.exe]
TCP    192.168.1.233:1050       52.226.139.121:https   ESTABLISHED
WpnService
[svchost.exe]
TCP    192.168.1.233:1074       40.97.31.50:https      ESTABLISHED
[OUTLOOK.EXE]
TCP    192.168.1.233:1075       40.97.31.50:https      ESTABLISHED
[OUTLOOK.EXE]

```

Note 18

Other important net commands are net localgroup, net accounts, net config, net print, net share, and net view. Consider doing a Google search on these commands to find out how they work.

19-5a Module Summary

Securing Workstations and IoT Devices on a Network

- Most browsers allow you to sign in and sync data across devices and to the cloud; manage extensions, plug-ins, and passwords to websites;

block pop-ups and ads; clear the browsing cache; and control privacy settings.

- Browsers use digital certificates to validate the identity of websites.
- Internet Options in Control Panel can be used to manage proxy server settings for the Windows system and all installed browsers.
- To download a new browser securely, verify the download and installation routine is digitally signed and compare hashes for the downloaded file.
- Use a VPN connection to encrypt communication with a remote network across the Internet.
- A computer can use a USB or embedded broadband device with a SIM card to make a WWAN connection to the Internet via a cellular carrier.
- Windows can monitor a metered connection to send an alert when data usage has reached a threshold.
- Windows Defender Firewall in Windows 10/11 provides personal firewall services on a laptop or workstation to protect the computer from attack over the Internet.
- Z-Wave and Zigbee are wireless communication protocols used by IoT devices on a network. Both protocols use encryption. Neither supports TCP/IP without an additional protocol layer such as Z/IP or Zigbee IP. Zigbee is more robust than Z-Wave and is generally the choice for large-scale industrial use.

Securing a Multifunction Router for a SOHO Network

- A multifunction router for a small office/home office (SOHO) network might serve several functions, including router, switch, DHCP server, wireless access point (WAP), firewall, and file server.
- Place a router in a secure location, and if it is being used as a WAP, make sure it is centrally located for users.
- It's extremely important to change the administrative password on a router as soon as you install it, especially if the router also serves as a wireless access point.
- To configure a router to secure and serve the local network, you can update firmware, assign a static WAN IP address, reserve IP addresses for the DHCP server, configure UPnP, and configure QoS for priority applications.
- To allow certain network traffic initiated from the Internet past your firewall, you can use port forwarding, a DMZ, screened subnets, and content filtering with whitelists or blacklists.
- Access to the network can be controlled by allowing or denying certain applications and ports and by IP filtering.
- To secure a wireless access point, you can require a security key, change the default SSID, select specific Wi-Fi channels, disable guest access, and enable encryption (WPA, WPA2, or WPA3).
- An enterprise might use RADIUS, TACACS+, and/or Kerberos software to help with authentication to the network and/or enterprise

resources. On a wireless network, RADIUS or TACACS+ is used rather than a network security key to authenticate to the wireless network. TACACS+ is used specifically with Cisco devices. Kerberos is used within a network for a Windows client to authenticate to a Windows domain.

Using Remote Access Technologies

- File transfer technologies include FTP and HTTP-based technologies such as Dropbox and Google Drive.
- Windows 10/11 offers Remote Desktop Connection (RDC) and Microsoft Remote Assistance (MSRA) to remotely manage a Windows 10/11 desktop. Remote Desktop gives you access to your Windows desktop and file sharing from anywhere on the Internet. Remote Assistance lets you provide remote support to users but does not allow file sharing.
- Virtual Network Computing (VNC) is used for remote desktop management, screen sharing, and file transfers. Software must be installed on both the client and the server.
- Secure Shell (SSH) is open-source software that is preinstalled in most Linux and UNIX systems and provides an encrypted connection for a client computer to remotely control a Linux or UNIX host.
- Remote Monitoring and Management (RMM) software remotely monitors and manages systems to support IT personnel responsible for these systems either in-house or in a managed services provider (MSP) role.
- When evaluating third-party remote access applications, consider the security of the connection and how screens and files are shared.

Troubleshooting Network Connections

- Useful Windows command-line utilities for network troubleshooting are ping, hostname, ipconfig, nslookup, tracert, pathping, net use, net user, and netstat.

19-5c Thinking Critically

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. As an IT technician, you arrive at a customer's home office to troubleshoot problems they are experiencing with their printer. While questioning the customer to get an understanding of their network, you find they have a new Wi-Fi router that connects wirelessly to a new desktop and two new laptops, in addition to multiple smartphones, tablets, and the network printer. They also have several smart home devices, including security cameras, light switches, door locks, and a thermostat supported by an IoT controller hub. To work on the printer, which type of network will you be interacting with?

1. PAN

2. WAN
3. WMN
4. LAN

2. While you work on the customer's printer, they continue chatting about their network and the problems they've been experiencing. One complaint is that the Internet service slows down considerably in the evening. You suspect you know the cause of this problem: Their neighbors arrive home in the evening and bog down the ISP's local infrastructure. To be sure, you take a quick look at the back of their modem. What type of cable connected to the WAN port would confirm your suspicions and why?

3. Your customer then asks you if it would be worth the investment for them to have Ethernet cabling installed to reach each of their workstations instead of connecting them by Wi-Fi to the network. Specifically, they want to know if that would speed up communications for the workstations. You examine their router and find that it's using 802.11ac Wi-Fi. Would you advise them to upgrade to Ethernet? Why or why not?

1. Yes, because Ethernet is faster than 802.11ac.
2. Yes, because wired connections are always faster than wireless connections.
3. No, because installing Ethernet cabling is more expensive than the increased speed is worth.
4. No, because 802.11ac speeds are faster than Ethernet.

4. You run the ipconfig command on your computer, and it reports an IP address of 169.254.75.10 on the Ethernet interface. Which device assigned this IP address to the interface?

1. The ISP's DNS server
2. The local network's DHCP server on the SOHO router
3. The cable modem
4. The local computer

5. You've just received a call from human resources asking for assistance with a problem. One of your company's employees, Ahmed, has recently undergone extensive surgery and will be homebound for three to five months. He plans on working from home and needs a solution to enable frequent and extended access to the company network's resources. Which WAN technology will you need to configure for Ahmed, and which tool will you use to configure it?

1. WWAN using the Network Connections window
2. Wi-Fi using the Network and Sharing Center
3. Ethernet using the Network Connections window
4. VPN using the Network and Sharing Center

6. Your manager has asked you to configure a DHCP reservation on the network for a Windows computer that is used to configure other devices on a network. To do this, you need the computer's MAC address. What command can you enter at the command line to access this information?

7. You're setting up a Minecraft gaming server so you and several of your friends can share a realm during your gameplay. To do this, your friends will need to access your server over the Internet, which means you must configure your router to send this traffic to your

game server. Which router feature will you use, and which port must you open for TCP traffic?

8. While troubleshooting an Internet connection problem for your network, you restarted the modem and then the router. The router is now communicating with the Internet, which you can confirm by observing the blinking light on the router's WAN indicator. However, now your laptop is not communicating with the router. Order the following commands to confirm there is no connectivity, apply a fix to the problem, and confirm connectivity.

1. ping
2. ipconfig /renew
3. nslookup microsoft.com
4. ipconfig /release

9. You need a VPN to connect to a private, remote network in order to access some files. You click the network icon in your taskbar to establish the connection, and you realize there is no VPN option available on the menu. What tool do you need to use to fix this problem?

1. net command
2. netstat command
3. Network and Sharing Center
4. Network Connections window

10. To prepare to remotely work on a Linux server at work while you are at home, you install VNC Server for Linux by RealVNC (realvnc.com) on the system at work. When you get home, you install the VNC Viewer for Windows on your Windows 10 laptop. When you try to make the connection, you get an error about a refused connection. Which could be a cause of the error? (Choose all that apply.)

1. VNC Viewer for Windows will not work with a Linux server. Use Remote Desktop instead.
2. Port 5901 is not set for port forwarding on the corporate router. Configure the router next time you're in the office.
3. VNC Server for Linux must be configured to tunnel through SSH. Set up the SSH tunnel next time you're in the office.
4. A VNC solution will not work with Linux. Configure Remote Desktop on the Linux server, and use it with the Remote Desktop client on your home computer.

11. You're troubleshooting a network connection for a client at their home office. After pinging the network's default gateway, you discover that the cable connecting the desktop to the router had been damaged by foot traffic and is no longer providing a reliable signal. You replace the cable, this time running the cable along the wall, so it won't be stepped on. What do you do next?

1. Apply port forwarding on the router.
2. Use the ping command.
3. Use the hostname command.
4. Reboot the router.

12. Which type of server can function as a firewall?

1. Mail server
2. Proxy server
3. Print server
4. FTP server

13. Your company has recently been hired to install a smart security system for a large office building. The system will include security cameras, voice-controlled lights, smart locks, and smart thermostats. Some of the security cameras will be installed outdoors throughout the parking lot. Which wireless IoT protocol should your company use for the installation?

1. Wi-Fi, because it is always encrypted
2. Zigbee, because it is always encrypted
3. Z-Wave, because it is the fastest wireless standard
4. Bluetooth, because it is easiest to configure

14. Of the 10 devices shown earlier in [Figure 19-21](#), how many are assigned IP addresses?

1. Four: two phones, a web server, and a router
2. Three: two phones and a web server
3. Seven: a thermostat, a router, two phones, two bridges, and a web server
4. All 10

15. As a bank employee, you often work from home and remotely access a file server on the bank's network to correct errors in financial data. Which of the following services is most likely the one you are using to authenticate to the network and track what you do on the network?

1. RADIUS
2. Secure DNS
3. Active Directory
4. TACACS+

16. Mia works from home occasionally and needs to set up her Windows 10 computer at work so she can remote in from her home office. Which tools should she use?

1. Zoom
2. Remote Assistance
3. Secure Shell
4. Remote Desktop

17. Daunte frequently calls your help desk asking for instructions on how to use Windows 10. What is the best way to help Daunte?

1. Open a chat session with Daunte over Facebook and talk with him about Windows 10.
2. Use Remote Assistance to show Daunte how to use Windows 10, and point him to the log file created.
3. Explain to Daunte that a help desk is not the place to go to learn to use new software and that he needs to look elsewhere for help.
4. Email Daunte some links to online video tutorials about Windows 10.

18. Remote Desktop and Remote Assistance require a technician to change port settings and firewall settings, but third-party apps such as GoToMyPC do not. Why is this?

1. Microsoft makes its apps more secure than third-party apps.
2. GoToMyPC and other third-party apps use ports already left open for web browsing and don't require additional incoming connections.
3. Remote Desktop and Remote Assistance allow incoming connections at the same port 80 that is already left open for web browsing.
4. GoToMyPC and other third-party apps are not concerned about security because they depend on Windows to secure a network connection.

19. Manuel works on a help desk and is assigned a ticket that was automatically generated by a server because of an error. The error message states that the server has run out of storage space because logs were not set to delete at a certain size. Rather than going to the data center to physically access that server on the rack, what Windows tool might Manuel use to troubleshoot the server?

20. While investigating the settings on your SOHO router, you find two IP addresses reported on the device's routing table, which is used to determine where to send incoming data. The two IP addresses are 192.168.2.1 and 71.9.200.235. Which of these IP addresses would you expect to see listed as the default gateway on the devices in your local network? How do you know?

21. The documentation for your router says that it can provide content filtering to filter out keywords except for pages that use the HTTPS protocol. Why is that?

1. Privacy laws make it illegal to filter content in HTTPS pages.
2. HTTPS pages are encrypted, and the router cannot decrypt them to read the content.
3. The router must use its public key to transmit HTTPS pages.
4. The software to filter content in HTTPS pages is not installed on this particular router.

22. Your manager asks you to transmit a small file that includes sensitive personnel data to a Linux server on the network. The server is running a Telnet server and an SSH server. Why is it not a good idea to use Telnet to reach the remote computer?

1. Telnet transmissions are not encrypted.
2. Telnet is not reliable, and the file might arrive corrupted.
3. SSH is faster than Telnet.
4. SSH running on the same computer as Telnet causes Telnet not to work.

23. While troubleshooting an IPv4 network connection problem, you start to wonder if the local computer's NIC is configured correctly for TCP/IP settings. What command should you enter at the command prompt to test your theory?

24. Your SOHO router has failed, and you have installed a new router. The old router's static IP address on the network is 192.168.0.1. The new router has a static IP address of 10.0.0.1. You go to a computer to configure the new router, and you enter 10.0.0.1 in the browser address box. The router does not respond. You open a command prompt window and try to ping the router, which does not work. Next, you verify that the router has

connectivity, and you see that its local connection light is blinking, indicating connectivity. What is the most likely problem and its best solution?

1. The computer you are using to configure the router has a corrupted TCP/IP configuration. Restart the computer.
2. The router is defective. Return it for a full refund.
3. The computer and the router are not in the same subnet. Release and renew the IP address of the computer.
4. The computer and the router are not in the same subnet. Change the subnet mask assigned to the computer.

25. While troubleshooting a network connection problem, you run the command `ipconfig /all` in a command prompt window and get the following output:

Ethernet adapter Ethernet:

- o Connection-specific DNS Suffix.:
- o Description.....: Realtek PCIe GBE Family Controller
- o Physical Address.....: 54-53-ED-BB-AB-A3
- o DHCP Enabled.....: Yes
- o Autoconfiguration Enabled.....: Yes
- o Link local IPv6 Address.....: fe80::64d2:bd2e:fa62:b911%10 (Preferred)
- o IPv4 Address.....: 192.168.2.166 (Preferred)
- o Subnet Mask.....: 255.255.255.0
- o Lease Obtained.....: Sunday, August 19, 2022 10:56:41 AM
- o Lease Expires.....: Sunday, August 19, 2022 1:56:41 PM
- o Default Gateway.....: 192.168.2.1
- o DHCP Server.....: 192.168.2.1
- o DHCPv6 IAID.....: 257184749
- o DHCPv6 Client DUID.....: 00-01-00-01-18-81-16-9A-54-53-ED-BB-AB-A3
- o DNS Servers.....: 8.8.8.8 8.8.4.4
- o NetBIOS over Tcpip.....: Enabled

Is the computer using a wired or wireless network connection? What is the local computer's MAC address? What is the IP address of the router on the local network?

