8-1 Types of Networks and Network Connections

Core 1 Objective

- 2.7

Compare and contrast Internet connection types, network types, and their features.

A computer network is created when two or more computers can communicate with each other. Networks can be categorized by several methods, including the technology used and the size of the network. When networks are categorized by their size, or the physical area they cover, these are the categories used, listed from smallest to largest:

- **PAN.** A **PAN (personal area network)** consists of personal devices such as cell phones and laptop computers communicating at close range. PANs can use wired connections (such as USB or Lightning) or wireless connections (such as Bluetooth or near-field communications).
- **LAN.** A **LAN (local area network)** covers a small local area, such as a home, office, or a small group of buildings. LANs can use wired (most likely Ethernet) or wireless technologies (most likely Wi-Fi). A LAN allows workstations, servers, printers, and other devices to communicate and share resources.
- **SAN.** A **SAN (storage area network)** is a specialized, high-speed network for storing and sharing files. These storage locations can be accessed by network clients, as if they were directly connected to the local client machine.
- **WLAN.** A **WLAN (wireless local area network)** is a wireless-capable network that covers a small local area, just like a LAN.
- **MAN.** A **MAN (metropolitan area network)** covers multiple buildings in a large campus or a portion of a city, such as a downtown area. It's usually the result of a cooperative effort to improve service to its users. Network technologies used can be wireless (most likely LTE) and/or wired (for example, Ethernet with fiber-optic cabling).
- **WAN.** A **WAN (wide area network)** covers a large geographical area and is made up of many smaller networks. The best-known WAN is the Internet, or the World Wide Web. Some technologies that connect a single computer or LAN to the Internet include DSL, cable Internet, satellite, cellular WAN, and fiber optic.

Exam Tip

The A+ Core 1 exam expects you to be able to compare PAN, LAN, SAN, WLAN, MAN, and WAN networks.

Now let's look at network technologies used for Internet connections.

8-1a Internet Connection Technologies

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.
- 2.3

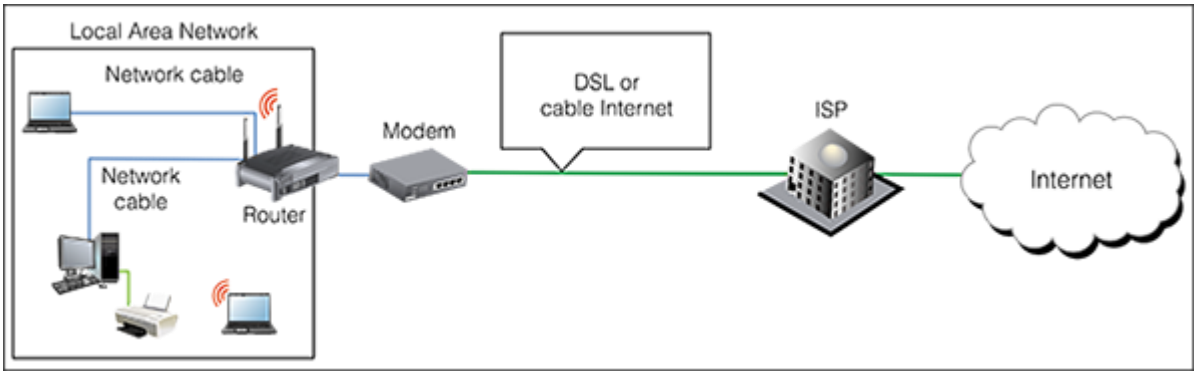
  Compare and contrast protocols for wireless networking.
- 2.7

  Compare and contrast Internet connection types, network types, and their features.

To connect to the Internet, a device or network first connects to an Internet service provider (ISP), such as Verizon or Spectrum. The common types of connections for SOHO networks are DSL and cable Internet. See Figure 8-1. When connecting to an ISP, know that upload speeds are generally slower than download speeds. These rates differ because users typically download more data than they upload. Therefore, an ISP devotes more of the available bandwidth to downloading and less of it to uploading.

Figure 8-1

The ISP stands between a LAN and the Internet



Networks are built using one or more technologies that provide varying degrees of bandwidth. **Bandwidth** is the theoretical maximum number of bits that can be transmitted over a network connection at one time, similar to the number of lanes on a highway. The networking industry refers to bandwidth as a measure of the maximum rate of data transmission in bits per second (bps), thousands of bits per second (Kbps), millions of bits per

second (Mbps), or billions of bits per second (Gbps). Bandwidth is the theoretical or potential speed of a network, whereas data throughput is the average of the actual speed. In practice, network transmissions experience delays, called latency, that result in slower network performance. For example, wired signals traveling across long cables or wireless signals crossing long distances through the air can cause signal strength degradation, resulting in latency. Latency is measured by the round-trip time (RTT) it takes for a message to travel from source to destination and back to source.

Table 8-1 lists network technologies used by local networks to connect to the Internet. The table is more or less ordered from slowest to fastest maximum bandwidth within each category, although latency can affect the actual bandwidth of any network. We explore many of these technologies in more depth throughout this module.

Table 8-1

Networking Technologies

Technology (Wireless or Wired)	Maximum Speed	Description
Wireless Internet Connection: Satellite and WiMAX		
Satellite	Up to 1000 Mbps	Requires an antenna to send to and receive from a satellite, which is in a rel position above the Earth.
WiMAX	Up to 1 Gbps	Requires a transmitter to send to and receive from a WiMAX tower up to 30 WiMAX was once popular in rural areas for wireless Internet connections, bu market space to cellular solutions such as LTE.
Wireless Internet Connection: Cellular		
3G cellular (third-generation cellular)	At least 200 Kbps, but can be up to 21 Mbps	Improved over earlier technologies and allows for transmitting data and vide CDMA or GSM mobile phone services. Speeds vary widely according to the re standards used.
4G cellular (fourth-generation cellular)	100 Mbps to 1 Gbps	Higher speeds are achieved when the mobile device stays in a fixed position. typically uses LTE (Long Term Evolution) technology.
5G cellular (fifth-generation cellular)	Up to 10 Gbps and beyond	5G services are now widespread across many major metropolitan areas; cov continue to increase as providers implement more coverage antenna.
Wired Internet Connection: Telephone		
Dial-up or regular telephone (POTS, for plain old telephone service)	Up to 56 Kbps	Slow access to an ISP using a modem and dial-up connection over phone lin

Technology (Wireless or Wired)	Maximum Speed	Description
SDSL (symmetric digital subscriber line)	Up to 22 Mbps	Equal bandwidth in both directions. SDSL is a type of broadband technology. (**Broadband** refers to a networking technology that carries more than one t on the same cabling infrastructure, such as DSL and telephone or cable Inter DSL uses regular phone lines and is an always-up or always-on connection th require a dial-up.
ADSL (Asymmetric DSL)	640 Kbps upstream and up to 24 Mbps downstream	Most bandwidth is allocated for data coming from the ISP to the user. ISP cu according to a bandwidth scale.
VDSL (very-high-bit-rate DSL)	Up to 70 Mbps	A type of asymmetric DSL that works only over a short distance.
Other Wired Internet Connections		
Cable Internet	Up to 160 Mbps, depending on the type of cable	Connects a home or small business to an ISP, usually comes with a cable tel subscription, and shares cable TV lines. If available, fiber-optic cable gives hi
Dedicated line using fiber optic	Up to 10 Gbps	Dedicated fiber-optic line from ISP to business or home. Speeds vary widely
Wired Local Network: Ethernet		
Fast Ethernet (100BaseT)	100 Mbps	Used for local networks.
Gigabit Ethernet (1000BaseT)	1000 Mbps or 1 Gbps	Fastest Ethernet standard for small, local networks.
10-Gigabit Ethernet (10GBaseT)	10 Gbps	Typically requires fiber media, is mostly used on the backbone of larger ente networks, and can also be used on WAN connections.
Wireless Local Network: Wi-Fi IEEE 802.11		
802.11a	Up to 54 Mbps	No longer used. Uses 5 GHz frequency.
802.11b	Up to 11 Mbps	Experiences interference from cordless phones and microwaves. Uses 2.4 GH
802.11g	Up to 54 Mbps	Compatible with and has replaced 802.11b. Uses 2.4 GHz frequency.
802.11n (Wi-Fi 4)	Up to 600 Mbps	Uses multiple input/multiple output (MIMO), which means an access point ca four antennas to improve performance. Uses both 2.4 and 5 GHz frequencies
802.11ac (Wi-Fi 5)	Theoretically up to 7 Gbps, but currently limited to 1.3 Gbps	Supports up to eight antennas and supports **beamforming**, which detects t connected devices and increases signal strength in those directions. Uses 5 G only.
802.11ax (Wi-Fi 6)	10 Gbps	This throughput is possible when using the 160 MHz channel spacing and the streams. Uses both 2.4 and 5 GHz frequencies.

Technology (Wireless or Wired)	Maximum Speed	Description
Bluetooth	Up to 25 Mbps for version 4.0	Originally defined under IEEE 802.15, but now maintained by the Bluetooth S Group (SIG).

Cable Internet and DSL are two options to make an Internet connection for a home network. Let's first quickly compare these two technologies and then look at fiber-optic dedicated lines, satellite, cellular WAN, wireless Internet service providers, and long-range fixed wireless connections that may be found in commercial applications.

Exam Tip

The A+ Core 1 exam expects you to be able to compare these network types used for Internet connections: cable, DSL, dial-up, fiber, satellite, ISDN, and cellular (tethering and mobile hotspot).

Cable Internet

Cable Internet is a broadband technology that uses cable TV lines and is always connected (always up). With cable Internet, the TV signal to your television and the data signals to your computer or LAN share the same **coaxial (coax) cable**, an older cable form that is still used today in local area networks. The cable modem converts the computer's digital signals to analog when sending them and converts incoming analog data to digital.

DSL Broadband

DSL (digital subscriber line) is a group of broadband technologies that covers a wide range of speeds. DSL uses ordinary copper phone lines and a range of frequencies on the copper wire that are not used by voice, making it possible for you to use the same phone line for voice and DSL at the same time. When you make a regular phone call, you dial in as usual. However, the DSL part of the line is always connected (always up) for most DSL services.

With DSL, static over phone lines in your house can be a problem. The DSL company normally provides filters to install at each phone jack (see Figure 8-2), but the problem still might not be fully solved. Figure 8-3 shows a **DSL modem** that can connect directly to a computer or to a router on your network.

Figure 8-2

When DSL is used in your home, filters are needed on every phone jack except the one used by the DSL modem

Figure 8-3

This DSL modem connects to a phone jack and a computer or router to provide broadband connection to an ISP

Both cable and DSL connections typically require a modem device at the entry to your SOHO network. Although you might be able to find the modem's default login instructions online, you'll likely never have to change

any settings on the modem itself. Configuring a DSL or cable modem consists of plugging the correct cables into the correct ports. For example, Figure 8-4 shows a cable modem with the ISP coax cable connected on the right. The yellow Ethernet cable connects to the local network, and a phone line is plugged into the Voice-over-IP (VoIP) phone service provided by the ISP over the Internet. Also notice the Reset button in the figure, which you can use to reset a modem to its factory default settings. When troubleshooting a modem, try rebooting it first, and only use the reset as a last resort.

Figure 8-4

Use a cable modem to connect the ISP's coaxial cable to the LAN's Ethernet cable

Dedicated Line Using Fiber Optic

Another broadband technology used for Internet access is **fiber optic**. This technology connects a dedicated line from your ISP to your place of business or residence. This dedicated line is called a point-to-point (PTP) connection because no other business or residence shares the line with you. Television, Internet data, and voice communication all share the broadband **fiber-optic cable**, which reaches all the way from the ISP to your home. This line then connects to an **optical network terminal (ONT)**. The ONT serves as a modem for the fiber connection (see Figure 8-5). Alternatively, the provider might install fiber-optic cabling up to your neighborhood and then run coaxial cable (like that used in cable Internet connections) for the last leg of the connection to your business or residence. Upstream and downstream speeds and prices vary.