26. Which two of the following hosts on a corporate intranet are on the same subnet?

1. 192.168.2.143/8
2. 172.54.98.3/16
3. 192.168.5.57/8
4. 172.54.72.89/16

19-5d Hands-On Projects

Hands-On Project 19-1

Researching a Wireless LAN

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.6

Suppose you have a DSL connection to the Internet in your home, and you want to connect two laptops and a desktop computer in a wireless network with access to the Internet. You need to purchase a multifunction wireless router like the ones you learned to configure in this module. You also need a wireless adapter for the desktop computer. (The two laptops have built-in wireless networking.) Use the web to research the equipment needed to create the wireless LAN, and answer the following questions:

1. Save or print two webpages showing two different multifunctional wireless routers. What is the brand, model, and price of each router?
2. Save or print two webpages showing two different wireless adapters a desktop computer could use to connect to the wireless network. Include one external device that uses a USB port and one internal device. What is the brand, model, and price of each device?
3. Which router and wireless adapter would you select for your home network? What is the total cost of both devices?

Hands-On Project 19-2

Using Google Chrome

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 2.10

Microsoft Edge is not the only browser available, and many users prefer others such as Mozilla Firefox ([mozilla.org](https://www.mozilla.org)) or Google Chrome ([google.com](https://www.google.com)). Go to the Google website, and download and install Google Chrome. Use it to browse the web. How does it compare with Microsoft Edge? What do you like better about it? What do you not like as well? In what situations might you recommend that someone use Chrome rather than Microsoft Edge? What security features does Google Chrome offer? What are the steps to import your favorites list from Edge into Chrome?

Hands-On Project 19-3

Practicing Using a VNC Product

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 4.9

In the module, in [Figure 19-59](#), you saw RealVNC installed as a viewer on a Mac computer, controlling the desktop of a Windows 10 computer. Do the following to practice setting up your own VNC desktop management scenario. You might want to work with a partner, with each of you using your own computer for this project. Although each person can have their

own RealVNC account to do this project, to keep things simple, the partners will share the same RealVNC account to make the connection:

1. **1**
Go to RealVNC at realvnc.com, and sign up for RealVNC. You will need an email address to sign up for the free trial. Download and install the RealVNC server on one computer. Sign in to RealVNC server on your computer.
2. **2**
On a different computer, install the RealVNC viewer. Sign in to RealVNC in the viewer software using the same email account you used in step 1.
3. **3**
Use the viewer on the second computer to control the desktop on the first computer. Can you use the viewer to open and use a chat window that works on the server host?
4. **4**
When you are finished with this project, sign out of the software, and perhaps uninstall it.

Hands-On Project 19-4

Setting Up a Persistent Network Drive

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.2

Using two networked computers, do the following to set up and test a persistent network drive:

1. **1**
On the computer that will host the network drive:
 1. Create a folder under the root of drive C: named MyShare, and create one file in the folder.
 2. Share the folder on the network, giving users read/write permissions to the folder.
 3. Run the `hostname` command to find out the computer name.
2. **2**
On the second computer:
 1. Run the `net` commands to map a persistent network drive onto the MyShare folder on the first computer.
 2. Test the folder to make sure you can copy the file in the folder to your computer and write a new file to the shared folder.
 3. Restart your computer. Is the network drive persistent?
 4. Run the `net` command to delete the mapped drive.

Hands-On Project 19-5

Scanning a Network for Connected Devices

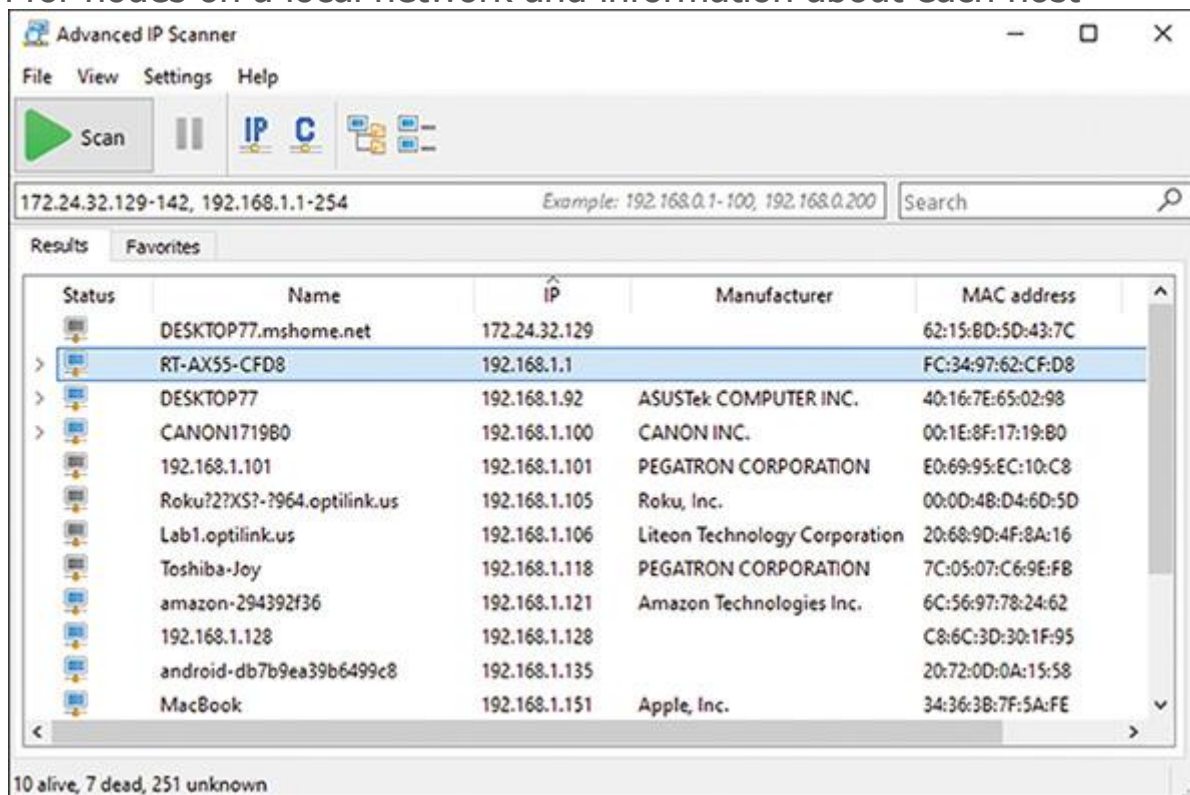
- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.2

To help document devices connected to your network, you can use Advanced IP Scanner. Do the following to install and use the software:

1. **1**
Go to advanced-ip-scanner.com, and then download and install Advanced IP Scanner by Famatech Corp. Install and run the software.
2. **2**
Make sure the range of IP addresses includes all the IP addresses on your network. Click **Scan**. [Figure 19-67](#) shows the results of one scan. Notice the software reports nodes on the network, their IP addresses, services they are running, and shared folders.

Figure 19-67

Scan for nodes on a local network and information about each host



The screenshot shows the Advanced IP Scanner application window. The interface includes a menu bar (File, View, Settings, Help), a toolbar with a 'Scan' button, and a text input field for IP ranges. The input field contains '172.24.32.129-142, 192.168.1.1-254' and an example '192.168.0.1-100, 192.168.0.200'. Below the input field are tabs for 'Results' and 'Favorites'. The 'Results' tab is active, displaying a table of discovered hosts. The table has columns for Status, Name, IP, Manufacturer, and MAC address. The status of each host is indicated by a small icon (green for alive, red for dead, grey for unknown). The table lists 13 hosts, including desktops, printers, and various IoT devices. At the bottom of the window, a status bar indicates '10 alive, 7 dead, 251 unknown'.

Status	Name	IP	Manufacturer	MAC address
Alive	DESKTOP77.mshome.net	172.24.32.129		62:15:BD:5D:43:7C
Alive	RT-AX55-CFD8	192.168.1.1		FC:34:97:62:CF:D8
Alive	DESKTOP77	192.168.1.92	ASUSTek COMPUTER INC.	40:16:7E:65:02:98
Alive	CANON1719B0	192.168.1.100	CANON INC.	00:1E:8F:17:19:B0
Alive	192.168.1.101	192.168.1.101	PEGATRON CORPORATION	E0:69:95:EC:10:C8
Alive	Roku?2?X5?-7964.optilink.us	192.168.1.105	Roku, Inc.	00:0D:4B:D4:6D:5D
Alive	Lab1.optilink.us	192.168.1.106	Liteon Technology Corporation	20:68:9D:4F:8A:16
Alive	Toshiba-Joy	192.168.1.118	PEGATRON CORPORATION	7C:05:07:C6:9E:FB
Alive	amazon-294392f36	192.168.1.121	Amazon Technologies Inc.	6C:56:97:78:24:62
Alive	192.168.1.128	192.168.1.128		C8:6C:3D:30:1F:95
Alive	android-db7b9ea39b6499c8	192.168.1.135		20:72:0D:0A:15:58
Alive	MacBook	192.168.1.151	Apple, Inc.	34:36:3B:7F:5A:FE

10 alive, 7 dead, 251 unknown

19-5e Real Problems, Real Solutions

Real Problem 19-1

Using a Port Scanner

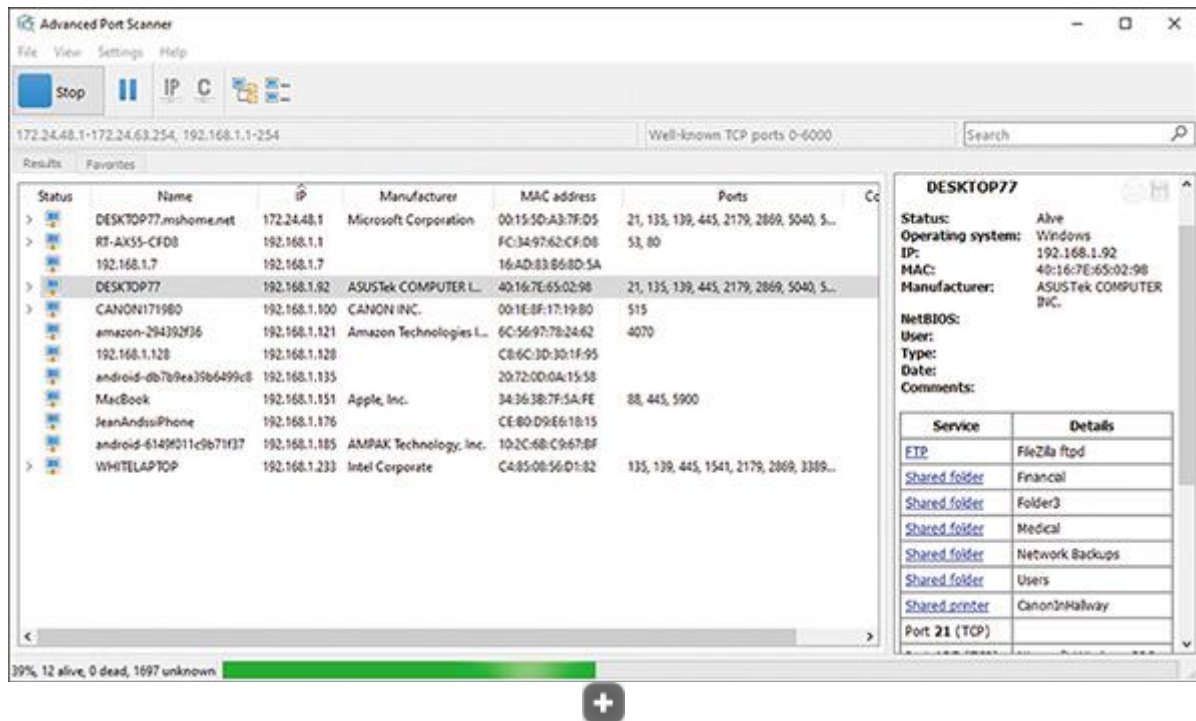
- **Est. Time:** 30 minutes
- **Core 2 Objective:** 1.2

Port-scanning software can be used to find out how vulnerable a computer is with open ports. This project requires the use of two computers on the same network to practice using port-scanning software. Complete the following steps:

1. **1**
On computer 1, download and install Advanced Port Scanner by Famatech at advanced-port-scanner.com. Install and run the software.
2. **2**
Open the **Network and Sharing Center**, click **Change advanced sharing settings**, and turn off network discovery and file and printer sharing.
3. **3**
In the Advanced Port Scanner window, make sure that the range of IP addresses includes the IP address of computer 2. Change the default port list to TCP ports 0 through 6000. Then click **Scan**.
4. **4**
Browse the list, and find computer 2. List the number and purpose of all open ports found on computer 2.
5. **5**
On computer 2, turn on network discovery and file and printer sharing. Open the **System** window, click **Remote settings**, and allow Remote Assistance connections to this computer. Close all windows.
6. **6**
On computer 1, rescan and list the number and purpose of each port now open on computer 2. [Figure 19-68](#) shows the results for one computer, but yours might be different.

Figure 19-68

Advanced Port Scanner shows open ports on networked computers



Real Problem 19-2

Implementing More Security for Remote Desktop

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 4.9

When Hakim travels on company business, he finds it's a great help to be able to access his office computer from anywhere on the road using Remote Desktop. However, he wants to make sure his office computer and the corporate network are as safe as possible. One way you can help Hakim add more security is to change the listening port that Remote Desktop uses. Knowledgeable hackers know that Remote Desktop uses port 3389, but if you change this port to a secret port, hackers are less likely to find the open port. Search the Microsoft Knowledge Base articles (support.microsoft.com and docs.microsoft.com) for a way to change the listening port that Remote Desktop uses. Practice implementing this change by doing the following:

1. Set up Remote Desktop on a computer using a business or professional edition of Windows. This computer is your host computer. Use another computer (the client computer) to create a Remote Desktop session to the host computer. Verify that the session works by transferring files in both directions.
2. Next, change the port that Remote Desktop uses on the host computer to a secret port. Save or print a screenshot showing how you made the change. Use the client computer to create a Remote Desktop session to the host computer using the secret port. Print a screenshot showing how you made the connection using the secret port. Verify that the session works by transferring files in both directions.
3. What secret port did you use? What link on the Microsoft websites gave you the information you needed?

Real Problem 19-3

Using SSH and PuTTY

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 4.9

Follow these steps to install Linux in a VM, and use the PuTTY program for remote access to the Linux host via an SSH connection:

1. **1**
To download Ubuntu Server, go to releases.ubuntu.com, and download the latest release of Ubuntu Server install image, which is an ISO file.
2. **2**
In Windows 10/11 Pro, open **Hyper-V Manager**, and use it to create a new VM. Use the downloaded ISO file to install Ubuntu Server in the VM. What is the server name, your user name, and your password? Accept all default settings. When you get to the screen that gives you the option to install the OpenSSH server, choose to install the server. Notice that Ubuntu allows you to import your SSH keys from GitHub or Launchpad. It is not necessary to import SSH keys at this time.
3. **3**
Remove the ISO file from the VM's virtual DVD drive, and reboot the server.
4. **4**
Sign in to Ubuntu Server, and enter this command to install some networking tools, including the `ifconfig` command:


```
sudo apt install net-tools
```
5. **5**
Enter the `ifconfig` command to find out the IP address of the server. What is its IP address?
6. **6**
Go to putty.org and download and install the PuTTY program on your Windows 10/11 computer. Launch **PuTTY**.
7. **7**
Enter the IP address of your server in the PuTTY window, and make sure PuTTY is set to use SSH. What port does SSH use? Connect your Windows 10/11 computer to the Ubuntu Server in an SSH session. When asked if you trust the host key the server presented, click **Accept**.
8. **8**
Remotely log in to the server with your Ubuntu Server user name and password. Try the `hostname` command in the PuTTY window. Did the command return the name of the Ubuntu Server?
9. **9**
Use this command in the PuTTY window to shut down the server:

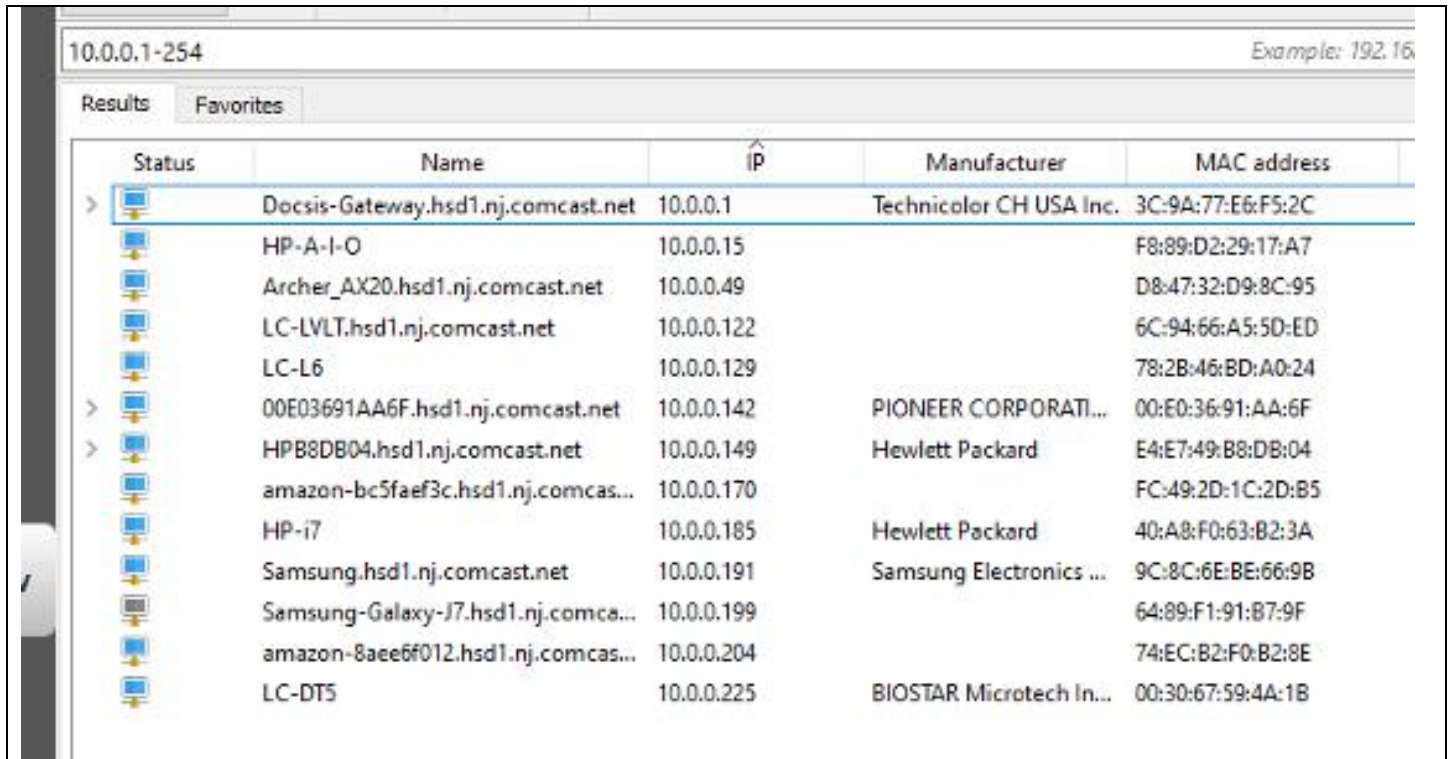
```
sudo shutdown now
```

10.

10

You can now close all windows.

Be sure to save your Ubuntu Server VM because you'll need it again for the module "[Linux and Scripting](#)," where you learn much more about Ubuntu Server.



The screenshot shows a network scanner interface with a search bar at the top containing '10.0.0.1-254' and a hint 'Example: 192.168.1.1'. Below the search bar are two tabs: 'Results' and 'Favorites'. The 'Results' tab is active, displaying a table of discovered devices. Each row includes a status icon (a blue computer monitor with a yellow arrow), a name, an IP address, a manufacturer, and a MAC address. The table is sorted by IP address in ascending order.

Status	Name	IP	Manufacturer	MAC address
>	Docsis-Gateway.hsd1.nj.comcast.net	10.0.0.1	Technicolor CH USA Inc.	3C:9A:77:E6:F5:2C
	HP-A-I-O	10.0.0.15		F8:89:D2:29:17:A7
	Archer_AX20.hsd1.nj.comcast.net	10.0.0.49		D8:47:32:D9:8C:95
	LC-LVLT.hsd1.nj.comcast.net	10.0.0.122		6C:94:66:A5:5D:ED
	LC-L6	10.0.0.129		78:2B:46:BD:A0:24
>	00E03691AA6F.hsd1.nj.comcast.net	10.0.0.142	PIONEER CORPORATI...	00:E0:36:91:AA:6F
>	HPB8DB04.hsd1.nj.comcast.net	10.0.0.149	Hewlett Packard	E4:E7:49:B8:DB:04
	amazon-bc5faef3c.hsd1.nj.comcas...	10.0.0.170		FC:49:2D:1C:2D:B5
	HP-i7	10.0.0.185	Hewlett Packard	40:A8:F0:63:B2:3A
	Samsung.hsd1.nj.comcast.net	10.0.0.191	Samsung Electronics ...	9C:8C:6E:BE:66:9B
	Samsung-Galaxy-J7.hsd1.nj.comca...	10.0.0.199		64:89:F1:91:B7:9F
	amazon-8aee6f012.hsd1.nj.comcas...	10.0.0.204		74:EC:B2:F0:B2:8E
	LC-DT5	10.0.0.225	BIOSTAR Microtech In...	00:30:67:59:4A:1B

10.0.0.1-254 Example:				
Results Favorites				
Status	Name	IP	Manufacturer	MAC address
▼	Docsis-Gateway.hsd1.nj.comcast.net	10.0.0.1	Technicolor CH USA Inc.	3C:9A:77:E6:F5:2C
	HTTP, XFINITY (Xfinity Broadband Router Server)			
▼	HP-A-I-O	10.0.0.15		F8:89:D2:29:17:A7
	RDP (Tunnel is Microsoft SChannel TLS: unknown service)			
	Archer_AX20.hsd1.nj.comcast.net	10.0.0.49		D8:47:32:D9:8C:95
▼	LC-LVLT.hsd1.nj.comcast.net	10.0.0.122		6C:94:66:A5:5D:ED
	RDP (Tunnel is Microsoft SChannel TLS: unknown service)			
▼	LC-L6	10.0.0.129		78:2B:46:BD:A0:24
	RDP (Tunnel is Microsoft SChannel TLS: unknown service)			
▼	00E03691AA6F.hsd1.nj.comcast.net	10.0.0.142	PIONEER CORPORATI...	00:E0:36:91:AA:6F
	HTTP, DMP - User Interface (GoAhead-Webs)			
▼	HPB8DB04.hsd1.nj.comcast.net	10.0.0.149	Hewlett Packard	E4:E7:49:B8:DB:04
	HTTP, nginx			
	amazon-bc5faef3c.hsd1.nj.comcas...	10.0.0.170		FC:49:2D:1C:2D:B5
▼	HP-i7	10.0.0.185	Hewlett Packard	40:A8:F0:63:B2:3A
	RDP (Tunnel is ssl: unknown service)			
	Samsung.hsd1.nj.comcast.net	10.0.0.191	Samsung Electronics ...	9C:8C:6E:BE:66:9B
	Samsung-Galaxy-J7.hsd1.nj.comca...	10.0.0.199		64:89:F1:91:B7:9F
	amazon-8aee6f012.hsd1.nj.comcas...	10.0.0.204		74:EC:B2:F0:B2:8E
▼	LC-DT5	10.0.0.225	BIOSTAR Microtech In...	00:30:67:59:4A:1B
	RDP (Tunnel is Microsoft SChannel TLS: unknown service)			

Lab 19-1: Implementing Network Security Measures

Exercise 1 - Logical Security

The three main types of security controls are Administrative, Logical (or technical), and Physical. Administrative controls include policies, procedures, rules, standards, regulations, and frameworks. Physical security controls include doors, locks, fences, lighting, cameras, etc. Logical controls are typically software-based and are often found in endpoints, servers, networking devices, and security appliances such as firewalls, proxy servers, intrusion detection and prevention systems, and SIEM systems.

In this exercise, logical network security controls will be discussed.

Learning Outcomes

After completing this exercise, you should be able to:

- Know about the Principle of Least Privilege

- Explain the Uses of Access Control Lists (ACL)
- Configure Email Security

After completing this exercise, you should have further knowledge of:

- Multifactor Authentication (MFA)
- Using a Hard Token
- Using a Soft Token
- Short Message Service (SMS)
- Voice Call
- Authenticator Application

Task 1 - Principle Of Least Privilege

Principle of Least Privilege is the foundation for all access control systems and methods. The principle of least privilege requires users, devices, and applications to be given only the minimum level of privileges that are necessary to complete the task. The least privilege does not apply only to human users but also to systems and applications.

There is a closely related security control called **Need to Know**. In high security operations, especially in military and government systems, users or subjects are given clearance. Resources or objects are given a classification. Clearance, classification, and need to know are used to assign privileges in this type of environment.

In a Windows Workgroup, privileges are assigned using **Local Users and Groups**. This is suitable for small network operations but can be difficult to manage. Each user needs to be given permission on every system they have access to. There is no central administrative console for the configuration of all systems.

In a Windows Domain, permissions are handled centrally on a Domain Controller server, using **Active Directory** and **Group Policy**.

In this task, you will view the policies that can be configured in a Windows WorkGroup and Windows Domain.

In the **Active Directory Users and Computers** window, notice that you have two users on the right pane **Administrator - User** and **Guest - User**.

Everything else is standard Windows **Security Group**. Active Directory works with Group Policy as follows: Permissions are assigned to Groups, then users are added to one or more Groups. The User inherits their permissions from the Groups they belong to.

Task 2 - Access Control Lists (ACL)

An Access Control List is a list of permissions associated with an object or resource. The ACL specifies which users or system processes are allowed to access the resource. For instance, if Amy has permissions to **read/write** and Bob only has permissions to **read**, Amy's permissions are higher than Bob's.

Access control lists are used in many places on a network. One of the most common is **a network firewall**. In firewalls, access control lists are commonly known as **firewall rules**. Firewall rules are written in order and are applied from the first rule to the last. If the first rule matches the traffic, all the other rules will be overridden. The rules will specifically **ALLOW** connections based on attributes such as Source IP address, Destination IP address, Source Port Number, and Destination Port Number. The final rule is the **DENY REST** rule. It blocks all traffic that is not specifically allowed in earlier rules.

Other resources that may use access control lists include **file systems** (read, write, modify, execute, delete), **Active Directory and LDAP directories** (user and group permissions, role-based access controls (RBAC)), **network devices** such as **firewalls, routers, and switches** (rules), and **relational databases** (permissions).

```
%ProgramFiles%\application\application.exe
```

Multifactor Authentication (MFA)

In the beginning, if you were logging in to a system, resource, or network, all you needed was a user ID and password. Now, due to the threat of passwords being hacked using methods such as Brute Force and Dictionary attacks, a password on its own is not a very good form of security. Passwords need to be at least 15 characters to be able to withstand automated password cracking. But if you give your password away as the result of phishing or social engineering exploits, the length won't matter.

Current solutions to this problem include "passwordless" and multifactor authentication. Multifactor authentication requires two or more different types of authentication from the list below. Two authentication methods from the same category are not considered to be valid. For instance, a password and a PIN number are both from the authentication type of something you know.

2FA and MFA require factors from two or more of the following categories:

- **Knowledge-based** - Something you know, such as a password, PIN, or challenge questions and answers.
- **Possession-based** or physical device - Something you have, such as an ID card or badge, smart card, digital certificate, phone app, or RSA token or fob.
- **Biometrics** or bodily characteristics - Something you are, such as a fingerprint, palm print, hand geometry, retina scan, iris scan, facial scan, or voice recognition.
- **Location** - Somewhere you are, as determined by GPS devices, including a smartphone, IP address, MAC address, and machine name or Fully Qualified Domain Name (FQDN).
- **Behavioral** - Something you do, such as keyboard typing cadence, mouse dynamics, EUBA or end-user behavior analytics, or even a written signature.

Task 4 - Configure Email Security

Email is the exchange of messages between two users using different systems over a network. Early email used **File Transfer Protocol (FTP)**. The **Simple Mail Transfer Protocol (SMTP)** was invented in 1983. By 1995 the current suite of email protocols **SMTP, Post Office Protocol (POP), and Internet Message Access Protocol (IMAP)** was being used to send (SMTP) and receive (POP or IMAP) email messages. Later on, **Hypertext Transport Protocol (HTTP)** became another way to display email or what we call **webmail** or email on a web browser on services such as AOL, Yahoo, Hotmail, and Gmail.

As security became more important, new secure protocols were developed. Many security tools were developed for email. Security tools include message encryption, email sender identification and authentication, spam and phishing email filters, and email anti-malware scanners. Most of these security controls run on top of the older insecure protocols, so email security still has issues.

Let's start with email message encryption. Here is a table of the email ports and protocols. These protocols establish secure communications using Transport Layer Security (TLS) in the same manner that a browser connects to an HTTPS website.

Protocol	Secure Port	Insecure Port
----------	-------------	---------------

Post Office Protocol (POP)	995	110
Internet Message Access Protocol (IMAP)	993	143
Simple Mail Transfer Protocol (SMTP)	587(STARTTLS), 465	587, 25
Hypertext Transfer Protocol (HTTP)	443 (HTTPS)	80 (HTTP)

Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is a secure encryption protocol used to send emails with end-to-end encryption. It is supported by most email services and applications. S/MIME requires the use of Digital Certificates and Public Key Infrastructure (PKI). The contents of the email are encrypted, but the metadata contained in the email headers is sent in plain text.