Figure 8-5

AN ONT connects the ISP's fiber cable on the left and coverts it to a data-connection cable that is connected into your home

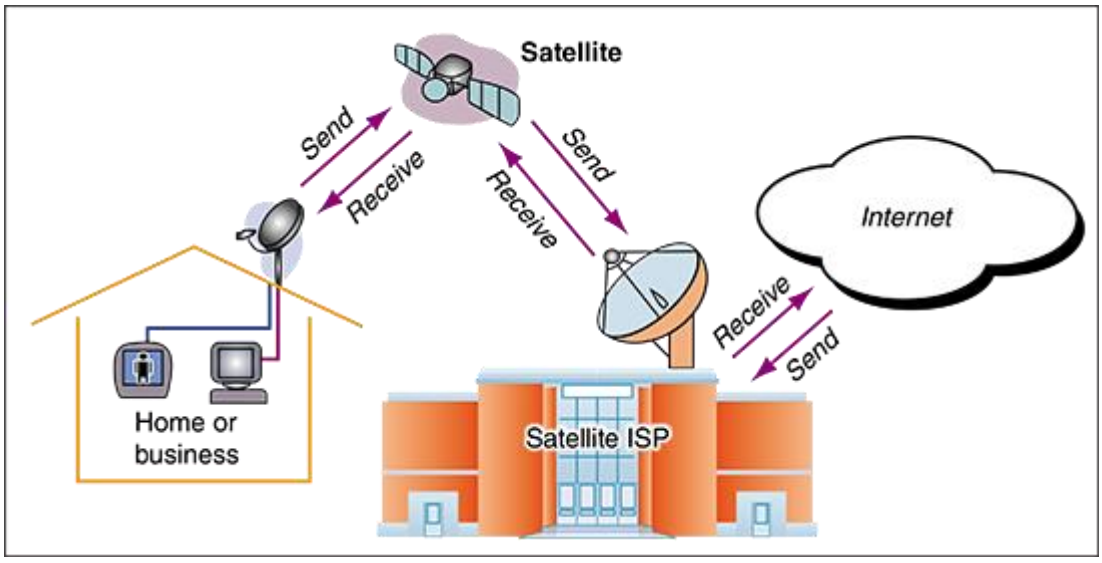
Wikimedia Commons

Satellite

People who live in remote areas and want high-speed Internet connections often have limited choices. DSL and cable options might not be available where they live, but satellite access is available from pretty much anywhere. Internet access by **satellite** is available even on airplanes. Passengers can connect to the Internet using a wireless hotspot and satellite dish on the plane. A satellite dish mounted on top of your house or office building communicates with a satellite used by an ISP offering the satellite service (see Figure 8-6). One disadvantage of satellite is that it requires line-of-sight wireless connectivity without obstruction from mountains, trees, and tall buildings. Another disadvantage is that it experiences higher delays in transmission (latency), especially when uploading, and is therefore not a good solution for an Internet connection that will be used for videoconferencing or voice over Internet.

Figure 8-6

Communications by satellite can include television and Internet access

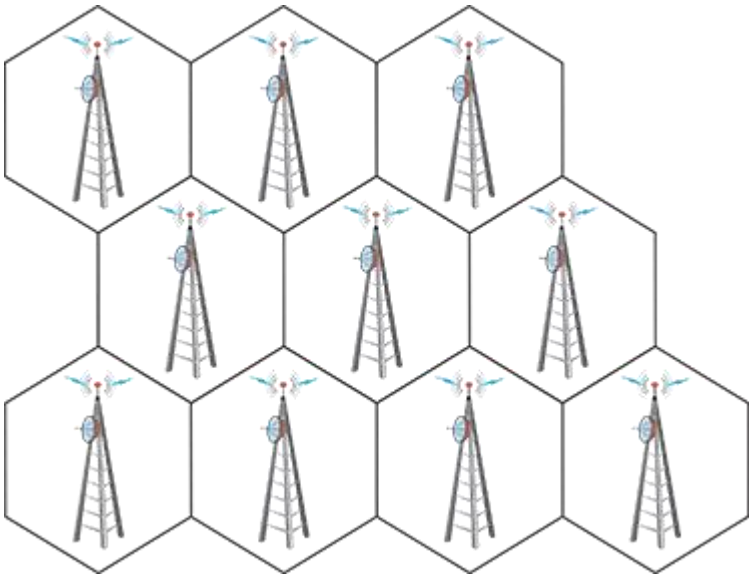


Cellular WAN

A cellular network, also called a cellular WAN because it consists of cells, is provided by companies such as Verizon and AT&T. Each cell is controlled by a base station (see Figure 8-7), which might include more than one transceiver and antenna on the same tower to support various technologies for both voice and data transmission.

Figure 8-7

A cellular network is made up of many cells that provide coverage over a wide area



Cellular devices require a **SIM (subscriber identity module) card** to be installed in the device; the card contains the information that identifies your device to the carrier (see Figure 8-8).

Figure 8-8

A SIM card contains information about the cellular networks it is authorized to connect to

Most smartphones are linked by the manufacturer to a specific cellular provider and will need to be validated on that provider's network to connect to it. To connect a computer using mobile broadband to a cellular network, you need the hardware and software to connect and, for most networks, a SIM card. The bulleted list that follows includes the options for software and hardware devices that can connect to a cellular network and general steps for how to create each connection. Keep in mind that when you purchase any of these devices from a carrier or manufacturer, detailed instructions are most likely included for connecting to the cellular network.

- **Embedded mobile broadband modem.** A laptop or other mobile device might have an embedded broadband modem. In this situation, you still need to subscribe to a carrier. If a SIM card is required, insert the card in the device. For some laptops, the card slot might be in the battery bay, and you must remove the battery to find the slot. Then use a setting or application installed on the device to connect to the cellular network.
- **Cell phone tethering.** You can tether your computer or another device to your cell phone. The cell phone connects to the cellular network and provides communication to the tethered device. To use your phone for tethering, your carrier contract must allow it. The phone and other device can connect by way of a USB cable (see Figure 8-9), a proprietary cable provided by your cell phone manufacturer, or a Bluetooth or Wi-Fi wireless connection. Your carrier is likely to

provide you software to make the connection, or the setting might be embedded in the phone's OS.

Figure 8-9

Tethering a laptop to a cell phone using a USB cable

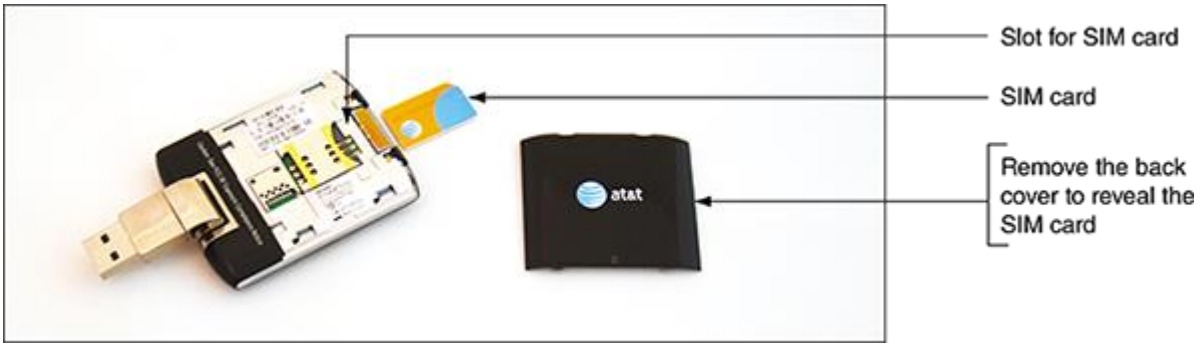
- **USB broadband modem.** For any computer, you can use a USB broadband modem (sometimes called an air card), such as the one shown in Figure 8-10. The device requires a contract with a cellular carrier. If needed when using a USB broadband modem, insert the SIM card in the modem (see Figure 8-11). When you insert the modem into a USB port, Windows finds the device, and the software stored on the device automatically installs and runs. A window provided by the software then appears and allows you to connect to the cellular network.

Figure 8-10

A USB broadband modem by Sierra Wireless

Figure 8-11

A SIM card with subscription information on it may be required to use a cellular network for data



- **LTE home Internet.** Some cellular companies offer home Internet service through their cellular WAN infrastructure. Verizon calls its service LTE Home Internet, and AT&T calls its service FWI (Fixed Wireless Internet). The ISP installs an LTE router at the home, possibly with an external antenna, which then connects wirelessly to the ISP's cellular network. The router provides a Wi-Fi hotspot as well as a few Ethernet ports for wired devices. Typically, the router can't be moved to other locations like a smartphone can—it's designed to be used only at the location where the subscription is established. Data usage caps also may apply.

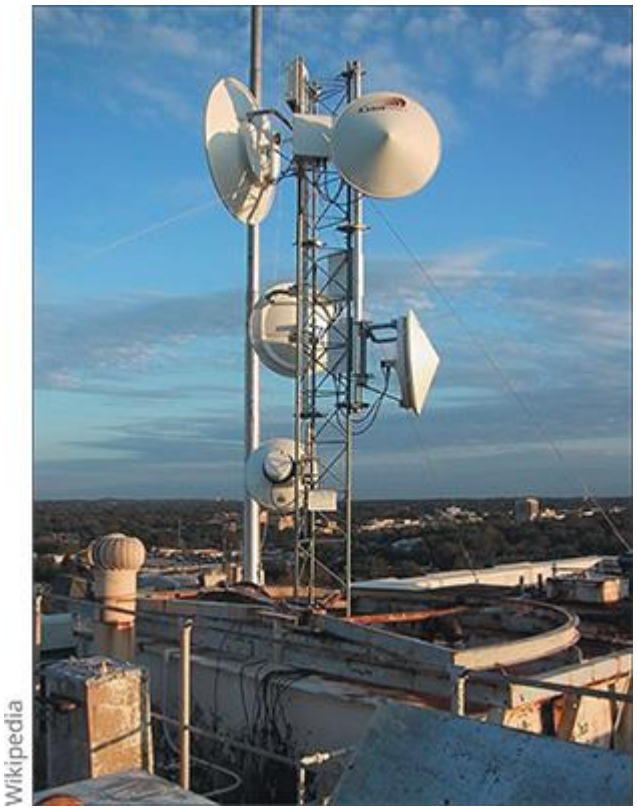
- **Mobile hotspot.** Some mobile devices can create a **mobile hotspot**, which allows computers and other mobile devices to connect by Wi-Fi to the device and, through that connection, to the Internet. Some cellular ISPs, such as AT&T, also offer devices dedicated to this purpose.

Wireless Internet Service Providers

A **wireless Internet service provider (WISP)** provides wireless network coverage to a certain location using wireless broadband. These providers used to be found only in rural areas where conventional networking technologies such as cable or DSL were not available. Now, however, they can be found in metropolitan areas as well. Consisting of wireless transmitters and customer premise antennae, as shown in Figure 8-12, these networks can expand Internet coverage across the globe. Another example of a WISP was seen in the WiFi101 network project that ran from 2008 to 2015 in East Palo Alto, California. As part of that project, Google provided completely free wireless coverage to the entire community.

Figure 8-12

WISP access point in Tyler, Texas



Wikipedia

Long-Range Fixed Wireless

Long-range fixed wireless (LRFW) networks are used to provide low-cost, point-to-point connections. These networks are typically unregulated and

provide an alternative to either cellular or satellite Internet access. These systems use highly directional antennas, which transmit at high power, to transmit the wireless signal across large distances, sometimes more than 100 miles. A LRFW antenna is shown in Figure 8-13.

Figure 8-13

Long-range fixed wireless antennas are mounted on rooftops to ensure clear line of sight

Wikimedia Commons

Currently, LRFW networks outside the United States use **unlicensed frequencies** within the 2.4 and 5 GHz spectrum—like your SOHO Wi-Fi—but require direct line of sight with the antenna. Unlicensed means the frequency has not been assigned for this use and is not regulated by any governing body.

In August 2011, the FCC began making room for **licensed frequencies** for these systems to operate and also began regulating regulate their use within the United States. By licensing the 7 and 13 GHz frequencies for point-to-point connections and setting limits for how much power these networks can transmit with, the FCC is setting the regulatory requirements to operate these networks, to include the maximum power and frequencies. These parameters are also intended to ensure that these networks do not interfere with other communication networks.

Now that you understand some basics about the different types of networks and methods of connecting those networks to the Internet, you're ready to learn about different devices used to connect computers to local networks.

8-2 Identifying Network Hardware and Infrastructure

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.
- 2.3

  Compare and contrast protocols for wireless networking.
- 2.4

  Summarize services provided by networked hosts.
- 2.6

  Compare and contrast common network configuration concepts.
- 3.1

  Explain basic cable types and their connectors, features, and purposes.