Pretty Good Privacy (PGP) and OpenPGP

PGP and its more commonly used open-source variation **OpenPGP** is an encryption protocol used for sending highly secure end-to-end-encrypted (E2EE) emails. It's popular for both email encryption and file encryption.

Email Sender Identification and Authentication Methods

- **Sender Policy Framework (SPF)** is an authentication method used in emails to prevent threat actors from replicating a sender's email address. This was designed to stop spammers from sending messages that spoofed somebody else's domain and block phishing and malware attachments.
- **DomainKeys Identified Mail (DKIM)** is another authentication method to block spoofed sender addresses. DKIM allows an email server to ensure the sender is legitimate. This helps DKIM to block spam and phishing emails. DKIM signs an email with a digital signature, which can be verified and authenticated, to prevent spoofing.
- **Domain-Based Message Authentication, Reporting & Conformance (DMARC)** is an email authentication protocol that works together with DKIM and SPF. DMARC can only be used when both SPF and DKIM have been correctly configured. DMARC provides analysis and reporting about who is sending emails from a given domain.

You have the following fields:

- The **Incoming email server** will be in the following format: **mail.mydomain.com**, **pop.mydomain.com**, or **imap.mydomain.com**.
- For the **Account type**, you can select **POP3** or **IMAP4** from the drop-down menu.
- The **Outgoing mail server** will be in the following format: **mail.mydomain.com** or **smtp.mydomain.com**.
- The four fields have checkboxes enabled by default. The first two fields ensure there's proper authentication when sending emails.
- Requires SSL for incoming and outgoing emails; when enabled, will use encryption for the email account.

Using a Hard Token

A Hard Token or hardware token is a physical device used for authentication. They are commonly known as key fobs, security tokens or USB tokens. RSA key fobs are a common example of a hard token.

It may be used as a single form of authentication or as part of a two-factor or multifactor authentication system. As part of MFA, it would be a possession-based or something-you-have authentication method.

There are two main types of hard tokens, synchronous and asynchronous. A synchronous token is synchronized with an authentication server. The token generates a six-digit one-time password (OTP) which needs to be entered into the login screen flow. An asynchronous token uses a series of challenge/response entries to authenticate.

Using a Soft Token

A Soft Token or software token is similar to a hard token. Typically, a hard token is associated with a specific hardware device. A soft token is a software application that can be installed on different devices such as smartphones, tablets, laptops, or other computer systems. These software applications generate a synchronous six-digit OTP code that has to be entered in the logon screen flow within a short period of time, usually 30 or 60 seconds.

Short Message Service (SMS)

Another way to deliver a one-time password (OTP) is via Short Message Service (SMS) or smartphone text message. This is a fairly common method, even though they are not considered very secure. SMS does not use an encrypted channel and can be intercepted as plaintext. As such, it is susceptible to SIM cloning attacks.

Voice Call

Voice call or call-back has been an authentication method used as far back as with early RADIUS authentication servers. A user attempting to dial into the company's analog dial-up modem pool and connect to the network is often authenticated and then waits for the system to call back. Then an analog dial-up connection is made.

This system is still used to send OTP codes to users. To complete the authentication, the system calls you back with an automated message that includes the OTP.

A telephone call can also be used to verify the sender of an email and any contents, such as file attachments. This can be used to avoid falling for suspicious phishing emails. Some banks make a telephone call to confirm wire transfers or EFT requests before committing to the funds being transferred.

Authenticator Application

It is a specific type of soft token that is available for smartphone platforms and includes smartphone apps such as Google Authenticator, Authy, LastPass Authenticator, or Microsoft Authenticator. These software applications also generate a synchronous six-digit OTP code that has to be entered in the logon screen flow within a short period of time, usually 30 or 60 seconds.

Which security control requires users, devices, and applications to be given only the minimum level of permissions that are necessary to complete the task?

- ☐ Multifactor Authentication (MFA)
- ☐ Hard token
- ☒ Principle of Least Privilege
- ☐ Access Control Lists (ACL)

Which network devices rely on Access Control Lists (ACL) to permit network connections? [Choose all that apply]

- ☐ Router
- ☐ Firewall
- ☐ Switch
- ☐ Printer
- ☐ Server

Which of the following are Multifactor Authentication (MFA) factors? [Choose all that apply]

- ☐ Location
- ☐ Possession-based
- ☐ Knowledge-based
- ☐ Biometrics
- ☐ Profession
- ☐ Behavioral

Which of these is **not** an Email domain authentication method? [Choose all that apply]

- ☐ TLS
- ☐ S/MIME
- ☐ SPF
- ☐ DMARC
- ☐ DKIM

Which type of security control includes policies, procedures, rules, standards, regulations, and frameworks?

- ☐ Logical control
- ☐ Physical control
- ☐ Administrative control
- ☐ Soft token

Exercise 1 - Wireless Security

Wireless itself is inherently unsecure. Well, how do we actually start implementing security on it? Find out more next

Wireless SOHO Security.

And if you don't know exactly what that means. The good thing is I have somebody here that actually does understand that, which is Mr. Wes Bryan. Now Wes, the very fact is people have been using the word SOHO for quite a bit of time now. But if you're new to the industry and not exactly sure, tell us what that means and why wireless is such a big part of it.

Sure, so SOHO stands for small office, home office. And a lot of times what we use that term to describe. And maybe an office if you will could be a home office could be office that literally, maybe we hear that term mom and pop store, right? Maybe somebody is running right out of their home, doesn't necessarily have to be at home.

It could be a place of business, but typically it is no more than 10 computers, all right? You can have multiple, you could have more devices on your networks, but a lot of times what you'll see is that it's really restricted. To more of what like Microsoft calls a workgroup, right?

10 computers, nothing more after that we have to move into more of a business or an enterprise type network in order to maintain it. So what we're gonna be talking about in this episode is some of the security settings that you can implement, like Ronnie says. To kind of secure a wire or a communication technology that it is inherently unsecure.

So we're gonna talk about that all in this episode.

When it comes down to that small office, home office, even if we actually have everything cable together, more than likely we're also gonna include wireless in that type of network here. So, when we start doing that and we start to say, hey, we want to buy a wireless access point.

What are some of security features we're actually looking at here.

Yeah, Ronnie. So one of the first things that we have to do when we purchased our wireless access point, remember it could be on the shelf for a little while. And, just because it's on the shelf doesn't mean that the manufacturer stops developing software for it and the software and it's not really software.

What I'm talking about is the code that is in the firmware. One of the first things that we have to do before we put any device into implementation before we connect any user to it, is we need to update the firmware that is gonna be important. The other thing that we have, we have to do is we have to change the defaults.

And that's because when you first buy an access point, you're gonna open the instructor or the the instruction manual and you're gonna see there's a default user name and password. You can actually go up on the manufacturer's website and you can find that default user name and password.

So that presents a problem. That means that if I use those defaults and I put this access point into production, then I have a potentially exploitable access point. Because everybody can gain access to the default user name and the default password. So for instance, some of them will require you before you even go to configure them, they're gonna require you to do something like this.

So, you're gonna have to create a user name or potentially change the user name. Let me zoom in here a little bit. And then what we're gonna do, is we will create our password and let's see if I can type the password, same password twice, nope. Apparently I cannot, so we'll try that one more time.

There we go, and then from here we can confirm that the password has been changed, right? So that's one of the first things that you need to do. Now remember I also talked about the firmware, we've got a little W A 12 01 TP link that is on our desk.

And by the way keep in mind what we're using here are some emulators to and you can go up to TP link's website. And they have a lot of emulators for almost every product they have in the market. So if you have never been in one of these web interfaces and you wanna get your hands on that, go to TP Link's website.

Now, once we've done that, let me flip over to the access point that we've got here on our counter, that we're also using. Remember I said the next thing that you have to do is you have to get the firmware. Now, if we look all the way at the bottom of this screen, I can see what the firmware number is, right?

So it tells me what the firmware build is, the version number and now it's up to me to go up to TP Link, put in my model number and download the latest firmware, right? And then once we do that we can come into system tools here. And while the web interfaces are gonna probably be different in the different devices that you can figure.

For the most part, they have a lot of the same settings and again, it's just a different coat of paint if you will. And then if I scroll down over here on the left hand side, you can see that there's a firmware upgrade. Now, I will tell you that I'm gonna show you this.

I have already gone to TP link and I've downloaded the firmware, I'm not going to do this here in the show. For the same reason I'm gonna tell you all to be careful with this, all right? When you upgrade your firmware, you wanna make sure that there is no, there isn't a chance.

The chance is very, very slim, that you could interrupt that upgrade process, which means never do this during a lightning storm. Never do it during a rainstorm. Make sure your device is plugged in, and that it will not be unplugged or powered down during the firmware updates. So for instance, it's asking me, where's the new firmware file?

I could browse to it, I could point it to the new firmware file and then I could flash that firmware. Again, that's how the process would do, and then I could choose upgrade. So that's one of the things that we have to do. The other thing that they also call out is going over to the wireless settings.

If I go over to the wireless settings, they talk about changing the default S S I D, right? That's called the service set identifier. It's essentially a network name and it's what other devices will use to identify this access point in this network. Well, they tell you to change the default S S I D, why?

Well, the default S S I D, you can see for instance for this one in here says TP link, write in the name. So that let's anybody that's outside of your network know that when it's broadcasting the S S I D, you have a TP link so they can use it for reconnaissance if you will.

And they can start to figure out what your devices on your network and what they need to attack. So we typically change the default S S I D. Ronnie, here's another one, and I tell you, I know it's called out on the exam and this is the hiding of the S S I D.

They say disabled S S I D broadcast, all right? Now there's schools of thought on this and I'm not gonna get into the lectures on that and the the different debates, okay? All right, when you hide the S S I D. All right it means that for somebody to find that network you will have to manually on the client type in the appropriate S S I D.

Because your access point isn't broadcasting out it out there, it's not gonna show up in your wire available wireless network list. So that's what I would say about doing that. The other thing too is if you have any services that might be running on your access point that you aren't currently using, disable them.

Why? Because that disables the ports that are associated with those services. So for instance, in my home router that I had my home wireless access point. Ronnie, it had an FTP server. All right, it wasn't enabled by default, but if I wanted to enable it, I could enable it.

We don't just enable things because we think we might use them. Make sure that you are using them, especially with something like FTP, because it's inherently insecure. So make sure you disable unnecessary services, which by association closes down open ports and if you need a port to be open, then use something like port forwarding.

And what that says is when a request for that service comes in, we're gonna forward that request for the to a specific intended, computer within your network. So those are some of the first things Ronnie, firmware and defaults. We need to upgrade our firmware and steer away from the defaults.

Yeah, all that actually makes sense because the very fact of everybody tends to buy these things, and that means that they actually set those defaults there. And so everybody can get into whatever your system is gonna be if you don't change those Just by you plugging that in.

Now we actually have to protect ourselves more than that, because not only is it inherently unsecure in terms of that. So how do we actually begin to secure the signal that we're talking about?

Sure. So that's gonna be through two things, right? And two things, one is going to be authentication and the next one is going to be encryption.

Alright, authentication means I am only going to allow those devices on my network that can prove they are who they say they are by typing in the password that we set up on the wireless network. Then we also use encryption. Not only do I want to know that only the authorized devices are authorized to connect to my network when they send and receive communications.

I want that wireless access point to wrap that information into a cryptographic wrapper if you will that we call encryption. So that as it passes through transmitter and receiver, if somebody's out there listening to your network, they might be able to get the information. But there's no way they could unwrap it and remove that outer layer of encryption and it keeps your data safe.

Now, it doesn't just by default keep your data safe because you have options. And we need to talk about those options. All right. Now, if we look here. And by the way, ladies and gentlemen, this goes for 2.4 and five gigs. All right. But I want you to know that we have a few different options when it comes to the encryption or the authentication methods that we can use.

Some of them aren't options anymore. And that's because some of them have been around for a very long time. Like web. Wired equivalent privacy is one of the oldest encryption technology or authentication technologies if you will within wireless networks and it's considered weak. Stay away from it. However, as time went on, one of the things that happened, you have a consortium out there called the WiFi Alliance.

And it's just a consortium of all wireless manufacturers. And they were working with a corporation or a body that we should know about the IEEE. The IEEE new web wasn't strong enough. So they started working on the next generation of the authentication technologies and the WiFi alliance said we need something right now because the WEP is so weak.

Alright. And they released what was known as W P A. And we can see that that's in the list to that's wifi protected access. WPA was the successor to WEP. However, it is still weak today because it would use a technology called the temporal key integrity protocol. That is technical jargon for the fact that the key that encrypts that information is gonna change constantly.

All right. But the problem was it was still using that weak encryption underneath the hood. So it was just a temporary thing until the IEEE would formally standardize the entire authentication protocol and they would release it as WPA2. Now let's be careful because WPA2 technically is the WiFi alliance marketing name.

It's the second revision of the WiFi protected access. However, the IEEE remember their standards typically follow the 802 designation. And they released this under the wireless local area network specification of 802.11 11 I. So if you see that IEEE specification and WPA2 they're the same thing. All right now WPA2 its encryption technology would give us access to something known as AES.

And that's the advanced encryption standard. Alright. It wraps it in something known as CCMP. It was the successor to TKIP. I don't need you to know the entire acronym. It's a huge acronym but just understand that WPA2 is stronger than WPA. Now, currently what we have released out there in the wild and gaining popularity is WPA3.

And when we talk about WPA3, it also allows us AES. But it also has this technology that allows your wireless clients and the wireless access points to authenticate and your hands off. All right. And I put some information about that technology, it's called the simultaneous authentication of equals, well beyond the scope of this exam.

But at least in there enough that you know that currently that is the strongest authentication protocol we have. I want you to associate TKIP with WPA CCMP and AES with WPA3 or WPA2. AES also forms the basis for WPA3. If you have to choose one or the other WPA2 is the least.

You should be using today and you should be starting to lean towards WPA3.

Yeah. So all the devices, essentially if they can negotiate the strongest possible encryption, that's really what we want to ensure that we can set it to. You will have devices though that try and connect and if they can't connect using that higher standard.

You'll probably have to back down to whatever the recommended is or less if you actually choose to but at least do some type of encryption overall. Now we along with this though. Okay. We also have that ability like you actually said to use something called like WPS. Right?