In this section of the module, you learn about the hardware devices that create and connect to networks. We discuss desktop and laptop devices, switches, bridges, and other network devices, along with the cables and connectors these devices use.

8-2a Switches and Virtual LANs

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.
- 2.6

  Compare and contrast common network configuration concepts.

Recall that a switch is a device that connects other devices on a network. Two types of switches are managed and unmanaged switches.
An **unmanaged switch** requires no setup or configuration other than connecting network cables to its ports. It does not require an IP address and is appropriate for SOHO networks. A **managed switch,** seen in Figure 8-14, has firmware that can be configured to monitor and manage network traffic. It's appropriate for larger networks and can be used to manage QoS for prioritizing network traffic and to control speeds for specific ports. The firmware on a managed switch is accessed through a browser using the

switch's IP address, which is similar to how you access the firmware on a router. A switch requires an IP address only for the purpose of accessing its firmware to configure the switch.

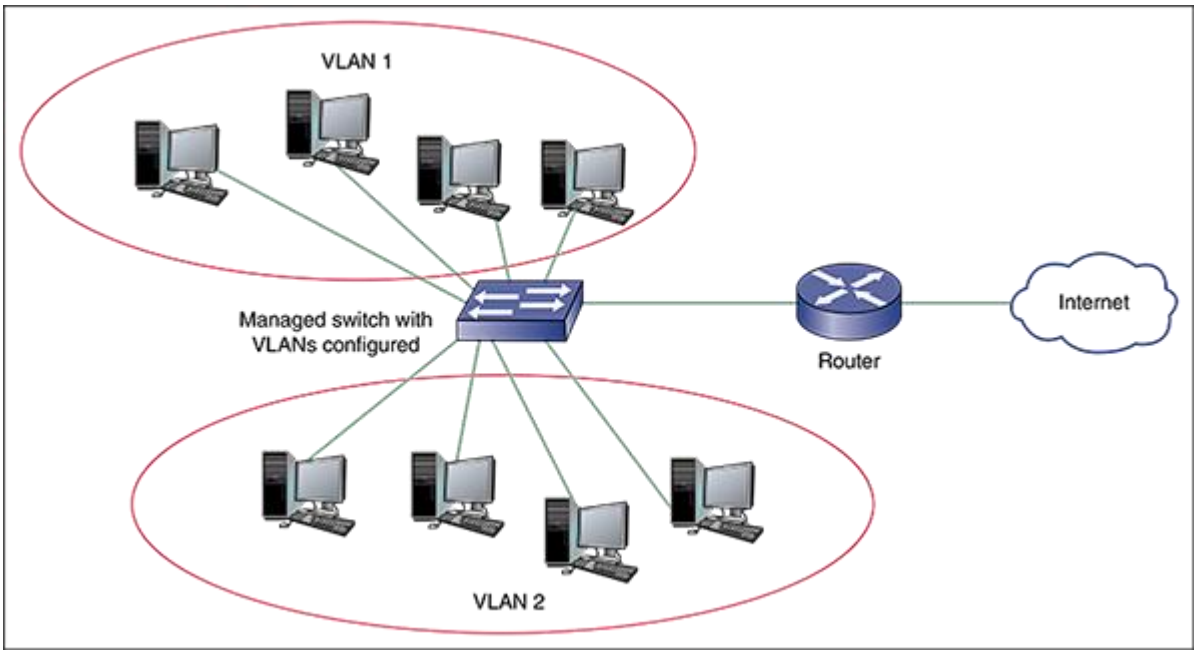
Figure 8-14

The Gigabit Ethernet switch has eight ports for device connections

You can also use a managed switch to break up a large LAN into smaller networks called **virtual LANs (VLANs)**, which can reduce network traffic. VLANs are created by assigning a group of physical ports on the switch to a different VLAN. In Figure 8-15, the one physical LAN is broken up into two virtual LANs. With network segmentation, broadcast traffic is reduced because it is limited to each VLAN.

Figure 8-15

Ports on a managed switch can be assigned to a VLAN to logically break up a network



You can also break up a large network by subnetting, which involves using a DHCP server and assigning different IP address ranges and subnet masks to each smaller network. Subnetting also helps reduce broadcast traffic on the network and can optimize the network for faster service.

Here are reasons you might add switches to your network:

- **To add network connections.** A SOHO router usually has four to eight ports in a built-in switch. When you need more connections, add a switch in a location where you have multiple workstations or printers that need to connect to the network. In practice, a small network might begin as one switch and three or four computers. As the need for more computers grows, new switches are added to provide these extra connections.
- **To regenerate the network signal.** An Ethernet cable should not exceed 100 meters (about 328 feet) in length. If you need to reach distances greater than that, you can add a switch in the line, which regenerates the signal. An alternative to using a switch for this purpose would be to simply use a **repeater** device that amplifies the signal onto the new extended cable run.
- **To manage network traffic.** Managed switches can be installed in strategic places on the network to subnet the network and manage network traffic to improve performance.

8-2b Wireless Access Points

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.

- 2.3

  Compare and contrast protocols for wireless networking.

You've already learned that a SOHO router can also be a wireless access point. In addition, a wireless access point can be a dedicated device. The wireless access point can also serve as a bridge, as shown in Figure 8-16. A **bridge** is a device that stands between two segments of a network and manages network traffic between them. For example, one network segment might be a wireless network and the other segment might be a wired network; the wireless access point (WAP) connects these two segments. Another use of a bridge can be found when a server is placed between two networks, as in the case of a proxy server. The server would have two network interface cards to connect to each network segment.

Figure 8-16

A wireless access point by TP-Link

Exam Tip

The A+ Core 1 exam expects you to know the functions and features of a switch, router, access point, repeater, firewall, and modem.

8-2c Ethernet Cables and Connectors

Core 1 Objective

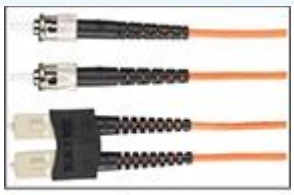
- 3.1

  Explain basic cable types and their connectors, features, and purposes.

Several variations of Ethernet cables and connectors have evolved over the years. They are primarily identified by their speeds and the types of connectors used to wire the networks. Table 8-2 compares cable types and Ethernet versions.

Table 8-2

Variations of Ethernet and Ethernet Cabling

Cable System	Speed	Cables and Connectors	Example of Connectors	Maximum Cable Length
10BaseT, 100BaseT (Fast Ethernet), 1000BaseT (Gigabit Ethernet), and 10GBaseT (10-Gigabit Ethernet)	10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps	Twisted-pair (UTP or STP) uses an RJ-45 connector.	 Courtesy of Tyco Electronics Courtesy of Tyco Electronics	100 meters or 328 feet
100BaseFL, 100BaseFX, 1000BaseFX, or 1000BaseX (fiber optic)	100 Mbps, 1 Gbps	Fiber-optic cable uses ST, SC, or LC connectors (ST and SC shown to the right)	 Courtesy of Black Box Corporation Courtesy of Black Box Corporation	Up to 2 kilometers (6562 feet)
10GBase ER, 10GBase SR, 10GBase SW, 10GBase SX	10Gbps	Fiber-optic cable using SC or LC connectors (LC shown to the right)		Up to 550 meters

Exam Tip

The A+ Core 1 exam expects you to know the details listed in Table 8-2. Given a scenario, you need to recognize that when a cable exceeds its recommended maximum length, limited connectivity problems can result.

Ethernet Standards and Cables

Ethernet can run at four speeds. Each version of Ethernet can use more than one cabling method. Here is a brief description of the transmission speeds and the cabling methods they use:

- **100 Mbps Ethernet or Fast Ethernet. Fast Ethernet** operates at 100 Mbps and typically uses copper cabling rated CAT-5 or higher. Fast Ethernet networks can support slower speeds of 10 Mbps, used by the original Ethernet standard, so devices that run at either 10 Mbps or 100 Mbps can coexist on the same LAN.
- **1000 Mbps Ethernet or Gigabit Ethernet.** This version of Ethernet operates at 1000 Mbps (1 Gbps) and uses twisted-pair cable and fiber-optic cable. **Gigabit Ethernet** is becoming the most popular choice for LAN technology. Because it can use the same cabling and connectors as Fast Ethernet, a company can upgrade from Fast Ethernet to Gigabit without rewiring the network.

- **10 Gbps Ethernet.** This version of Ethernet operates at 10 billion bits per second (10 Gbps) and typically uses fiber-optic cable. It can be used on LANs, MANs, and WANs and is also a good choice for network backbones. (A network backbone is a channel whereby local networks can connect to wide area networks or to each other.)

Twisted-Pair Cable

As you can see from Table 8-2, the two main types of cabling used by Ethernet are twisted-pair and fiber optic. **Twisted-pair cabling** uses pairs of wires twisted together to reduce crosstalk, which is interference that degrades a signal on the wire. It's the most popular cabling method for local networks and uses an RJ-45 connector. The cable comes in two varieties: **unshielded twisted-pair (UTP) cable** and **shielded twisted-pair (STP) cable**. UTP cable is less expensive than STP and is commonly used on LANs. STP cable uses a covering or shield around each pair of wires inside the cable that protects it from electromagnetic interference caused by electrical motors, transmitters, or high-tension lines. Additional coatings can also shield the cable from the elements outside and allow the cable to be buried in the ground. This is known as **direct burial** cable. STP cable costs more than unshielded cable, so it's used only when the situation demands it. Twisted-pair cable is rated by category (CAT), as listed in Table 8-3. A rating indicates how well a cable can handle alien crosstalk (crosstalk between cables in a bundle) and near-end crosstalk (NEXT), which is crosstalk between pairs of twisted wires within a cable where the wires terminate at the end of the cable.

Table 8-3

Twisted-Pair Categories

Twisted-Pair Category	Cable System	Frequency	Shielded or Unshielded	Comment
CAT-5	10/100 Base T	Up to 100 MHz	Either	Has two wire pairs and is sel
CAT-5e (Enhanced)	10/100 Base T, Gigabit Ethernet	Up to 350 MHz	Either	Has four twisted pairs and a sheath to help reduce crosst
CAT-6	10/100 Base T, Gigabit Ethernet, 10 Gigabit Ethernet at shorter distances	Up to 250 MHz	Either	Less alien crosstalk because core that keeps the twisted p
CAT-6A	10 G Base T	Up to 500 MHz	Either	Higher standards to reduce a end crosstalk

Note 1

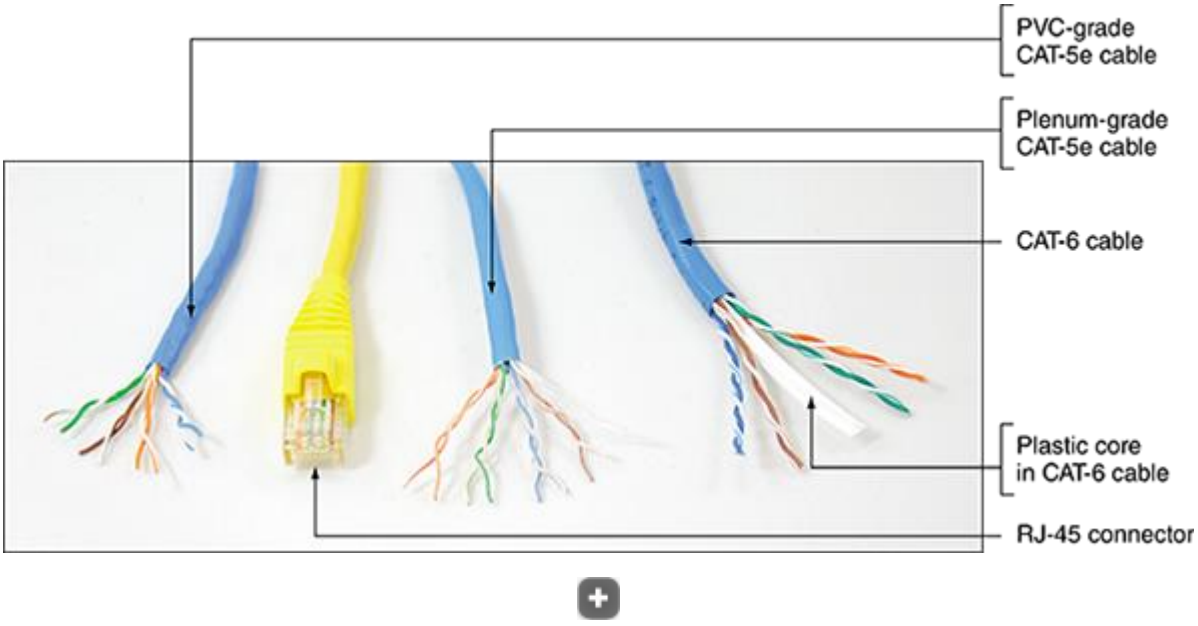
At the time of this writing, CAT-7 and CAT-8 cables are starting to be used; however, the specifications have not been fully approved by the TIA/EIA. These cables offer increased speeds at higher frequencies. CAT-7 is rated up to 10 Gbps at 600 or 1000 MHz, and CAT-8 is

rated up to 40 Gbps at 2 GHz. It should be noted that these cables are not for generic wiring within a building and will only be used in data centers for short runs between equipment such as switches and routers.

Figure 8-17 shows unshielded twisted-pair cables. Twisted-pair cable has four pairs of twisted wires for a total of eight wires. You learn more about how the eight wires are arranged later in this module.

Figure 8-17

Unshielded twisted-pair cables showing the twisted pairs. One cable has the RJ-45 connector attached. Note the core isolator in the CAT-6 cable.



Note 2

Normally, the plastic covering of a cable is made of **PVC (polyvinyl chloride)**, which is not safe when used inside the **plenum** (airspaces between the floors of buildings). In these situations, plenum cable covered with Teflon is used because it does not give off toxic fumes when burned. Plenum cable is two or three times more expensive than PVC cable. Because they can look essentially the same, check for labels printed on the cable to determine whether it's PVC or plenum rated.

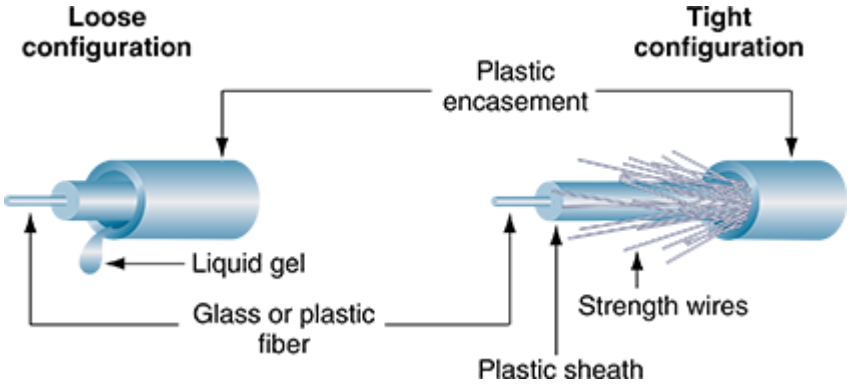
Fiber Optic

Fiber-optic cables transmit signals as pulses of light over glass or plastic strands inside protective tubing, as illustrated in Figure 8-18. Fiber-optic cable comes in two types: single-mode (thin, difficult to connect, expensive, and best performing) and multimode (most popular). A single-mode cable uses a single path for light to travel through it and multimode cable uses multiple paths for light. Both single-mode and multimode fiber-optic cables can be constructed as loose-tube cables for outdoor use or tight-buffered cables for indoor or outdoor use. Loose-tube cables are filled with gel to

prevent water from soaking into the cable, and tight-buffered cables are filled with synthetic or glass yarn, called strength wires, to protect the fiber-optic strands, as shown in Figure 8-18.

Figure 8-18

Fiber-optic cables contain a glass or plastic core for transmitting light



Fiber optic cables use a variety of connectors but the most common ones in networking are the **ST (straight tip) connector** shown in Figure 8-19, **LC (Lucent connector)** shown in Figure 8-20, and the **SC (subscriber connector)** shown in Figure 8-21. Depending on the hardware, the choice of connector should match the port you are connecting the cable to.

Figure 8-19

An ST (straight tip) fiber connector

Figure 8-20

An LC (Lucent connector) fiber connector has a locking clip that locks the cable into the port, similar to an RJ-45 connector

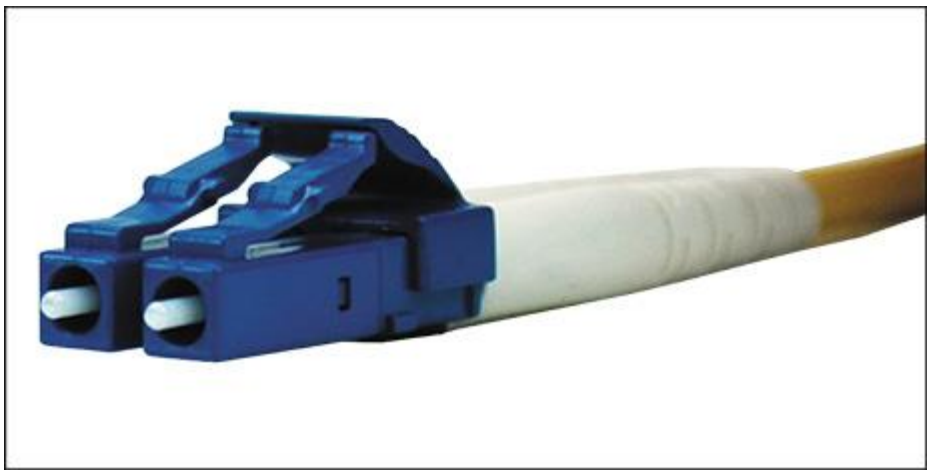


Figure 8-21

An SC (subscriber connector) fiber connector

Exam Tip

The A+ Core 1 exam expects you to know about the following cables and connectors: copper cables (coaxial cable with an F-type connector, CAT-5, CAT-5e, CAT-6, CAT-6a, and Ethernet STP and UTP cables with the RJ-45 connector), fiber-optic cable with ST, SC, and LC connectors, plenum cables, and the RJ-11 connector.

Coaxial

Coaxial cable, or coax, is a single conductor cable used to carry high-frequency electrical signals to customers. These cables have been around for many years and have been used for cable television, telephone, and Internet services. Coaxial cable was used for early implementations of Ethernet, but it is no longer used for that purpose. Today, the most common uses are for cable modem connections between a customer and Internet service provider. Common connectors using coaxial cable are the **BNC** and **F-Type**. BNC is normally found in industrial environments. Both are shown in Figure 8-22.

Figure 8-22

Coaxial cable normally uses the BNC (left) or the F-type connector (right)

Coaxial cable is categorized by its inner conductor diameter and outer jacket dimensions. RG-6 has widely replaced older RG-59 cables to support television and cable Internet connections.

8-2d Power over Ethernet (PoE)

Core 1 Objective

- 2.2

Compare and contrast common networking hardware.

Power over Ethernet (PoE) is a feature that might be available on high-end **PoE-rated switches** to allow power to be transmitted over Ethernet cable. There are two current PoE standards: **PoE** is specified in IEEE 802.3af, and **Power over Ethernet plus (PoE+)** is under 802.3at. The main difference is the power levels provided. PoE has a maximum of 15.4 watts, and PoE+ sends up to 25.5 watts through CAT-5 cabling to the device. Using this feature, you can place a wireless access point, webcam, IP phone, or other device that needs power in a position in a building where you don't have an electrical outlet. The Ethernet cable to the device provides both power and data transmissions. If your switch doesn't offer PoE, you can attach a **PoE injector** (see Figure 8-23), which adds power to an Ethernet cable.

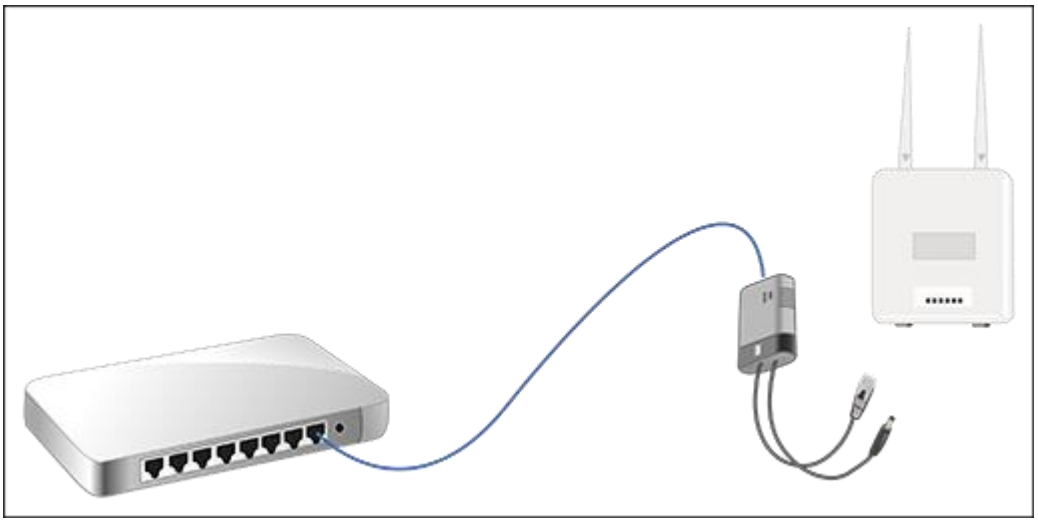
Figure 8-23

A PoE injector introduces power onto the Ethernet cable

Some devices, such as a webcam, are designed to receive both power and data from the Ethernet cable. For other devices, you must use a splitter that splits the data and power transmissions before connecting to the non-PoE device. Figure 8-24 shows a PoE switch, as well as a splitter used to provide power to a non-PoE access point. When setting up a device to receive power by PoE, make sure the device sending the power, the splitter, and the device receiving the power are all compatible. Pay special attention to the voltage and wattage requirements and the type of power connector of the receiving device.

Figure 8-24

Use a PoE splitter if the receiving device is not PoE compatible



8-2e Internet of Things (IoT)

Core 1 Objective

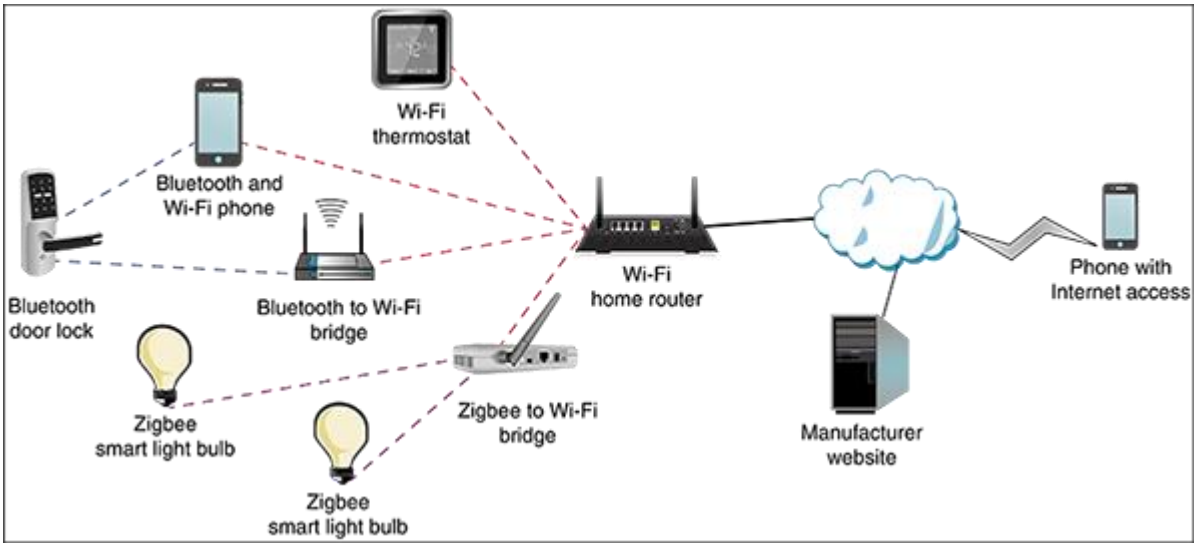
- 2.4

Summarize services provided by networked hosts.