Yes. Okay. And WPS is an interesting cause it's another authentication and actually sets up WPA2 underneath the hood. The problem with WPS, this is known as WiFi protected setup. And WPS is an important authentication protocol but it does have some issues. Alright. WPS uses a pin or a push button technology that you can ensure that a pin that is on the router.

An eight digit pin is the same thing that you would put on the client side and they can communicate together. Or you could just do push button and you don't do anything. All right, here's the problem with that. It sets up a secure network that ultimately falls back to WPA2.

But that handshaking process of passing that communication has been known to be weak and vulnerable and that's why. And let me show you WPS is actually in this wireless access point too. And you can see it's a push button method, this is the recommended method. Or we could use something like a pin.

And then it's up to me to put in that eight digit pin in the client when I'm challenged to what is the password to the wireless network. However, keep in mind it should be avoided today for stronger authentication encryption methods.

Sometimes we also see the ability to go ahead and enable MAC filtering.

Why would we choose to do that?

Okay, so every time that you go your client device, like for instance my wireless or excuse me, my laptop. When I go to connect to a wireless network, we go through an association process which is just me communicating with the my laptop communicating with the wireless access point.

The wireless access point can actually check the MAC address. In that association request and it can check it against the list if we decide to turn on MAC filtering. And can say, hey, I only want the devices that have these MAC addresses connecting to the wireless network. Or we could go the other way we could say, I don't want any device that has this MAC address connecting.

Let me show you what I mean. So we're in the same location, I haven't moved far. I'll kind of zoom out so you can see where we are and then we'll zoom back in there Ronnie. I can see just under WPS I have MAC filtering. All right now MAC filtering, you can see that I have a block list, which is kind of interesting because I put my own laptop in there just to kind of show you.

Now let me go ahead and I'm gonna delete this one and it's gonna ask me how you want to do that and it deletes it. Okay. So maybe I want to allow. So again, it can be in allow a block. Alright. I'm gonna say allow. And then what I can do is I can add.

Well what's kind of cool is if you already have an existing device and you're like me, you can't type to save your life, you can type in the MAC address here. I could choose view existing devices. All right. And I could see a couple of different devices that are connected to the wireless network here.

And I can turn around and I could choose those and I could connect them or put them in this list. And then when the association request goes on, your access point checks the MAC address, and if it matches, it depends on if it's a block or allow. It performs the appropriate action blocking you from the network or allowing you on the network depending on how you set these settings.

Now along with this we have the ability instead of just using the http which might be built into the access point. Also enable static I P addressing. Right?

Sure. Ronnie and that is another one of those things where there's a debate should you use static I P address.

Well you can and you should for certain things but I'm gonna tell you if you have hundreds of wireless devices like mobile devices that are connecting to your wireless network. You will have an administrative nightmare on your hands trying to statically map all those I P addresses. Now if you have a pretty and I'm gonna say static not moving employees set that always has the same devices then it's not too hard to enable static I P addressing and you can configure each one of their devices.

That's a lot of times. Not realistic. I know we don't do that here at our at I T pro T V. On our wireless network. However, there are certain types of devices that you want to have static I P addresses right? I want my access point to have the same effect, especially if it's also being my router.

I wanted to have a static I P address that I do not want to change. Right? And I might not have to set that. That might be something that's just done by default. If I have a printer on my network. I might not want that I P address to change so I might want to do static I P address and you can actually see here.

I can set up a D H C P server here and I could enable it or I could disable it. Alright. It's all up to me but if I disable it, keep in mind the DHCP allows my clients to connect to the network. And I don't have to do anything if I disable this, I have now increased the administrative burden of managing the I P addresses within this wireless network.

So there's not a right or wrong way but you have to consider security and convenience. It's always a balance.

Sometimes they we also see an access point to the ability to actually have firewall settings in there too. Right.

We do now. It's interesting Ronnie because this 12 01, it doesn't have any firewall settings.

So what I'm gonna do is I'm gonna switch over to the wifi settings on this links. This it's a wifi six industrial router and let me go back to the default page. So you see how I got there and I'm gonna go from here. We can go to administer or excuse me.

Apple get it eventually. It's network go to network here and we have down here under firewall we've got the basic settings right. We can do I P address filtering but we can also set access control lists too. And we can set them based on packets that don't match rules are passed by this device or packets that match the rules are filtered by this device.

So it really just depends on the kind of like when we say with Mac filtering, do you want to do and allow or do you want to do a deny? Right. So blacklisting is denying packets and the white listing is allowing packets as likewise too. So we can always also potentially set a firewall.

Now, if you now in all transparency, if you have an access point like this, that doesn't have a firewall, chances are you have another firewall that's on your network that is providing that service as well. So it really just depends on how you set up the soho.

Now, a lot of access points today, especially kind of some of the fancier ones also give us the ability to do content filtering.

Yeah. Content filtering is or it might be considered called parental controls to. Content filtering is a way that you can say, hey, certain key words, certain phrases, certain websites, certain topics if you will. I don't want to allow my devices to connect to those websites and it's a way that at the access point level we can say, hey, if you are trying to get to and reach to reach these sites.

If you're using these keywords, we're not gonna allow that information to pass to the access point. Again, content filtering, I want you to think about places where there's the obvious stuff that we don't want on a work network, right? But there's other things that maybe you don't think about as well.

Maybe we don't want things like gambling sites being available within our networks as well. So we can block that content based on a certain set of criteria and what the ability is of the access point.

One of the things that most people have issues with in terms of security might be the placement of the access point to the place it too close to the wall.

And now of course the signal extends out beyond that. So talk about placement a little bit.

Sure. So we have to do things like site surveys with our wireless access points and we got to find out what is the coverage area that we need. Do we need highly directional antennas?

Like Ronnie said, hey, we've put that at maybe you put that access point close to the wall because that's the only place you could put it. Well then we need to make sure that we have highly directional antennas that are facing back to the location of the coverage area that we need.

If we need a greater coverage area in a spot where maybe our, we don't think that our signal is going to reach. We use things like Omni directional signals. So it really depends on where your signal needs to propagate because if you put, let's take Ronnie's example here.

If you put your access point right against the wall and you're now bleeding that signal over in the parking lot. Remember that's radiated energy and your communications could be being captured by somebody that you're not even aware is sitting in that parking lot. So you have to have a little bit of strategy when it comes to antenna placement as well as your AP placement.

You don't want to be putting your AP your access point in a break room right next to a microwave and wonder why every day at 12 o'clock when somebody starts using the microwave. Why you're getting very, very bad signal quality. So pay attention to your signal quality. Remember you have your wifi analyzer is you can always do things like analyze the signal strength and make sure that you place them appropriately.

Now in some of those settings that we see on wireless access point, we might see the term radius or tack acts or 802.1 X. What is that about?

Sure. Okay. So when we talk about that, those are all remote access technologies. Right. And if you're in a home network, let me show you here, let me open up my wireless settings here and I'm gonna go to wireless specifically.

All right. There is the ability to have a couple different types of authentication methods. Alright when you are in a home environment or you're in a smaller soho environment like we're talking about chances are you're going to use what is known as P S K. P S K is technical jargon for a pass phrase.

Think of it as a password and here's that password. Now what does that mean? It means when I go to connect to this network it's gonna challenge me and say enter the network password and I'm gonna enter that in. And if I've entered the password incorrectly into the interface correctly make sure I say that right.

Then I connect to the network. If you are in an enterprise level environment chances are you're gonna have access to greater infrastructure and you're gonna want to control and strengthen this process. The security around it because you do not want people writing down a password and sharing it and then allowing other people on a work network that should never have been there.

So what they'll do is they'll switch to something known as enterprise mode. Now I want you to notice something, notice something that happened when I changed enterprise mode no longer do I have a passport. What I have is a radius server. I P address radius is the remote access dial in user service and it is what we use to authenticate remote clients trying to make their way into a wireless network.

But that isn't the only thing that we couple this with a lot of times well couple it with something known as 802.1 X. And that is port based authentication. That means when an authentication request comes in. Hey, I want to join the network. The access point says, wait I got 802.1 X on.

I'm gonna close down the porch. Hold on a second. Let me go. Talk to somebody here real quick and then it'll turn around. It'll talk to the radius server now a lot of times. Your radius server is not going to do the authentication right there because that's a security vulnerability.

It can. But a lot of times what it'll do is it'll talk to another directory server on the back end within your network and that directory server will say yeah, I know who Ronnie Wong is. Yeah, go ahead. Develop a pass phrase for him. Send it back out.

Let the access point know. And then the access point that's got the 802.1 x, technology on it. He says all right. You're allowed to be on this network and there's more to it that's overly simplified. But it allows you on that network at the end of the day.

Radius allows your company to control the pass phrases that are entered from the radius server. Not manually. Alright, anytime we talk about a user name entering a pass or user entering a password that comes with all the vulnerabilities of human nature. Alright, this says let the machine do it on your behalf and that's what we use inside of our corporate environments.

Now Ronnie, I'd like to bring you in here because there is one technology that I know that you've had to deal with before and, so radius is an industry wide standard. It's widely supported out there. However, it is not our only option. There is another one out there.

Can you talk a little bit about this terminal access control access control system. What an acronym more commonly known as Tacas+.

Yeah, when it comes down to the idea of tacacs plus, it works similar to the way that radius does work. It provides for us the ability to do authentication, authorization and accounting but it actually secures the entire thing.

Whereas radius really does secure the password during that initial phase of doing all the things that it actually needs to do. It is a much more complex system but it is a more secure system to be able to do so. But Tacas+ itself is Cisco proprietary. So when you actually do set up a server like this, it is gonna be based on the Cisco technology itself which is not the easiest to go ahead and set up.

And if you're actually doing this on a router today, a lot of times you actually do, the only thing you really have to do is make sure that you're pointing to the right IP address. But you were setting it up manually there'd be a lot more configuration that you'd have to do.

So it's a little bit more secure in that sense where everything in that process is secured all the way through the entire authentication process, the entire handshake everything about it. And that's what really makes it more secure.

Thanks Ronnie. And that's one of the things that we should take away from the remember radius and tech acts our remote access technologies 802.1 X export based authentication.

And a lot of times they're used together to strengthen the security of your wireless network. Now I do want you to keep in mind that while they are commonly used as a way to strengthen wireless security, they can be used in wired networks as well. And that's something at the end of the day, I want you to be able to recognize in a situation where they say.

Which of these technologies will allow us to strengthen our security in our wireless access point enterprise mode with radius most likely is gonna be the choice that wins out at the end of the day. Alright, well thank you again for actually helping us to understand a little bit more about the wireless soho security but there is plenty more to come.

Which of the following does SOHO stand for?

- ☐ Small Operating Home Office
- ☒ Small Office Home Office
- ☐ Small Office Help Office
- ☐ Small Option Home Office

When going over the wireless settings, why is it recommended to change the default SSID?

- ☐ To be able to see what devices people in other networks use
- ☐ To be able to share your devices with others within your network
- ☐ To be able to share the devices you are using with others outside your network
- ☒ Anybody from outside your network will be able to figure out what devices you are using and what they could attack

Which of the following would you use to secure a signal? [Choose all that apply]

- ☐ Network Name
- ☒ Authentication
- ☐ Device Names
- ☒ Encryption

Which of the following would be the best way to ensure that devices on your network do not gain access to certain websites containing specified words?

- ☐ Content Deleting
- ☒ Content Filtering
- ☐ Content Enabling
- ☐ Content Creation

Which of the following are examples of Remote Access Technologies? [Choose all that apply]

- ☒ 802.1 X
- ☒ TACACS
- ☐ WPA3
- ☒ RADIUS

Lab 19-3: Securing a SOHO Network

Exercise 1 - Home Router Settings used to Increase the Security Posture

In this exercise, SOHO and home router settings that can be changed to increase the strength of the security posture will be discussed.

You will learn about the importance of changing the default information that is supplied with the computer and networking equipment. You will also learn about the placement of these devices to ensure the best performance and security and protocols such as IP and Content Filtering to limit the exposure of the network to certain traffic.

Home Router Settings

Home routers are usually supplied by an Internet Service Provider (ISP) and allow you to connect your system in the home network to the Internet. The different settings that can be configured to improve security are discussed below.

Change Default Passwords

Username and passwords are two of the most commonly used methods for protecting our networks, computers, and data. Our equipment comes with default usernames and passwords from the manufacturer. As a best practice for security, these should be changed and should be done during the initial configuration. This is necessary because those usernames and passwords are typically easy to guess and remember. Default router passwords are written in manuals and are available online, so if you're having trouble configuring your router, check the product manual for the default password.

Threat actors can do the same. If you can look it up, they can also have access. For instance, a common login for a home router would be a username of admin and a password of admin. If you don't change your router's password,

anyone who has access to it can change its settings and even lock you out. You can relate this to purchasing a home. When purchasing a home, it is common practice to change the locks on the doors. Anyone with the old key would still be able to enter the house, so extra precaution is taken. The same is true for our computer equipment. Any default passwords should always be changed.

The following is a general description of how to change the password on your router. This will change the password to access the router and make configurations. Because routers are manufacturer-created and not standardized, each one will have a slightly different setup.

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing ipconfig.
- Log in with the default username and password.
- Go to the settings or security tab.
- Select Change Router Password or a similar option.
- Enter the new password.
- Save the new settings.

Another default password that should be changed is the pre-shared key that connects to the wireless access point and provides Wi-Fi access to devices. Similar to router configuration passwords, these passwords are simple to guess and easy to find. The password is frequently found on the bottom of the device itself. The following is a general description of how to change the password for your pre-shared key. Because routers are manufacturer-created and not standardized, each one will have a slightly different setup.

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing ipconfig.
- Log in with the default username and password unless you have changed it
- Click the wireless tab.
- In the name or SSID box, change the name of the network to the desired name.
- Choose the highest security level possible. It should be WPA2-PSK (AES)
- Enter a new passphrase into the text box.
- Click Save.

IP Filtering

IP filtering, in conjunction with network address translation (NAT), can help protect your PC and network from malicious actors. Filtering IP addresses allows users to control what traffic enters and exits the network. Rules are created, and packets entering and leaving the network are inspected to ensure that they comply with the rules specified.

Filtering addresses helps to reserve our private address space as well. You can use NAT to conceal your unregistered private IP addresses behind a set of registered IP addresses. This aids in the protection of your internal network from outside networks.

Listed below are some common IP Filtering techniques:

- **Route Filtering** - This process helps filter out undesirable routes. Filters can be applied at the routers either before or after the routes are announced. In some cases, routers do not have enough main memory to store the entire global Border Gateway Protocol table. There is only so much space to store, and the local database is limited in size. Applying filters helps conserve memory. This practice is not recommended because it can result in suboptimal routing or even communication failures with small networks, as well as disrupt the normal flow of traffic.
- **Firewall Filtering** - A firewall is a device or software application that allows or denies network transmissions based on a set of rules. Its purpose is to protect networks from unauthorized access while allowing legitimate traffic to pass through an access control list. Many routers that transfer data between networks include firewall components, and many firewalls can also perform basic routing functions.

- **Email Filtering** - Email filters work by, among other things, matching a regular expression, a keyword, or the sender's email address. More advanced solutions use IP blacklists, techniques for classifying documents, and complex image analysis algorithms to prevent messages from reaching protected mailboxes. Clean messages are delivered to the user's mailbox, while tainted messages are routed to a quarantine application for review or even ignored. Email filtering can be very useful within an organization but can become a problem when an IP is improperly blacklisted.

Disadvantages of IP Filtering:

- Malicious traffic is frequently routed through Botnets, allowing it to bypass the filter.
- It can be easily circumvented by using IP spoofing, VPNs, or proxies.
- When using NAT, IP addresses are frequently shared by multiple users.
- Maintaining the Blacklist can become a tedious task.

Firmware Updates

Firmware is software that is embedded in hardware. Simply put, it is "software for hardware." However, because software differs from firmware, the two terms should not be used interchangeably. Devices that you might consider to be strictly hardware, such as an optical drive, network card, programmable switches, and routers, all have software programmed into a special chip contained within the hardware itself. This tells the piece of hardware how to act and what to do. Firmware updates are released by equipment manufacturers to improve performance or add new features to their devices. You can get these updates by going to the manufacturer's website.

Below are the common steps to updating your home router's firmware:

- Connect the router to your PC. You will need an Ethernet cable.
- Open your browser, navigate to the manufacturer's website, and locate the firmware update. Download it.
- Files will usually be zipped. Unzip them.
- Enter your router's IP address into your web browser.
- Log in with the default username and password unless you have changed it.
- On the home page, select the downloaded firmware to update your router.
- Select the firmware file previously downloaded and uploaded.
- Reboot your router to finish the upgrade.

Content Filtering

With the invention of the World Wide Web, users began to have access to several resources. Hence, the need for content filtering became a necessity in many situations.

There are numerous reasons why users choose to restrict access to certain content, including online gambling, social networking sites, dating sites, intellectual property, child safety, and national security. Content filtering is not just enabled at the end user's terminal, it is done throughout the data movement process. There are national mandates that are in place banning traffic and content from other specified countries.

ISP carriers may install blocking tools and filters to control traffic on the network. At the local network level, end users' terminals are required to meet specifications in the network security policy. Enterprise environments will typically have a well-designed content filtering program, whereas SOHO environments will not.

Below are some considerations when deciding on content filtering:

- Who will be subject to the filtering?
- How well defined will the policy be?
- How will this affect the end-user, and what are the possible negative outcomes?

Common Types of Content Filtering:

- **IP & Protocol Based Blocking** - IP-based blocking entails installing network barriers such as firewalls that block all traffic to a specific set of IP addresses. Protocol-based blocking employs other low-level network identifiers, such as a TCP/IP port number that can identify a specific application on a server or a type of application protocol. These fundamental approaches to content blocking do not block content directly; rather, they block traffic to known IP addresses, TCP/IP ports, or protocols associated with some content or an application. IP and protocol-based blocking can also be performed on user computers by software, typically for network security reasons.
- **Firewall & Deep Packet Inspection (DPI)** - Devices that sit between the end-user and the rest of the Internet and filter based on specific content, patterns, or application types are used. Because all content must be evaluated against a pre-defined set of rules, this type of network blocking is computationally intensive and thus considered expensive. DPI blocking can also be done by software on user computers, typically for network security reasons. DPI blocking requires some type of signature or information about the content to be effective. Keywords, traffic characteristics such as packet sizes or transmission rates, filenames, or other content-specific information may be included. DPI blocking is a powerful tool for blocking or throttling specific applications, such as peer-to-peer file-sharing or Voice over IP (VoIP) traffic and data file types.
- **URL Blocking** - URL-based blocking is a popular blocking method that can occur on a single computer or in a network device that connects the computer to the rest of the Internet. URL blocking only works with web-based applications and is not intended to be used to block non-web applications. A URL blocking filter intercepts the flow of web traffic and compares the URL in the HTTP request to a local database or online service. The URL filter will allow or deny the requested connection to the webserver based on the response.
- **Platform Blocking** - The most common type of platform blocking is search engine blocking. This technique is frequently considered for other platforms with user communities like entertainment or social media sites. It is extremely difficult to use network-based or URL-based techniques to block individual content elements, such as a specific news article. Access to the entire site would have to be blocked in order to block the content.
- **DNS-Based Content Blocking** - DNS-based content blocking examines and controls DNS queries. A specialized DNS resolver performs two functions in DNS-based content blocking: in addition to performing DNS lookups, the resolver checks names against a block list. When a user's computer attempts to use a blocked name, the special server returns erroneous information, such as the IP address of a server displaying a notice that the content has been blocked. As a result, the user can't easily access the content.

Physical Placement

A SOHO router is designed and marketed specifically for small and home offices. It can handle more traffic because of enhanced equipment. A SOHO network can consist of both wired and wireless computers. Because these networks are also intended for business use, they may include printers as well as voice over IP (VoIP) and fax over IP technology. Where the router/access point is setup in a SOHO environment can play a big part in its ability to function at the highest level with wireless clients.

There are some common suggestions listed below:

- Place the router/access point as close to the center of the environment as possible. Signal strength radiating from your wireless access point degrades the further out it goes. If placed in the center of the environment, the coverage space can be maximized.
- Place the router/access point as high as possible so the signal radiates evenly and disperses throughout the SOHO environment.
- Use additional access points or a repeater to extend the signal. If areas of the SOHO environment are getting signals, additional access points can be added, or repeaters can be used to extend the signal from the original router/access point.
- Minimize the number of walls that can interfere with the signal. The wavelengths can have trouble penetrating through walls, especially in the 5GHZ range.
- Do not place them inside cabinets. This degrades the signal because it bounces around in the cabinet.

- Electronic and common household devices can be working on the same frequencies that our traffic is being carried and can create interference. Microwaves and remote controls are known for working within the 2.4 GHz range.
- Disable the WPS button. This feature allows users to enter the network without having to enter the credentials. On the router, a button is pressed that broadcasts out a signal, which is then used to connect to the network. This is very problematic, and thus the WPS button should be disabled for best security practices.

There are some security concerns inherent within a SOHO network. Small businesses, unlike larger corporations, typically cannot afford to hire a professional staff to manage their networks. Because of their financial and community standing, small businesses are more likely to be targets of security attacks than households.

It can be difficult to know how much to invest in network infrastructure to meet a company's future needs as it grows. Overinvesting too soon wastes money, while underinvesting can have a negative impact on business productivity. Monitoring network load and the responsiveness of the company's top business applications can aid in the identification of bottlenecks before they become critical.

Dynamic Host Configuration Protocol (DHCP) Reservations

In SOHO and enterprise environments, you are likely to be using a dynamic host configuration protocol to manage the IP space. DHCP is responsible for distributing IP addresses to the network. In a SOHO environment, this is likely built into the capability of the router. In an enterprise environment, this is likely to be a function of a server. DHCP will automatically distribute an IP address to a machine entering the network.

Would we want devices to have the same IP address all the time? The answer is yes. Some devices like printers and servers should be statically set in the network because they provide services and should be easily found. In order to set a device statically and ensure that DHCP is not going to give it to another machine, a DHCP reservation needs to be set.

Below is a general description of the process of setting a DHCP reservation in a SOHO environment with DHCP being provided by the router.

Open the command line and type `ipconfig /all`. Capture the details for the default gateway and the MAC address of the machine. A Wi-Fi card and Ethernet port need to have two different MAC addresses and will have to have a different IP as well. Write down whichever IP you use the most.

- Enter your router's IP address into your web browser. This is also known as the default gateway and can be located in the command line by typing `ipconfig`.
- Log in with the default username and password unless you have changed it.
- Find the DHCP reservation setting. It might also be listed under Static Lease or some variation.
- Type in the MAC address of the desired machine for the MAC address field.

Type in the IP address desired for the Static IP address field.

- Repeat the steps for any other computers, servers and printers that require a static address.

Static Wide-Area Network (WAN) IP

A wide area network IP is a public or global IP address that is routable on the Internet. This type of address is usually assigned via an Internet Service Provider and gives users access to the World Wide Web. You can find out what your WAN IP address is by a simple search on the Internet. This is different than the Local Area Network (LAN), where an IP will be given from the private IP address range from a DHCP server or after being statically set.

Below are the different IP ranges and the private address space for each.

Public IP Ranges:

- Class A: 1.0.0.0 - 126.255.255.255
- Class B: 128.0.0.0 - 191.0.1.255
- Class C: 192.0.0.0 - 198.17.255.255

Private Ranges:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16. 0.0 – 172.31.255.255
- Class C: 192.168. 0.0 – 192.168.255.255

Universal Plug and Play (UPnP)

PnP and UPnP are 2 terms that are very similar but have some clear distinctions. Plug and play (PnP) is a collection of operating system standards that enable hardware connectivity via automatic device detection and configuration. When new hardware is connected to a computer, it is automatically detected, and the necessary files and drivers are installed, allowing the hardware to function and communicate.

Universal Plug and Play (UPnP) is a set of protocols and technologies that enable devices to discover and connect to one another automatically. When it functions properly, it automates all of the complex steps required for devices to communicate with one another, whether directly or through a network. To support zero-configuration networking, Universal Plug and Play employs standard networking protocols.

When a device joins or creates a network, UPnP does the following:

- Provides an HTML-based user interface for controlling or viewing the device's status.
- The device is updated.
- Gives an IP address to the device and informs the network.
- Describes the device's capabilities, such as whether it is a server, printer, or scanner, as well as the device's network availability and shares to the other network devices.

Common uses for Universal Plug and Play:

- Adding a network-attached printer.
- Using a media server to share photos and stream content.
- Home Automation & Surveillance.

However, this technology is not without flaws. There can be issues with security. The main problem with Universal Plug and Play is that it lacks an authentication mechanism. It simply trusts that the devices attempting to access and use the network are legitimate and grants access. Many of the network security features put in place to stop threat actors can be circumvented by a compromised computer. This risk, however, can be greatly mitigated with proper implementation.

Screened Subnet

A screened subnet, DMZ, or triple-homed firewall all refer to a network in which a firewall with three network interfaces is used. This enables it to provide some additional protection against cyber-attacks from outside sources.

A separate network is established in which internet-facing appliances can be installed. For example, Techies Company hosts a website on a web server that is set up to be in the screened subnet. When a user searches for the web page on the internet, they will only be able to access the screened subnet area. All of Techies Company's private data that they do not want to be exposed is kept on a separate network. If an employee from Techies

Company was working from home, they would be able to use their credentials to authenticate and get into the subnet.

Exercise 2 - Wireless Settings to Increase Security

In this exercise, Wireless networks and ways that can be used to secure them will be discussed.

You will learn about the importance of the SSID, changing the default settings, hiding an SSID and how it can help with security.

The different types of encryption and Wi-Fi standards and accounts to use, to help protect our wireless environments will be discussed. You will also learn about channels and their importance to wireless communications and discuss best practices to increase network performance.

Wireless Specific Settings

Wireless security settings should be properly configured to ensure there is no threat from malicious users accessing the wireless network in a SOHO. The different wireless-specific settings will be discussed below.

Changing the Service Set Identifier (SSID)

The Service Set Identifier is the name of the wireless access point, which allows users to connect to the network and have access to Wi-Fi. Routers are shipped with a default SSID from the manufacturer. Changing this can help to improve the posture for security reasons. Usually, default SSIDs are paired with default passwords on the internet documentation and can help threat actors identify the type of router being used. It is easier for them to find and execute this information to exploit your wireless network.

To change the SSID, generic instructions are provided below:

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing `ipconfig`.
- Log in with the default username and password unless you have changed it.
- Go to the wireless menu.
- Change the default SSID to the desired SSID.
- It is also recommended that you change the Pre-Shared Key (PSK).
- Save the new settings.

Disabling SSID Broadcast

Turning off SSID Broadcasting adds an extra layer of security to a wireless network. This will not broadcast the network name, so users will not be able to see your network name when attempting to connect to a network. Users who want to join will need to know the network's name. The network's name is very specific. If Techies Company created a network called Techies, it must be entered exactly as such. Users attempting to connect to Techies would be unable to connect to the network. This type of security will help keep out common users and unskilled threat actors.

The SSID can be compromised with the help of some simple and free tools. This level of security provides no encryption and is considered slightly higher than having an open network.

To disable the SSID broadcast, generic instructions are provided below:

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing ipconfig.
- Log in with the default username and password unless you have changed it.
- Go to the wireless menu.
- Enable the checkbox to hide SSID.
- It is recommended that you also change the default SSID to a desired SSID.
- Best practice is to change the Pre-Shared Key (PSK) as well.
- Save the new settings.

Encryption Settings

To provide maximum protection, wireless network security relies on a combination of encryption, authentication, and authorization. Encryption is concerned with protecting information within a session, reading the information in a data stream and modifying it so that it is unreadable to users outside the network.

Routers will receive packets of information from a device and apply the encryption standard to them. Block cipher is most commonly used, where a set size of data is filled and then encrypted in chunks. There are also stream ciphers that encrypt information bit by bit, instead of waiting for a block to fill to encrypt.

There are four encryption protocols available on most routers today.

1. Wired Equivalent Privacy (WEP) encrypts information packets as they are sent out from the access point or wireless network card using the RC4 stream cipher algorithm. Once the access point receives the packets sent by the user's network card, it decrypts them. Instead of being encrypted in blocks, each byte of data is encrypted bit by bit with a unique packet key. This ensures that if a hacker cracks the packet key, the only information leaked is that which is contained in that packet. A pre-shared password, a state array, and an initialization vector are combined to form the packet key (IV). The IV is a computer-generated 3-byte random number. It is either prepended or appended to the ciphertext before being sent to the receiver, where the computer removes the IV before decrypting the ciphertext. All and all, this encryption is a very weak encryption standard and was almost immediately cracked upon its release.

2. Wi-fi Protected Access (WPA) encrypts information packets as they are sent out from the access point or wireless network card using the Temporal Key Integrity Protocol (TKIP). This protocol is considered to be cracked and is no longer considered safe. When a device connects to a WPA network successfully, keys are generated through a four-way handshake between the access point and the device. A message integrity code is included when TKIP encryption is used to ensure that the data is not spoofed. It takes the place of WEP's weaker packet guarantee, known as cyclic redundancy check. All in all, this encryption standard is better than WEP but has since been updated.