The **Internet of Things (IoT)** is a term that is used to describe physical devices that are connected directly to a network and communicate directly to the Internet. Examples of IoT devices include cameras, doorbells, baby monitors, health and fitness wearable technology, and even refrigerators and other appliances. A smart home network using a variety of devices and wireless technologies (such as Bluetooth, Wi-Fi, and Zigbee) might look something like the one shown in Figure 8-25. These devices are all directly or indirectly connected to the Internet and allow for remote monitoring of your home or appliances from anywhere in the world.

Figure 8-25

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



IoT devices are normally centered around increasing quality of life and convenience; however, they do bring questions of privacy and security because they can be accessed remotely. Imagine someone being able to connect to your cameras or baby monitor from across the globe and spy on you. If you decide these devices should be a part of your smart home, be sure to implement IoT security features that you learn about in the module "Network Security and Troubleshooting."

8-2f Devices and Software to Enhance Networking

Core 1 Objectives

- 2.4

  Summarize services provided by networked hosts.

- 2.6

  Compare and contrast common network configuration concepts.

The best networks are those that make data, services, and other resources available to employees, customers, and others in the most efficient and reliable way. In this section of the module, we explore infrastructure software and hardware designed to improve network efficiency, reliability, monitoring, and security. Let's begin with looking at software designed to monitor and improve network performance.

Software-Defined Networking

Software-defined networking (SDN) uses software applications and programs to essentially virtualize networking. SDN applications replicate how a switch, router, or other networking hardware functions, all while constantly monitoring the status of each device. An SDN architecture separates the movement of the data (referred to as the data plane) from the hardware device (referred to as the control plane). By separating these two functions, an SDN can make smarter decisions about the path data should take across the network, configuring priorities for certain data or automating connections. This high-level view and the monitoring of the entire network are different from traditional hardware networks because the network can be configured remotely in the SDN application without having to configure individual networking devices.

Note 3

To view a short video about how a SDN works, go to youtube.com/watch?v=XFXdWg1p5to.

SCADA Systems

Supervisory control and data acquisition (SCADA) systems are embedded computer systems designed to monitor and control machinery from a single location. For example, a manufacturing plant can use SCADA to supervise an assembly line, or a nuclear power plant can use SCADA to control power production. SCADA systems can be used in commercial buildings to monitor heating, ventilation, and air conditioning (HVAC) and water supply systems. Because these systems control and operate important

and critical systems, they should be protected from regular network access using a VLAN or dedicated subnet. Remote access to these systems should also be minimized or eliminated if possible. A SCADA system control room is shown in Figure 8-26.

Figure 8-26

A SCADA control station can visually show the systems it monitors for easy visual identification

Wikimedia Commons

Unified Threat Management (UTM) Appliance

Recall that a router stands between the Internet and a private network to route traffic between the two networks. It can also serve as a firewall to protect the network. A next-generation firewall (NGFW) combines basic firewall functions with antivirus/anti-malware functions and perhaps other functions as well. NGFW components might be installed on a dedicated appliance, router, server, or even in the cloud. In addition, an NGFW device can offer comprehensive **unified threat management (UTM)** services. A UTM appliance, also called a security appliance, stands between the Internet and a private network, as does a router, and it protects the network (see Figure 8-27). Figure 8-28 shows a UTM appliance by FortiNet.

Figure 8-27

A UTM appliance is considered a next-generation firewall that can protect a private network

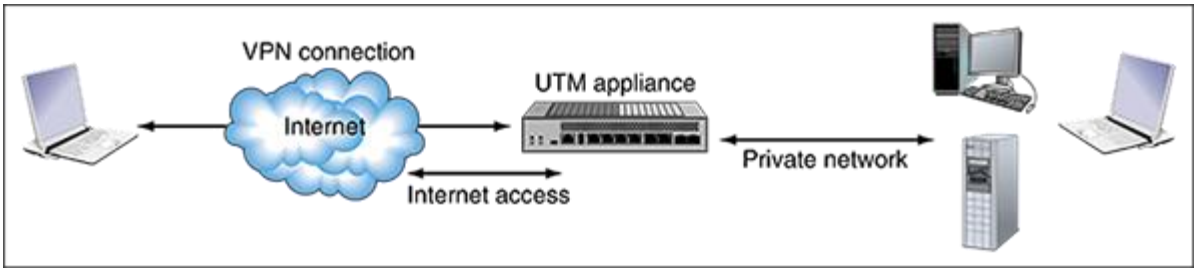
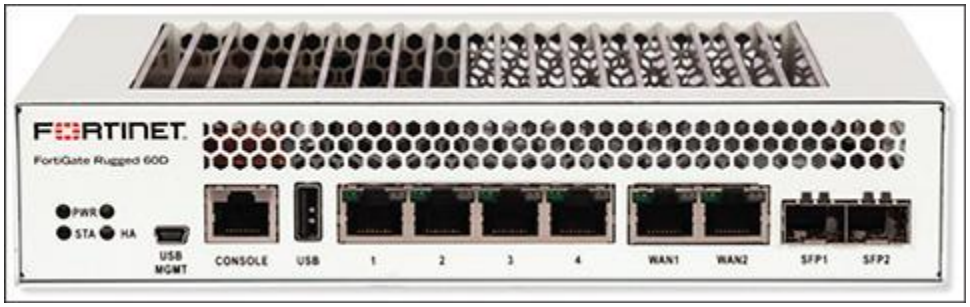


Figure 8-28

A FortiNet FortiGate Rugged 60D UTM appliance



A UTM appliance might offer these types of protections and services:

- **Firewall.** The firewall filters incoming and outgoing network traffic according to IP addresses, ports, the type of messages the traffic contains, and how the message was initiated.
- **Antivirus and anti-malware software.** This software is usually much more advanced than what might be installed on a server or workstation.
- **Spam gateway.** Spam gateways are used to control spam content and emails from entering a network. This helps to reduce the amount of content being sent into the network.
- **Identity-based access control lists.** These lists control access of users or user groups and can log and report activity of these users and groups to reveal misuse, data leaks, or unauthorized access to resources. The company can use this feature to satisfy legal auditing requirements for detecting and controlling data leaks.
- **Intrusion detection system.** An **intrusion detection system (IDS)** monitors all network traffic and creates alerts when suspicious activity happens. IDS software can run on a UTM appliance, router, server, or workstation.
- **Intrusion prevention system.** An **intrusion prevention system (IPS)** not only monitors and logs suspicious activity like the IDS, but it can also prevent the network traffic from entering the network, based on a set of rules programmed into it.

- **Endpoint management server.** An endpoint management server provides monitoring of various endpoint devices on the network, from computers and laptops to mobile devices like smartphones, tablets, or even barcode readers. The service can ensure that endpoints are kept up to date with current anti-malware requirements, operating system patches, and application updates. The system will restrict the device's access to the network until that device meets the security requirements, which gives an additional layer of protection to other network resources.
- **VPN.** The appliance can provide a **virtual private network (VPN)** to remote users of the network, as shown in Figure 8-27. This allows for secure remote access of your private network. You learn how to set up a VPN in the Core 2 module "Networking Security and Troubleshooting."

Exam Tip

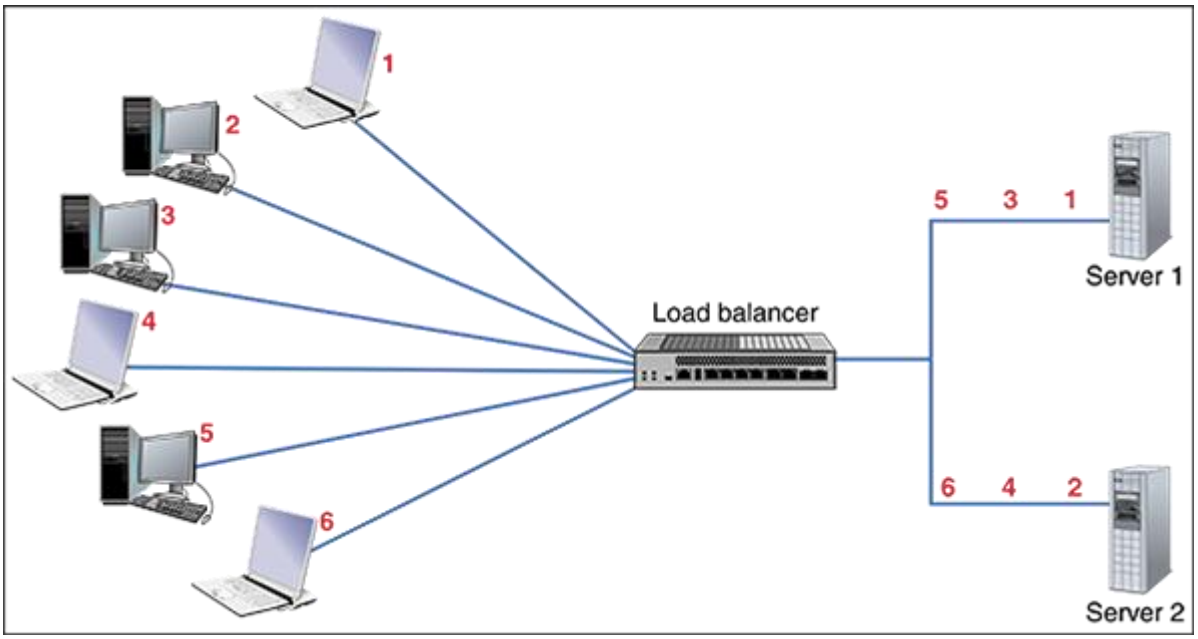
The A+ Core 1 exam expects you to be able to summarize the purposes of services provided by a UTM appliance, including an IDS, IPS, endpoint management server, and VPN provider.

Load Balancer

A **load balancer** helps to ensure high-demand systems and applications are available when a user needs to access them. By spreading the information or connection requests across multiple physical systems, the load balancer ensures that no single system is overloaded. Among other uses, load balancers are sometimes deployed on shopping and social media web servers. As illustrated in Figure 8-29, the devices on the left send requests (marked by the numbers) that are spread across the two servers on the right. This ensures the two servers do not get overloaded. Load balancers, sometimes called elastic load balancers, are used frequently within cloud computing to spread the incoming requests across virtual servers in the cloud. The load balancer can also create new copies of the virtual server as the demand increases or shut down these systems as the demand decreases.

Figure 8-29

A load balancer distributes the incoming request on the left to the servers on the right



8-3 Configuring Network Infrastructure

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.
- 2.3

  Compare and contrast protocols for wireless networking.
- 2.8

  Given a scenario, use networking tools.
- 3.1

  Explain basic cable types and their connectors, features, and purposes.

In the module "Networking Fundamentals," you learned to configure a workstation and SOHO router to create a small network and connect it to a device (for example, a DSL or cable modem) that provides Internet access. If your network is not strictly a wireless network, you also need cabling and perhaps one or more switches to create a wired network. This section covers what you need to know to set up and troubleshoot both a wired and wireless network.

8-3a Designing a Wired Network

Core 1 Objective

- 2.3

Compare and contrast protocols for wireless networking.

Begin your network design by deciding where to place your router. If the router is also your wireless access point, take care in where you place it. Place the wireless access point near the center of the area where you want your wireless hotspot to maximize its range for users and minimize your Wi-Fi network's exposure to unauthorized users outside your building. The router also needs to have access to your modem, and the modem needs access to the cable TV or phone jack where it receives service. For a business, the router, modem, and servers are often placed in an electrical closet that can be locked, with additional wireless access points placed where additional coverage is needed. Next, consider where the wired workstations will be placed. Position switches in strategic locations to provide extra network drops to multiple workstations.