3. Wi-fi Protected Access 2 (WPA2) encrypts information packets as they are sent out from the access point or wireless network card using the Advanced Encryption Standard (AES) algorithm. When WPA2 is enabled with the strongest encryption option, anyone within network range may be able to see the traffic, but it is scrambled using the most recent encryption standards and is accepted by the Department of Defense as the industry standard. This standard has stood for quite some time and is still continued to be supported.

4. Wi-fi Protected Access 3 (WPA3) is the most recent generation of Wi-Fi security, released in 2018. It has not yet gained widespread acceptance, but it aims to improve some security aspects that WPA2 lacks, such as securing open networks, protecting simple passwords, and simplifying device configuration.

Disabling Guest Access

Most routers allow the capability to create separate networks for your personal devices and guests who are accessing the Wi-fi. In high traffic areas where customers may need Wi-fi, for example, coffee shops, a guest network will be vital. In general, if one is not needed, you may want to consider disabling the account. It is inherently

not secure, so it is susceptible to unwanted connections. The more users connecting to the Wi-fi and using the bandwidth, the slower the service will be. Also, guest networks are the first door into your network for a skilled threat actor. Below are the generic steps for you to access your router and check to make sure the guest account is disabled. Each router will have a slightly different interface due to them being manufacturer-specific.

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing `ipconfig`.
- Log in with the default username and password unless you have changed it.
- Go to the wireless menu.
- On the main pane, you should see the guest network. Make sure the check box is not enabled; deselect it if it is.
- Click Save.

Changing Channels

Wi-Fi channels are the channels that your wireless Internet network uses to send and receive data. Having more channels can help your Internet connection run faster. The number of WiFi channels that you have and are able to use is determined by the type of router that you have. Most routers use the 2.4 GHz frequency, which has 14 channels and the 5 GHz frequency, which has 45 channels. Each one of these network types has its advantages and disadvantages. We will cover those below and give a generic description of how to access and change the channel of your Wi-Fi.

2.4 GHz, as previously stated, has 14 channels. This may appear to be sufficient, but keep in mind that these signals are radio waves that radiate omnidirectionally. As a result, there are only three recommended channels that you should use so that their frequencies do not overlap and can help with signal interference. Channels 1, 6, and 11 do not overlap and are the three channels recommended for 2.4 GHz networks. It is a slower standard because the 2.4 GHz network has fewer channels and, thus, fewer lanes for traffic to move. It also happens to be a frequency that many of our household appliances, such as microwaves, remote controls, and IoT devices, use, which can cause interference with the frequency. The advantage of using a 2.4 GHz network is its coverage area and ability to spread through an environment regardless of walls.

5 GHz, has 45 channels. This is adequate and provides some flexibility in terms of channels and channel bonding to increase speed on the 5 GHz network. It is not imperative to choose a channel like 1, 6, or 11 due to channel availability. It is a faster standard than the 2.4 GHz network, which has fewer channels and thus fewer traffic lanes. The main disadvantage of using a 5 GHz network is its limited coverage area and ability to spread through walls. The signals are shorter and choppier, and they do not radiate as well as 2.4 GHz signals. The signals have a difficult time passing through structures.

The following is the process for changing your channel on your router:

- Use a Wi-Fi analyzer to see other networks around you. For the 2.4 GHz network, determine the best channel to switch to 1, 6 or 11.
- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing `ipconfig`.
- Log in with the default username and password unless you have changed it.
- Go to the wireless menu.
- Click on each standard 2.4 and 5 GHz.
- On the main pane of each page, you should see the channel.
- Select the desired channel.
- Click Save.

Exercise 3 - Firewall Features

In this exercise, you will learn about computer ports and their purpose. Port forwarding and its uses, as well as how to configure their settings, will be discussed.

Firewall Settings

SOHO routers have firewalls. The firewall settings can be configured to filter specific types of traffic from the Internet, disable unused ports, or access a particular device in the internal network.

Port Security & Disable Unused Ports

Ports are logical, and port number ranges from 0 to 65,535. **Well-known Port** numbers have a range from 0 to 1023 and are reserved for common TCP/IP applications. **Registered Ports** are for other less common protocols and range from 1024 to 49,151. The remaining range from 49,152 to 65,535 is covered by **Dynamic Ports**, which the computer uses to help monitor traffic.

Some ports may need to be open depending on what you do, while others may not. To keep computers secure, the state of their security should be frequently assessed. This is referred to as hardening the computer and decreasing the attack surface. For instance, if you are housing a web server, you would want to ensure that you have HTTP and HTTPS protocols enabled. Each of these has a standard port associated with its traffic. HTTP uses port 80, which is insecure, whereas HTTPS uses port 443, which uses TLS to provide encryption and is considered relatively safe. When you assess the networks and computers, you can determine the ports and protocols you need to use and harden the system accordingly.

The following are some common ports:

- 20/21 - File Transfer Protocol (FTP)
- 22 - Secure Shell (SSH)
- 23 - Telnet
- 25 - Simple Mail Transfer Protocol (SMTP)
- 53 - Domain Name System (DNS)
- 67/68 - Dynamic Host Configuration Protocol (DHCP)
- 80 - Hypertext Transfer Protocol (HTTP)
- 110 - Post Office Protocol 3 (POP3)
- 137/139 - Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)
- 143 - Internet Mail Access Protocol (IMAP)
- 161/162 - Simple Network Management Protocol (SNMP)
- 389 - Lightweight Directory Access Protocol (LDAP)
- 433 - Hypertext Transfer Protocol Secure (HTTPS)
- 445 - Server Message Block (SMB)/Common Internet Files (CIFS)
- 3389 - Remote Desktop Protocol (RDP)

Port Forwarding/Mapping

Port forwarding allows computers on the Internet to connect to a computer in a private network. It works in conjunction with Network Address Translation (NAT). For instance, if a user wants to connect to their PC remotely using remote desktop protocol, they will send a request to their public IP address over port 3389. The home router will have to be configured with port forwarding to send the traffic to the computer. Typically, there will be a port forwarding page where you will enter the port and IP addresses to which the permissions will be applied.

Remote desktop also has to be enabled on the home computer. Once configured, the remote desktop connection will be allowed, and port forwarding will occur. That is one example of port forwarding, but it has several other uses,

including Backups, Virtual Desktops, CCTV and Security & Game servers, to name a few. Below are generic steps to configure a router with port forwarding. Each router will have a slightly different interface due to them being manufacturer-specific.

- Enter your router's IP address into your favorite web browser. This is also known as the default gateway and can be located in the command line by typing ipconfig.
- Log in with the default username and password unless you have changed it.
- Click the Port Forwarding configuration page.
- Name the application.
- Enter the external port number.
- Enter the internal port number.
- Enter the IP address of the computer being connected to.
- Check Enabled.
- Click Save.

Which of the following is a set of protocols and technologies that enable devices to discover and connect to one another automatically?

- ☒ UPnP
- ☐ DHCP
- ☐ Screened Subnet
- ☐ PnP

Which Wi-Fi standard encrypts information packets as they are sent out from the access point or wireless network card using the RC4 stream cipher algorithm?

- ☐ Wi-fi Protected Access 2 (WPA2)
- ☐ Wi-fi Protected Access 3 (WPA3)
- ☒ Wired Equivalent Privacy (WEP)
- ☐ Wi-fi Protected Access (WPA)

What's the port number for Hypertext Transfer Protocol Secure (HTTPS)?

- ☐ 143
- ☐ 80
- ☐ 389
- ☐ 22
- ☒ 443

Which of the following are easily researchable and should be immediately changed upon setting up a device?

☐ UPnP

☒ Default Passwords

☐ Screened Subnet

☐ Firmware

Which of the following are IP Filtering techniques? [Choose all that apply]

☒ Email Filtering

☒ Firewall Filtering

☒ Route Filtering

☐ Password Filtering

Live Virtual Machine Lab 19-4: Remote Access Methods

Exercise 1 - Work with Remote Access Technologies

Remote Desktop Protocol is a remote connection protocol that allows users to directly connect one device to a Windows OS device. Port 3389 is used for Remote Desktop Protocol. It is a built-in remote management tool in Windows 10. You can connect to another computer's desktop using RDP, allowing you to work on the device remotely like you were sitting in front of it. You can troubleshoot issues and errors. Administrators can RDP to a Windows device and take over control of the system. Only one user can be signed in at a time, and the administrator takes precedence, and the user would be signed off. By default, the Remote Desktop feature is enabled in Windows 10.

Remote Assistance allows a user to request help from a technician. An email will be sent to the technician, and a password will have to be provided to secure the connection. Quick Assist is an update to Remote Assistance that allows a technician the ability to give a code to users to help them. The user enters it on their machine, and a series of permission checks are done before the connection is made. Using either Remote Assistance or Quick Assist, the technicians can simply view the user's screen or take control of the computer. The user will be able to view the screen at all times.

Task 2 - Secure a Remote Desktop Connection

When users virtually connect to a Windows system from another computer, they have complete access to the operating system, even though they are not in front of it. Although Remote Desktop has practical usage in different scenarios, there are obvious security risks as well. For example, a hacker may gain access to the user's credentials and attempt to connect to the system remotely.

Click the **Start** charm and type the following:

```
local security policy
```

Task 3 - Setup Remote Assistance

Microsoft Remote Assistance is a Windows utility that allows users to ask for assistance with invitations. The invitation can be sent as an attachment in an email or by using quick connect. The technician would then connect to the session and enter the password. At that point, they would be able to access the shared screen, and the user could receive the assistance they requested. Since the release of Quick Assist in Windows 10, Remote Assistance has been, in a way, decommissioned. Any easy links to it have been removed, and Quick assist is now the preferred method.

Click the **Start** charm and type the following:

```
remote assistance
```

Note: The option to **Save this invitation as a file** can be used to send the invitation as an attachment through email. **Easy Connect** is an additional application that both parties should install to negotiate the session seamlessly.

Quick Assist

Quick Assist is part of the Remote Desktop Protocol family and is also used to assist users. The user receives a code from the technician and can share their screen once the code is used. The technician then receives an invitation and has the option of just viewing or being able to control the machine. Once the selection is made, one last set of permission is sent back to the user needing assistance to start the session. There are controls in the Quick Assist window to end a session and to take control back from the technician. Quick Assist was introduced in Windows 10 and is an update to remote assistance.

Virtual Network Computing (VNC)

Another type of Remote Desktop Connection is Virtual Network Computing. Different vendors provide VNC applications, several of which are open source. Virtual Network Computing is the process of connecting to a remote device to manage the device remotely. The local user connected to the device can see what the remote user is doing. The fundamental difference between VNC and RDP is that the local user will not see what the remote user is doing when an RDP session is initiated.

VNC gives a similar experience across all operating systems but with fewer features and capabilities than RDP. VNC is sluggish and ineffective for virtualization. VNC has the potential to be less secure than RDP. Both technologies give users the ability to troubleshoot issues for users and remotely connect for productivity. Users would use RDP if they needed to file share. Users would use VNC for uses like presentations. VNC will use port 5900 by default.

Exercise 2 - Work with Secure Shell Protocol (SSH)

Like RDP, secure Shell SSH is a popular way to log on to and administer computers in a secure manner. SSH operates on three main principles:

- The transport layer is responsible for server authentication
- The user authentication protocol validates the user
- The connection protocol creates the encrypted tunnel

It's a secure alternative to insecure methods like Telnet that sends information in plain text. Through encryption, SSH enables safe communication and preserves the integrity of data.

Task 1 - Perform Basic Configuration for the OpenSSH Server

OpenSSH is available in the Linux repositories. Advanced Package Tool (APT) Repositories hold several APT package files. OpenSSH is widely used for remote administration or remote file transfer. It uses SSH to help secure its communication.

On the **Terminal** window, type the following command:

```
sudo apt update
```

To install the OpenSSH Server, type the following:

```
sudo apt install openssh-server
```

After the installation, you will verify if **OpenSSH** is running.

Type the following command and press **Enter**:

```
sudo systemctl status ssh
```

Task 2 - Connect with the OpenSSH Server

After performing the basic configuration, you will need to test the connection with the OpenSSH server.

Click the **Start** charm. Scroll down and select **PuTTY (64-bit)**.

Step 2

On the **PuTTY Configuration** window, type the following in the **Host Name (or IP address)** field to connect to PLABUBUNTU:

```
192.168.0.5
```

Ensure the **SSH** option is selected, and the **Port** is **22**.

Exercise 3 - Virtual Private Network (VPN)

Virtual Private Networks are used to keep information private over unsecure networks. VPNs can be used to connect remote users to their offices, secure shopping and banking data, use public Wi-Fi, or maintain anonymity while browsing the Internet. The data remains hidden using encapsulation, tunneling and encryption. Users will connect to a Virtual Private Network server and will be authenticated. Any information that is then sent is encrypted and wrapped in another packet that is encrypted as well. Once the data is received on the other end, the outer packet is removed, and the information decrypted for use.

VPN Server

A VPN Server is a server with VPN software installed that can be used by the end-users device to establish a connection. The purpose of this server is to provide VPN services, such as encrypting and encapsulating the data packets. Once packaged, the packets will be securely delivered over the Internet to the intended destination. In theory, VPN Servers can handle about 4,000 connections. But when many connections are being used, the server's response will be slow. Large organizations may want to consider additional VPN Servers in a Clustering and Load Balancing style management.

VPN Protocols

Internet Protocol Security IPSEC

This protocol secures messages by encrypting and authenticating them. Transport and Tunnelling Mode are the two functionalities that IPSEC offers. In Transport mode, encrypting and concealing the data is performed. The Tunnelling Protocol is responsible for securing data while it is being transported across the Internet to its destination.

Layer 2 Tunnelling Protocol L2TP

This VPN protocol is not secure and needs to be paired with a security protocol like IPSEC, which will function at 256-bit encryption. L2TP will create the tunnel and connection between the two points using a Point-to-Point protocol, allowing networking equipment to communicate securely. It is reliable, robust, adaptable, and broadly compatible and can handle most types of data. A downside is that it functions at lower speeds than other VPN technologies. It is very commonly used for network-to-network connections.

Point-to-Point Tunnelling Protocol PPTP

This VPN technology is one of the original VPN options available and is based on the Point-to-Point Protocol. PPTP has built-in encryption and authentication, but it is not to the level of some of today's other standards at only 128-bit encryption. This protocol is faster than L2TP. Although it can be used on the Internet, this protocol will likely be used inside an organization to secure traffic on the Local Area Network.