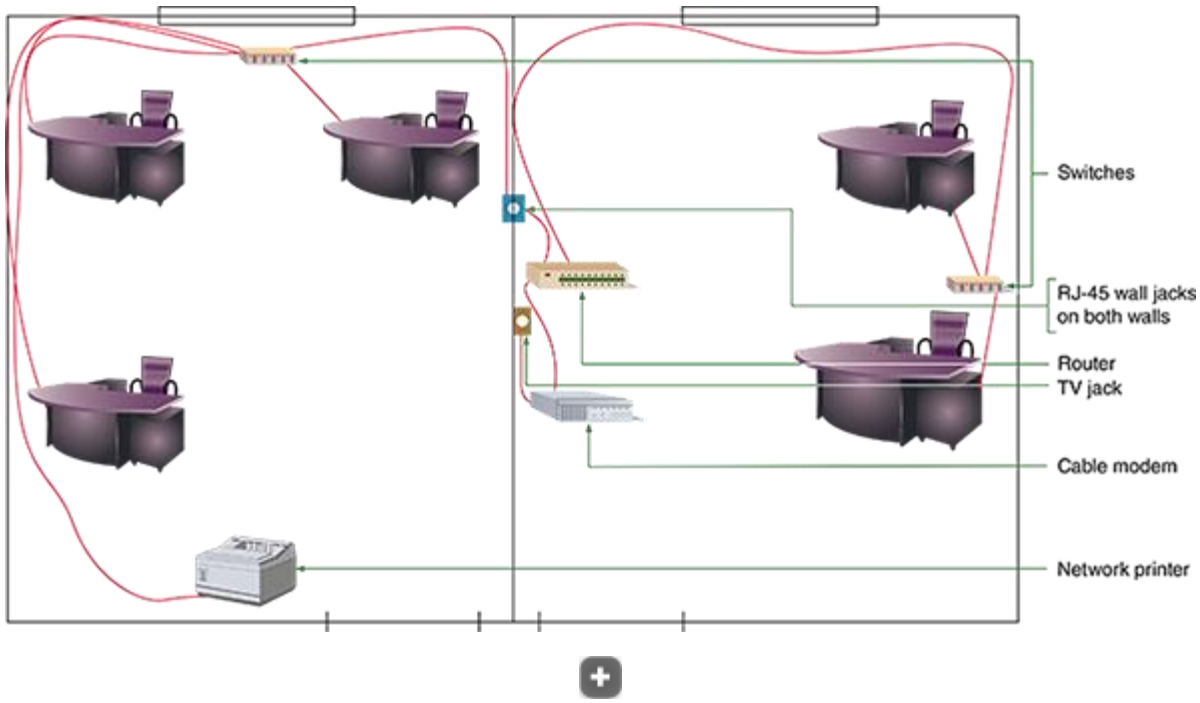
Some network cables might be wired inside walls of your building with wall jacks that use RJ-45 ports. These cables might converge in an electrical closet or server room to connect to switches. If network cables are lying on the floor, be sure to install them against the wall so they won't be a trip hazard. To get the best performance from your network, follow these tips:

- Make sure cables don't exceed the recommended length (100 meters for twisted pair).
- Use twisted-pair cables rated at CAT-5e or higher. (CAT-6 gives better performance than CAT-5e for Gigabit Ethernet, but it's harder to wire and more expensive.)
- Use switches rated at the same speed as your router and network adapters.
- For Gigabit speed on the entire network, use all Gigabit switches, network adapters, and routers. However, if some devices run at slower speeds, a switch or router can likely still support the higher speeds for other devices on the network.

Figure 8-30 shows a possible inexpensive wiring job where two switches and a router are used to wire two rooms for five workstations and a network printer. The only inside-wall wiring required is two back-to-back RJ-45 wall jacks on either side of the wall between the two rooms. The plan allows for all five desktop computers and a network printer to be wired with cabling neatly attached to the baseboards of the office without being a trip hazard.

Figure 8-30

Plan of the physical configuration of a small office



Now let's look at the tools you need to solve problems with network cabling, the details of how a network cable is wired, and how you can create your own network cables by installing RJ-45 connectors on twisted-pair cables.

8-3b Tools Used by Network Technicians

Core 1 Objective

- 2.8

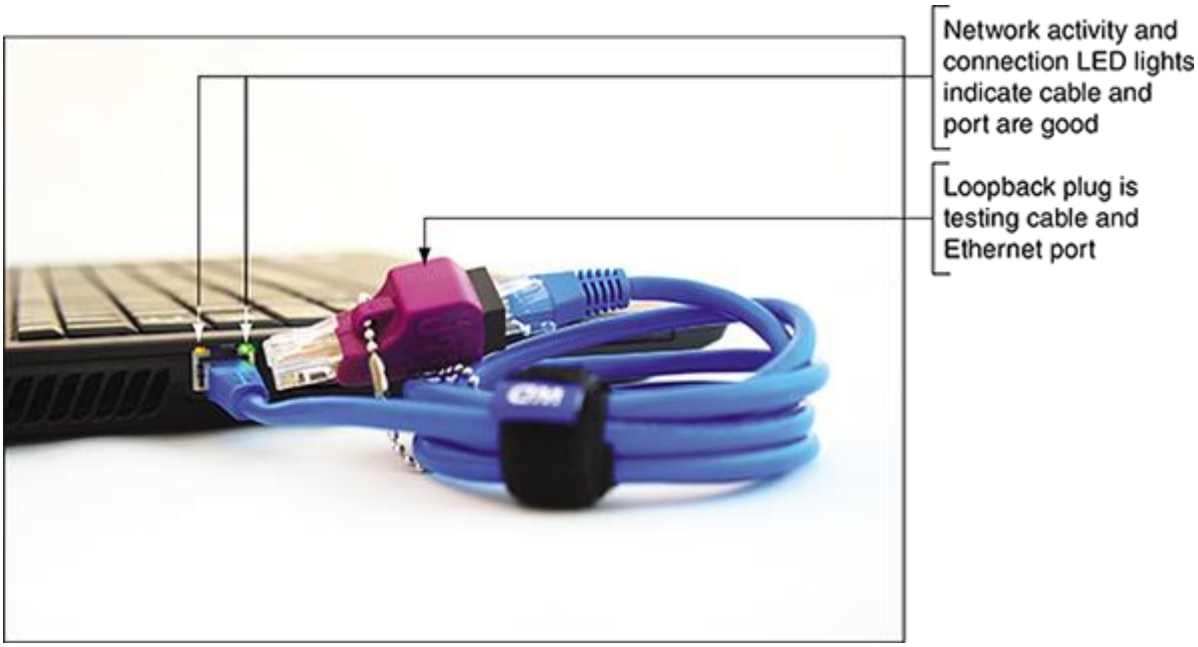
Given a scenario, use networking tools.

Here's a list of tools a network technician might want in their toolbox:

- **Loopback plug.** A loopback plug can be used to test a network cable or port. To test a port, insert the loopback plug into the port. To test a cable, connect one end of the cable to a network port on a computer or other device, and connect the loopback plug to the other end of the cable (see Figure 8-31). If the LED lights on the network port light up, the cable and port are good. Another way to use a loopback plug is to find out which port on a switch in an electrical closet matches up with a wall jack. Plug the loopback plug into the wall jack. The connecting port on the switch in the closet lights up.

Figure 8-31

A loopback plug verifies that the cable and network port are good



- **Cable tester.** A **cable tester**, or cable certifier, is used to determine if a cable is good or to find out what type it is if the cable is not labeled. You can also use a cable tester to locate the ends of a network cable in a building. A cable tester has two components, the remote and the base (see Figure 8-32).

Figure 8-32

Use a cable tester pair to determine the type of cable and/or if the cable is good

To test a cable, connect each component to the ends of the cable, and turn on the tester. Lights on the tester will show you if the cable is good and what type of cable you have. You'll need to read the user manual that comes with the cable tester to know how to interpret the lights.

You can also use the cable tester to find the two ends of a network cable installed in a building. Suppose you see several network jacks on walls in a building, but you don't know which jacks connect back to the switch. Install a short cable in each of the two jacks or a jack and a port in a patch panel.

A **patch panel** (see Figure 8-33) provides multiple network ports for cables that converge in one location such as an electrical closet or server room. Each port is numbered on the front of the panel. Use the cable tester base and remote to test the continuity between remote wall jacks and ports in the patch panel, as shown in Figure 8-34. Whereas a loopback plug works with live cables and ports, a cable tester works on cables that are not live. You might damage a cable tester if you connect it to a live circuit, so before you start connecting the cable tester to wall jacks, be sure that you turn off all devices on the network.

Figure 8-33

A patch panel provides Ethernet ports for cables converging in an electrical closet

Courtesy of Tripp Lite

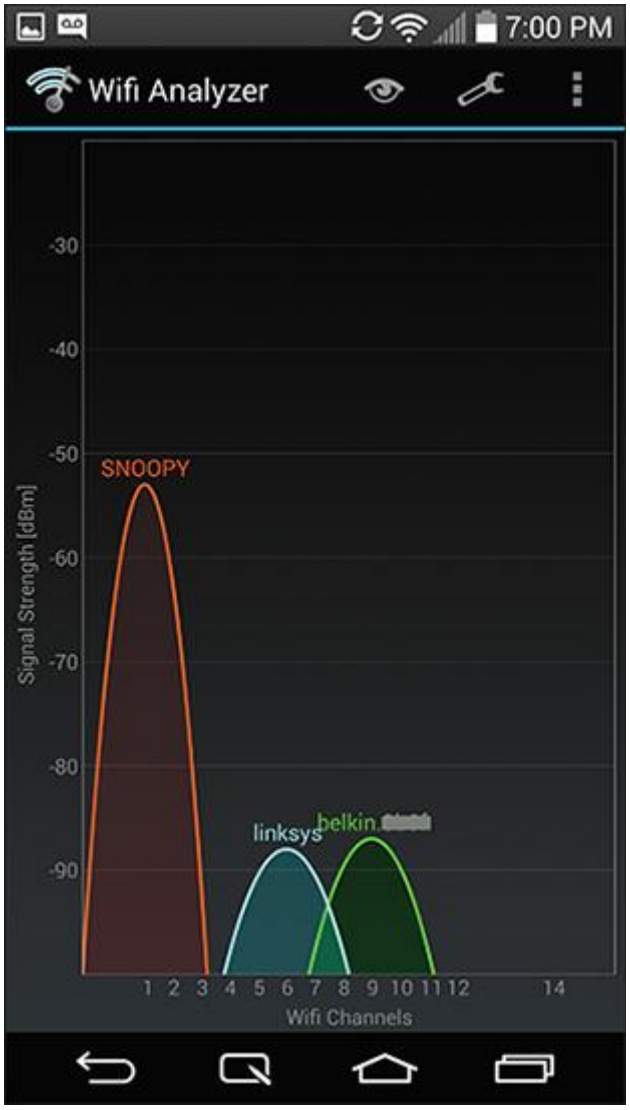
Figure 8-34

Use cable testers to find the two ends of a network cable in a building

- **Wi-Fi analyzer**. A **Wi-Fi analyzer** is software that can find Wi-Fi networks, determine signal strengths, help optimize Wi-Fi signal settings, and help identify Wi-Fi security threats. For example, you can use a Wi-Fi analyzer to find out which Wi-Fi channels are being used before you pick your channels. You can turn your smartphone into a Wi-Fi analyzer by installing a free or inexpensive app through your phone's app store (see Figure 8-35).

Figure 8-35

This Wi-Fi analyzer app detected three wireless networks



Source: Wi-Fi Analyzer app for Android

- **Toner probe.** A **tone generator and probe**, sometimes called a **toner probe**, is a two-part kit that is used to find cables in the walls of a building. See Figure 8-36. The toner connects to one end of the cable and puts out a continuous or pulsating tone on the cable. While the toner is putting out the tone, you use the probe to search the walls for the tone. The probe amplifies the audible tone, so you hear it as a continuous or pulsating beep. The beeps get louder when you are close to the cable and weaker when you move the probe away from the cable. With a little patience, you can trace the cable through the walls. Some toners can put out tones up to 10 miles on a cable and offer a variety of ways to connect to the cable, such as clips and RJ-45 and RJ-11 connectors.