Secure Socket Layer SSL and Transport Layer Security TLS

On the Internet, SSL and TLS are used to offer security and are a main component in the Public Key Infrastructure. Originally, data was transmitted on the Internet in plain text. Higher security levels were required after the emergence of the World Wide Web. People were now shopping and banking online as well as other tasks. SSL was created in 1995 by Netscape to help solve the problem with encryption and authentication. SSL is no longer supported and ended at version 3.0.

An update to SSL was needed. The Internet Engineering Task Force developed TLS 1.0 based on SSL 3.0 in 1999. The current version of TLS is version 1.3. The terms are used almost interchangeably in the industry, but there are slight differences. SSL is more complex; hence the cost of network and PC resources can be high. TLS uses new stronger ciphers when compared to SSL. TLS will provide alerts when there are bad certificates. The way the hashes are communicated for authentication is done differently.

OpenVPN

OpenVPN is an open-source VPN. This protocol has a variety of ways to allow connections and authentication. It can be used for peer-to-peer use with pre-shared keys or multiple users authenticating with certificates. It uses the

ciphers available in the SSL Library. It is compatible with all common operating systems today and is a very secure, very commonly used protocol.

Third-party VPN Services

There are 3rd party companies that provide VPN services. Some for free with limited features and servers. Others are available with a monthly subscription fee, unlocking more features and servers. You can have features such as hiding Internet traffic, obscure locations and help to bypass firewalls.

When choosing a personal VPN, you should consider the number of servers required, the location relative to your location and the number of connections allowed. Some commonly known VPN services include Express VPN, NordVPN, Surfshark, Proton VPN, Private Internet Access, and Ivacy. Each one will be slightly different with its own application interface but will generally function the same.

Exercise 4 - Third-party Tools for Remote Access

There are several built-in tools as part of the operating system, but many third-party vendors also provide remote access applications. Some of these applications can often have additional features and capabilities compared to the built-in tools. The features are usually available for a cost.

Remote Monitoring and Management

Remote Monitoring and Management technology is all about making life more efficient for the administrators. Using monitoring and management software, administrators connect to a centralized application to access statistics and information on networks and hosts. This technology simplifies the management of updates and patches, troubleshooting malfunctioning equipment, setting up new devices to the network, and monitoring service quality.

The Simple Network Management Protocol (SNMP) is used. This application layer protocol uses SNMP managers, SNMP agents, and Management Information Bases to monitor and report back to the administrator about the state of the equipment. The SNMP Manager is used by the administrator for monitoring. SNMP Agents are pieces of software installed on different devices on the network that report back to the SNMP with statistics and information about what is going on with them. The Management Information Base is a log of all the devices being managed by SNMP.

The level of security involved with SNMP will depend on the version used. SNMPv1 uses community strings for authentication and cannot be configured with TCP. SNMPv2 uses community strings to authenticate the devices and can be configured to use TCP. The newest version, SNMPv3, uses hash-based authentication and TCP, enhancing security. Examples of monitoring and management software include Jira Service Management, Connectwise Automate, Pulseway RMM, Solarwinds RMM, and Teamviewer Remote Management. Each provider has its own software and offers the same basic service with its own unique features.

Screen Sharing Software

The screen sharing software allows users to share their screens with co-workers for project creation, to help users, or for productivity. Whatever the use, screen sharing has made remote work much more possible. There are many different providers of enterprise-level screen sharing software, and many of them provide free versions. The following are some examples of screen sharing applications: Cisco Webex Meetings, Google Hangouts, Skype, UberConference, VNC Connect, and Whereby.

Video Conferencing Software

The video conferencing software allows people to establish a connection using live video and audio to simulate the sense of being together in person. This can be utilized for personal reasons as well as to have meetings and even conferences online. The following are some examples of video conferencing software: Skype, Zoho Meeting, and Zoom Meetings.

File Transfer Software

The file transfer software handles file transfers over a network from one user to another or from a server to another user. File Transfer Protocol can be used. Several third-party apps have also been developed to compensate for FTP's lack of security. Examples of file transfer software are Dropbox, Google Drive, Microsoft Teams and Smartsheet.

Desktop Management Software

The desktop management software allows administrators the ability to control all the different computing devices in the organization, from servers all the way down to mobile devices. Some common uses include managing virtual desktops, application control, device management, OS deployment, patch management, PC imaging, manage licensing and certificates, data loss prevention, remote wipe mobile devices, and restrict other user features. Some examples are Desktop Management Software Connectwise, Desktop Central, and Symantec Client Management Suite.

Which of the following is a built-in Windows tool that allows a user to connect to a computer remotely as if they were sitting right in front of it, and only one connection can be made at a time?

- ☐ Remote Assistance
- ☐ VNC
- ☐ Quick Assist
- ☒ Remote Desktop Protocol

In which of the following remote connection will a user request help from a technician with an invitation and a password to help secure the connection?

- ☐ Quick Assist
- ☒ Remote Assistance
- ☐ OpenSSH
- ☐ Remote Desktop Protocol

Which type of connection is initiated by the technician with a code that is given to the user to input? A series of permissions checks occur, and the user and technician will be connected.

- ☐ Remote Assistance
- ☐ RDP
- ☒ Quick Assist

☐ VNC

Quick Assist is an update to Remote Assistance that allows a technician the ability to give a code to users to help. The user enters it on their machine, and a series of permission checks are done before the connection is made.

Remote Assistance allows a user to request help from a technician. An email will be sent to the technician, and a password will have to be provided to secure the connection.

Remote Desktop Protocol (RDP) is a built-in graphical remote management tool in Windows 10. Using the Remote Desktop Protocol, you can connect to another computer's desktop. This allows you to work on the device remotely like you were sitting in front of it.

Virtual Network Computing (VNC) is another type of Remote Desktop Connection. The fundamental difference between VNC and RDP is that the local user will not see what the remote user is doing when an RDP session is initiated.

Which of the following is a secure connection with encryption and authentication that encapsulates packets and creates tunnels?

☐ OpenSSH

☐ SSH

☐ VNC

☒ Virtual Private Network

Which of the following remote access technology allows administrators the ability to remotely administer computers via the command line?

☒ SSH

☐ RDP

☐ Telnet

☐ VNC

Secure Shell, or SSH, is a command-line interface that allows you to connect to a remote computer in a secure manner. It's a secure alternative to insecure methods like Telnet. Through encryption, SSH enables safe communication and preserves the integrity of data.

Telnet is similar to SSH in that it is a command line tool for remote administration but does not have any security and sends information in plain text.

Remote Desktop Protocol (RDP) is a built-in graphical remote management tool in Windows 10. Using the Remote Desktop Protocol, you can connect to another computer's desktop. This allows you to work on the device remotely like you were sitting in front of it.

Virtual Network Computing (VNC) is another type of Remote Desktop Connection. The fundamental difference between VNC and RDP is that the local user will not see what the remote user is doing when an RDP session is initiated.

Module 19 Network Security and Troubleshooting

As an IT technician, you arrive at a customer's home office to troubleshoot problems they are experiencing with their printer. While questioning the customer to get an understanding of their network, you find they have a new Wi-Fi router that connects wirelessly to a new desktop and two new laptops, in addition to multiple smartphones, tablets, and the network printer. They also have several smart home devices, including security cameras, light switches, door locks, and a thermostat supported by an IoT controller hub. To work on the printer, which type of network will you be interacting with?

- ☐ a. PAN
- ☒ b. LAN
- ☐ c. WAN
- ☐ d. WMN

Your customer then asks you if it would be worth the investment for them to have Ethernet cabling installed to reach each of their workstations instead of connecting them by Wi-Fi to the network. Specifically, they want to know if that would speed up communications for the workstations. You examine their router and find that it's using 802.11ac Wi-Fi. Would you advise them to upgrade to Ethernet? Why or why not?

- ☐ a. Yes, because Ethernet is faster than 802.11ac.
- ☐ b. Yes, because wired connections are always faster than wireless connections.
- ☐ c. No, because installing Ethernet cabling is more expensive than the increased speed is worth.
- ☒ d. No, because 802.11ac speeds are faster than Ethernet.

You run the `ipconfig` command on your computer, and it reports an IP address of 169.254.75.10 on the Ethernet interface. Which device assigned this IP address to the interface?

- ☐ a. The cable modem
- ☐ b. The ISP's DNS server
- ☐ c. The local network's DHCP server on the SOHO router
- ☒ d. The local computer

You've just received a call from human resources asking for assistance with a problem. One of your company's employees, Ahmed, has recently undergone extensive surgery and will be homebound for three to five months. He plans on working from home and needs a solution to enable frequent and extended access to the company network's resources. Which WAN technology will you need to configure for Ahmed, and which tool will you use to configure it?

- ☐ a. WWAN using the Network Connections window
- ☒ b. VPN using the Network and Sharing Center
- ☐ c. Wi-Fi using the Network and Sharing Center
- ☐ d. Ethernet using the Network Connections window

You need a VPN to connect to a private, remote network in order to access some files. You click the network icon in your taskbar to establish the connection, and you realize there is no VPN option available on the menu. What tool do you need to use to fix this problem?

- ☐ a. net command

- ☐ b. Network and Sharing Center
- ☐ c. Network Connections window
- ☐ d. netstat command

To prepare to remotely work on a Linux server at work while you are at home, you install VNC Server for Linux by RealVNC (realvnc.com) on the system at work. When you get home, you install the VNC Viewer for Windows on your Windows 10 laptop. When you try to make the connection, you get an error about a refused connection. Which could be a cause of the error?

- ☐ a. VNC Server for Linux must be configured to tunnel through SSH. Set up the SSH tunnel next time you're in the office.
- ☐ b. Port 5901 is not set for port forwarding on the corporate router. Configure the router next time you're in the office.
- ☐ c. VNC Viewer for Windows will not work with a Linux server. Use Remote Desktop instead.
- ☐ d. A VNC solution will not work with Linux. Configure Remote Desktop on the Linux server, and use it with the Remote Desktop client on your home computer.

You're troubleshooting a network connection for a client at their home office. After pinging the network's default gateway, you discover that the cable connecting the desktop to the router had been damaged by foot traffic and is no longer providing a reliable signal. You replace the cable, this time running the cable along the wall, so it won't be stepped on. What do you do next?

- ☐ a. Use the hostname command.
- ☐ b. Apply port forwarding on the router.
- ☐ c. Use the ping command.
- ☐ d. Reboot the router.

Which type of server can function as a firewall?

- ☐ a. Print server
- ☐ b. Proxy server
- ☐ c. Mail server
- ☐ d. FTP server

Your company has recently been hired to install a smart security system for a large office building. The system will include security cameras, voice-controlled lights, smart locks, and smart thermostats. Some of the security cameras will be installed outdoors throughout the parking lot. Which wireless IoT protocol should your company use for the installation?

- ☐ a. Zigbee, because it is always encrypted
- ☐ b. Z-Wave, because it is the fastest wireless standard
- ☐ c. Wi-Fi, because it is always encrypted
- ☐ d. Bluetooth, because it is easiest to configure

As a bank employee, you often work from home and remotely access a file server on the bank's network to correct errors in financial data. Which of the following services is most likely the one you are using to authenticate to the network and track what you do on the network?

- ☐ a. Secure DNS
- ☐ b. Active Directory

- ☐ c. TACACS+
- ☐ d. RADIUS

Mia works from home occasionally and needs to set up her Windows 10 computer at work so she can remote in from her home office. Which tools should she use?

- ☐ a. Zoom
- ☐ b. Remote Desktop
- ☐ c. Remote Assistance
- ☐ d. Secure Shell

Daunte frequently calls your help desk asking for instructions on how to use Windows 10. What is the best way to help Daunte?

- ☐ a. Use Remote Assistance to show Daunte how to use Windows 10, and point him to the log file created.
- ☐ b. Email Daunte some links to online video tutorials about Windows 10.
- ☐ c. Explain to Daunte that a help desk is not the place to go to learn to use new software and that he needs to look elsewhere for help.
- ☐ d. Open a chat session with Daunte over Facebook and talk with him about Windows 10.

Remote Desktop and Remote Assistance require a technician to change port settings and firewall settings, but third-party apps such as GoToMyPC do not. Why is this?

- ☐ a. Microsoft makes its apps more secure than third-party apps.
- ☐ b. GoToMyPC and other third-party apps use ports already left open for web browsing and don't require additional incoming connections.
- ☐ c. GoToMyPC and other third-party apps are not concerned about security because they depend on Windows to secure a network connection.
- ☐ d. Remote Desktop and Remote Assistance allow incoming connections at the same port 80 that is already left open for web browsing.

The documentation for your router says that it can provide content filtering to filter out keywords except for pages that use the HTTPS protocol. Why is that?

- ☐ a. The router must use its public key to transmit HTTPS pages.
- ☐ b. Privacy laws make it illegal to filter content in HTTPS pages.
- ☐ c. HTTPS pages are encrypted, and the router cannot decrypt them to read the content.
- ☐ d. The software to filter content in HTTPS pages is not installed on this particular router.

Your manager asks you to transmit a small file that includes sensitive personnel data to a Linux server on the network. The server is running a Telnet server and an SSH server. Why is it not a good idea to use Telnet to reach the remote computer?

- ☐ a. Telnet transmissions are not encrypted.
- ☐ b. Telnet is not reliable, and the file might arrive corrupted.

- ☐ c. SSH is faster than Telnet.
- ☐ d. SSH running on the same computer as Telnet causes Telnet not to work.

Your SOHO router has failed, and you have installed a new router. The old router's static IP address on the network is 192.168.0.1. The new router has a static IP address of 10.0.0.1. You go to a computer to configure the new router, and you enter 10.0.0.1 in the browser address box. The router does not respond. You open a command prompt window and try to ping the router, which does not work. Next, you verify that the router has connectivity, and you see that its local connection light is blinking, indicating connectivity. What is the most likely problem and its best solution?

- ☐ a. The computer you are using to configure the router has a corrupted TCP/IP configuration. Restart the computer.
- ☐ b. The router is defective. Return it for a full refund.
- ☐ c. The computer and the router are not in the same subnet. Change the subnet mask assigned to the computer.
- ☐ d. The computer and the router are not in the same subnet. Release and renew the IP address of the computer

Which two of the following hosts on a corporate intranet are on the same subnet?

- ☐ a. 192.168.2.143/8
- ☐ b. 172.54.98.3/16
- ☐ c. 192.168.5.57/8
- ☐ d. 172.54.72.89/16