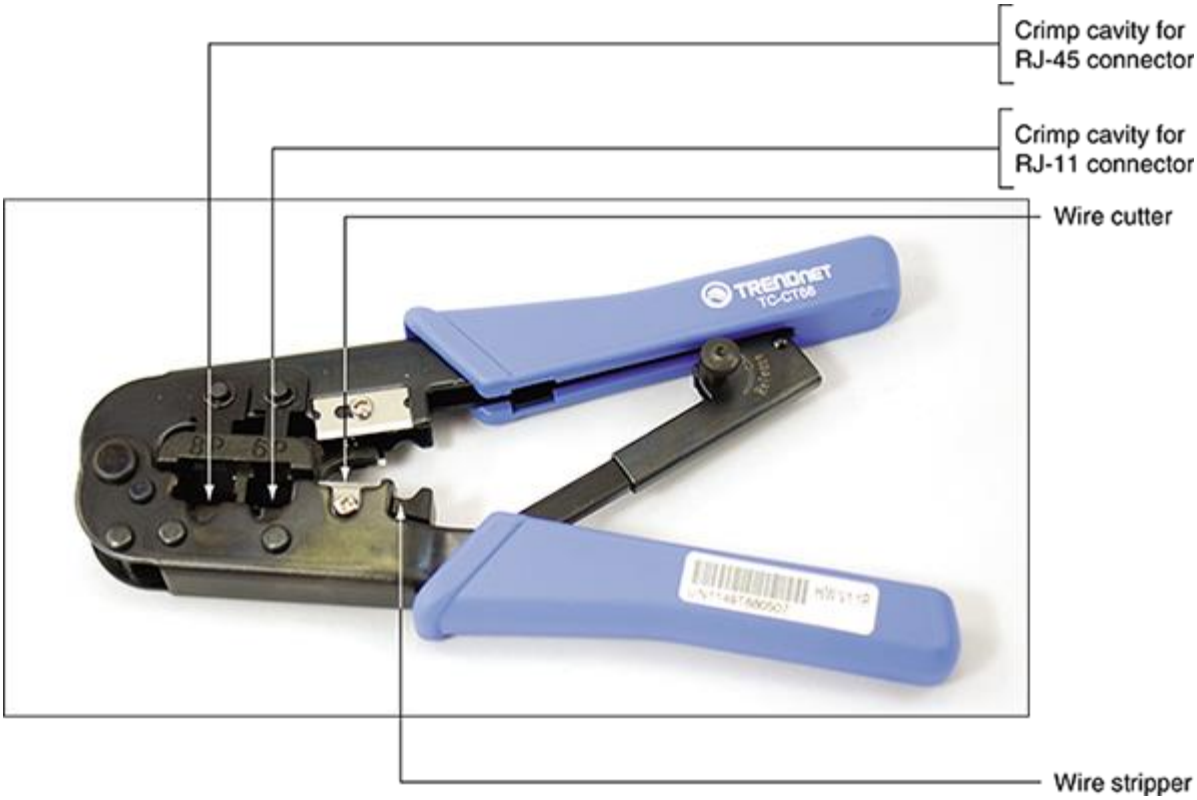
Figure 8-36

A toner and probe kit by Fluke Corporation

- **Cable stripper.** A **cable stripper** is used to build your own network cable or repair a cable. Use the cable stripper to cut away the plastic jacket or coating around the wires inside a twisted-pair cable so you can install a connector on the end of the cable. How to use cable strippers is covered later in the module.
- **Crimper.** A **crimper** is used to attach a terminator or connector to the end of a cable. It applies force to pinch the connector to the wires in the cable to securely make a solid connection. Figure 8-37 shows a multifunctional crimper that can crimp an RJ-45 or RJ-11 connector. It also serves double duty as a wire cutter and wire stripper.

Figure 8-37

This crimper can crimp RJ-45 and RJ-11 connectors



- **Punchdown tool.** A **punchdown tool** (see Figure 8-38) is used to punch individual wires in a network cable into their slots in a keystone RJ-45 jack, which is used in an RJ-45 wall jack. It can also be used to connect the cable to a patch panel or **punchdown block**, shown in Figure 8-39. In a project at the end of this module, you practice using a punchdown tool with a keystone jack.

Figure 8-38

A punchdown tool forces a wire into a slot and cuts off the extra wire

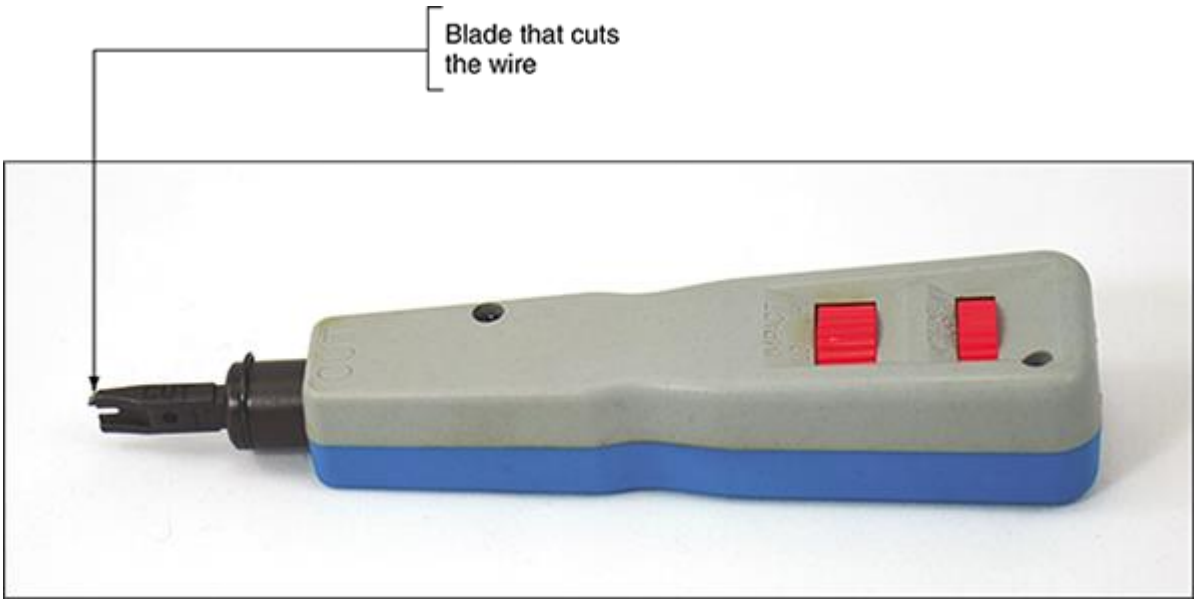


Figure 8-39

A punchdown block allows for multiple cables to be connected to a circuit

Source: Amazon.com, Inc.

- **Network Tap.** A **network tap** is used to provide a connection point for monitoring devices such as an IDS or IPS system and allows the device to be "inline" with the communications on the network. The device can then copy or monitor the traffic without affecting the data flow. A network tap is shown in Figure 8-40.

Figure 8-40

A network tap is used to connect to a network inline with the traffic for monitoring

Source: Amazon.com, Inc.

Now that you know about the tools you need to wire networks, let's see how the cables and connectors are wired.

8-3c How Twisted-Pair Cables and Connectors Are Wired

Core 1 Objectives

- 2.8

  Given a scenario, use networking tools.

- 3.1

  Explain basic cable types and their connectors, features, and purposes.

Two types of network cables can be used when building a network: a straight-through cable and a crossover cable. A **straight-through cable** (also called a **patch cable**) is used to connect a computer to a switch or other network device. A **crossover cable** is used to connect two like devices such as a switch to a switch or a computer to a computer (to make the simplest network of all).

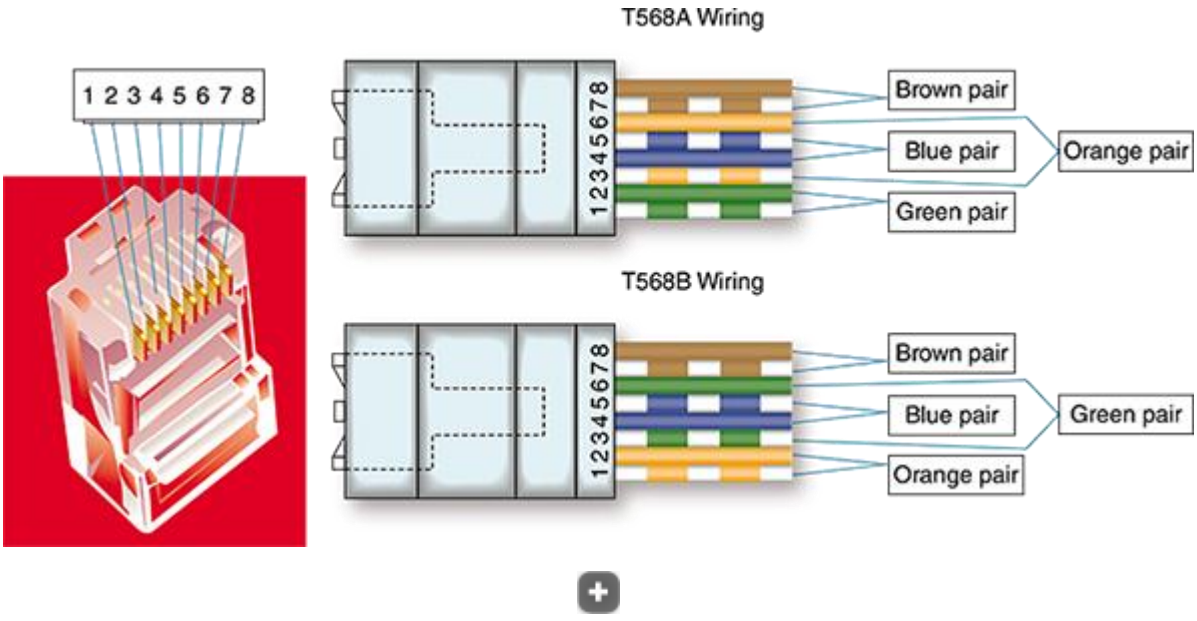
The difference between a straight-through cable and a crossover cable is the way the transmit and receive lines are wired in the connectors at each end of the cables. A crossover cable has the transmit and receive lines reversed so that one device receives off the line on which the other device transmits. Before the introduction of Gigabit Ethernet, 10BaseT and 100BaseT required that a crossover cable be used to connect two like devices such as a switch to

a switch. Today's devices that support Gigabit Ethernet use auto-uplinking, which means you can connect a switch to a switch using a straight-through cable and the devices will negotiate the transmit and receive links, so data crosses the connection successfully. Crossover cables are seldom used today except to connect a computer to a computer to create a simple two-node network.

Twisted-pair copper wire cabling uses an RJ-45 connector that has eight pins, as shown in Figure 8-41. 10BaseT and 100BaseT Ethernet use only four of these pins: pins 1 and 2 for transmitting data and pins 3 and 6 for receiving data. The other pins can be used for phone lines or for power (using PoE). Gigabit Ethernet uses all eight pins to transmit and receive data and can also transmit power on these same lines. Older telephone connections used an RJ-11 connector that had only four pins. This connector was slightly smaller than the RJ-45 used on the eight wire Ethernet cables today.

Figure 8-41

Pinouts for an RJ-45 connector



Twisted-pair cabling used with RJ-45 connectors is color-coded in four pairs: blue, orange, green, and brown, as shown in Figure 8-42. Each pair has one solid wire and one striped wire. Two standards have been established in the industry for wiring twisted-pair cabling and RJ-45 connectors: T568A and T568B. Both are diagrammed in Table 8-4. The **T568A** standard has the green pair connected to pins 1 and 2 and the orange pair connected to pins 3 and 6. The **T568B** standard has the orange pair using pins 1 and 2 and the green pair using pins 3 and 6, as shown in the diagram and the table. For both standards, the blue pair uses pins 4 and 5, and the brown pair uses pins 7 and 8.

Table 8-4

The T568A and T568B Ethernet Standards for Wiring RJ-45 Connectors

Pin	100BaseT Purpose	T568A Wiring	T568B Wiring
1	Transmit+	White/green	White/orange
2	Transmit-	Green	Orange
3	Receive+	White/orange	White/green
4	(Used only on Gigabit Ethernet)	Blue	Blue
5	(Used only on Gigabit Ethernet)	White/blue	White/blue
6	Receive-	Orange	Green
7	(Used only on Gigabit Ethernet)	White/brown	White/brown
8	(Used only on Gigabit Ethernet)	Brown	Brown

Note 4

The T568A and T568B standards, as well as other network wiring standards and recommendations are overseen by the Telecommunications Industry Association (TIA), Electronics Industries Alliance (EIA), and American National Standards Institute (ANSI).

If the wiring on one end of the cable matches the wiring on the other end, be it the T568A or T568B standard, you have a straight-through cable. If you're working on a 10BaseT or 100BaseT network and you use T568A wiring on one end of the cable and T568B on the other end, you have a crossover cable (see the diagram on the left side of Figure 8-42). For Gigabit Ethernet (1000BaseT) that transmits data on all four pairs, you must cross the green and orange pairs as well as the blue and brown pairs to make a crossover cable (see the diagram on the right side of Figure 8-42). Recall, however, that crossover cables are seldom used on Gigabit Ethernet. When you buy a

crossover cable, it is most likely wired only for 10BaseT or 100BaseT networks. If you ever find yourself needing to make a crossover cable, be sure to cross all four pairs so the cable will work on 10BaseT, 100BaseT, and 1000BaseT networks. You can also buy an adapter to convert a straight-through cable to a crossover cable, but the adapter most likely will only cross two pairs and work only for 10BaseT or 100BaseT networks, such as the adapter shown in Figure 8-43.

Figure 8-42

Two crossed pairs in a crossover cable are compatible with 10BaseT or 100BaseT Ethernet; four crossed pairs in a crossover cable is compatible with gigabit Ethernet

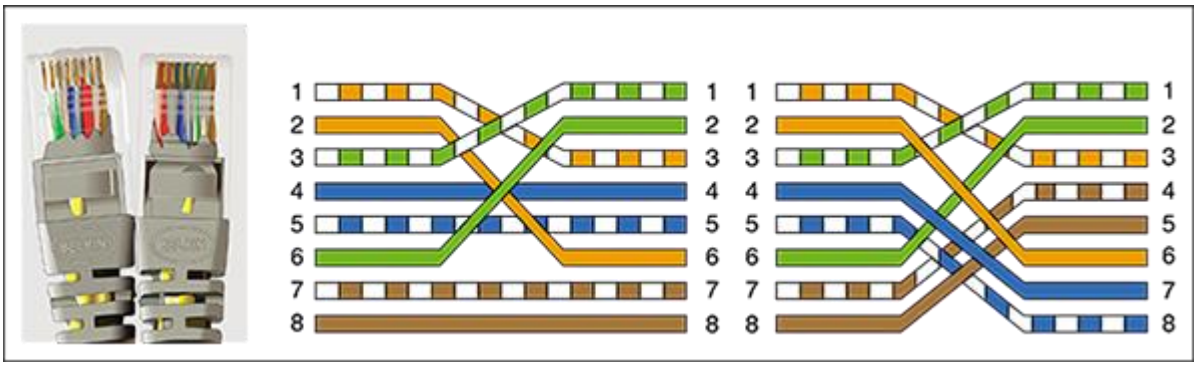


Figure 8-43

A crossover adapter converts a patch cable to a crossover cable for a 10BaseT or 100BaseT network

Although it's possible to mix standards on the same network, you should always be consistent with which standard you use. When you are wiring a network in a building that already has network wiring, be sure to find out if the wiring is using T568A or T568B, and then be sure you always use that

standard. If you don't know which to use, use T568B because it's the most common.

Applying Concepts

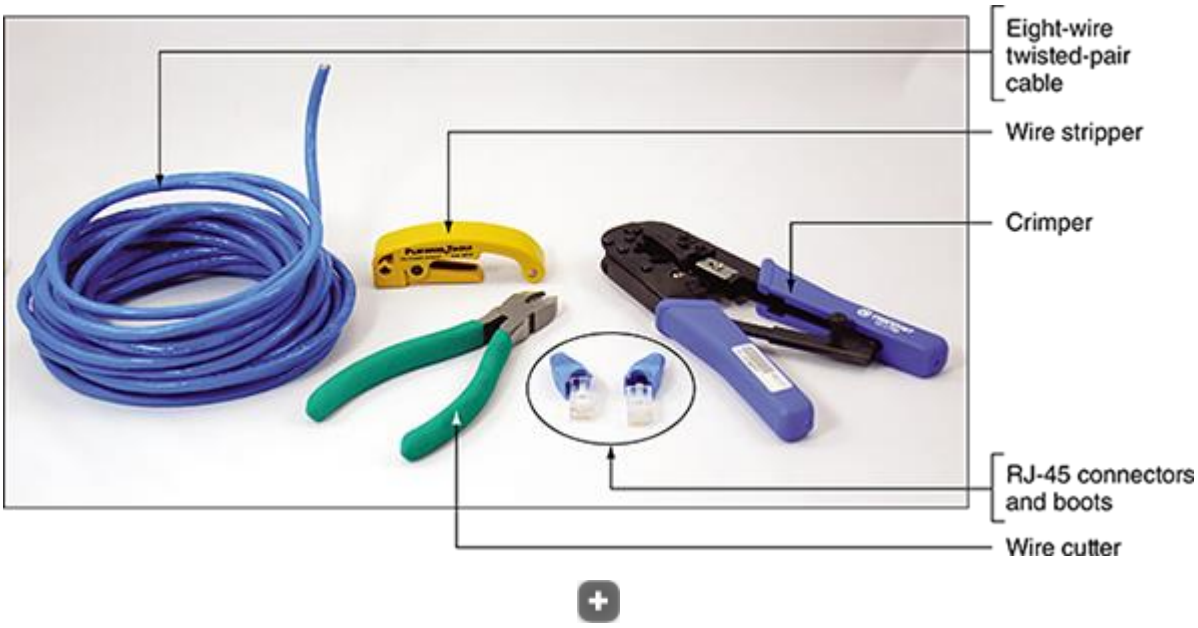
Making a Straight-Through Cable Using T568B Wiring

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 3.1

It takes a little practice to make a good network straight-through cable, but you'll get the hang of it after doing only a couple of cables. Figure 8-44 shows the materials and tools you'll need to make a network cable.

Figure 8-44

Tools and materials to make a network cable



Here are the steps to make a straight-through cable using the T568B standard:

1. 1
   Use wire cutters to cut the twisted-pair cable the correct length plus a few extra inches.
2. 2
   If your RJ-45 connectors include boots, slide two boots onto the cable. Be sure they're each facing the correct direction.
3. 3
   Use wire strippers to strip off about two inches of the plastic jacket from the end of the wire. To do that, put the wire in the stripper and rotate the stripper around the wire to score the jacket (see Figure 8-45). You can then pull off the jacket.

Figure 8-45

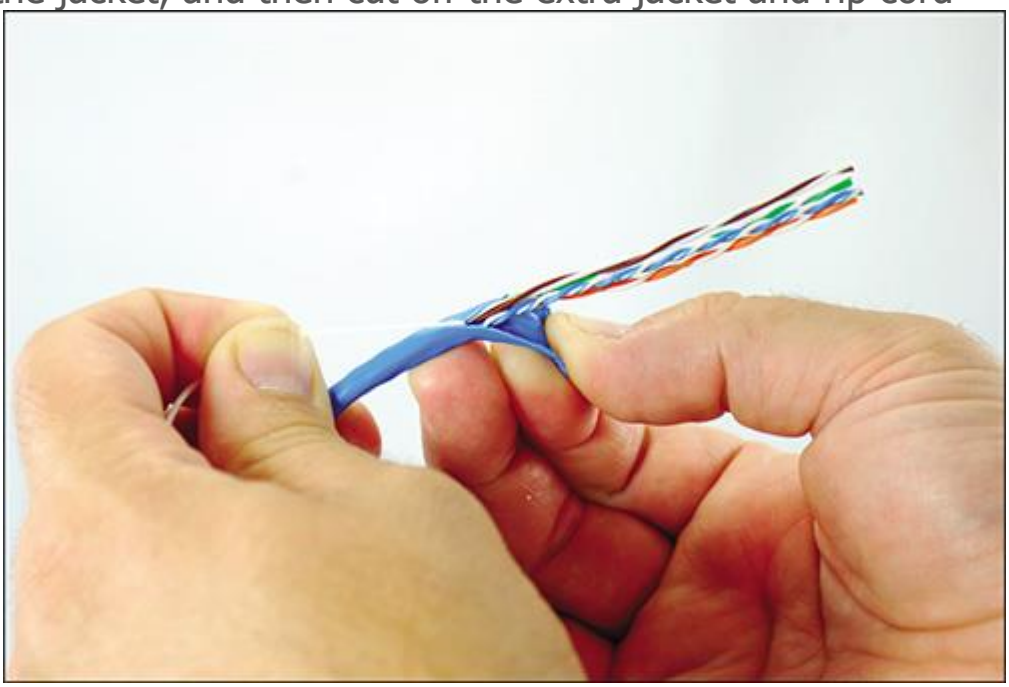
Rotate a wire stripper around the jacket to score it so you can slide it off the wire

4. 4

Use wire cutters to start a cut into the jacket, and then use the rip cord to pull the jacket back a couple of inches (see Figure 8-46). Next, cut off the rip cord and the jacket. You take the extra precaution of removing the jacket because you might have nicked the wires with the wire strippers.

Figure 8-46

Rip back the jacket, and then cut off the extra jacket and rip cord



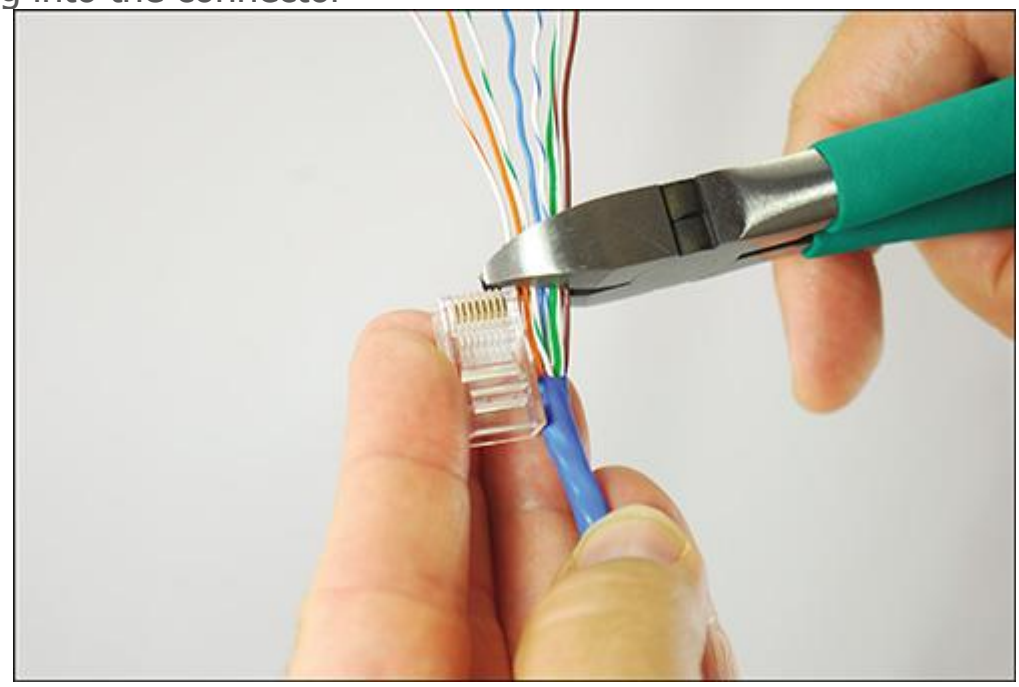
5. 5

Untwist each pair of wires so you have eight separate wires. Smooth each wire to straighten out the kinks. Line up the wires in the T568B configuration (refer to Table 8-4).

6. 6
Holding the tightly lined-up wires between your fingers, use wire cutters to cut the wires off evenly, leaving a little over an inch of wire. See Figure 8-47. To know how short to cut the wires, hold the RJ-45 connector up to the wires. The wires must go all the way to the front of the connector. The jacket must go far enough into the connector so that the crimp at the back of the connector will be able to solidly pinch the jacket.

Figure 8-47

Evenly cut off wires measured to fit in the RJ-45 connector with the jacket protruding into the connector



Note 5

You'll find several YouTube videos on network wiring. An excellent video by Ferrules Direct for making a straight-through cable is posted at youtube.com/watch?v=WvP0D0jiyLg.

7. 7
Be sure you have pin 1 of the connector lined up with the orange-and-white wire. Then insert the eight wires in the RJ-45 connector. Guide the wires into the connector, making sure they reach all the way to the front. (It helps to push up a bit as you push the wires into the connector.) You can jam the jacket firmly into the connector. Look through the clear plastic connector to make sure the wires are lined up correctly, that they all reach the front, and that the jacket goes past the crimp.

8. 8
Insert the connector into the crimper tool. Use one hand to push the connector firmly into the crimper as you use the other hand to crimp the connector. See Figure 8-48. Use

plenty of force to crimp. The eight blades at the front of the connector must pierce through to each copper wire to complete each of the eight connections, and the crimp at the back of the connector must solidly crimp the cable jacket to secure the cable to the connector (see Figure 8-49). Remove the connector from the crimper, and make sure you can't pull the connector off the wire.

Figure 8-48

Use the crimper to crimp the connector to the cable

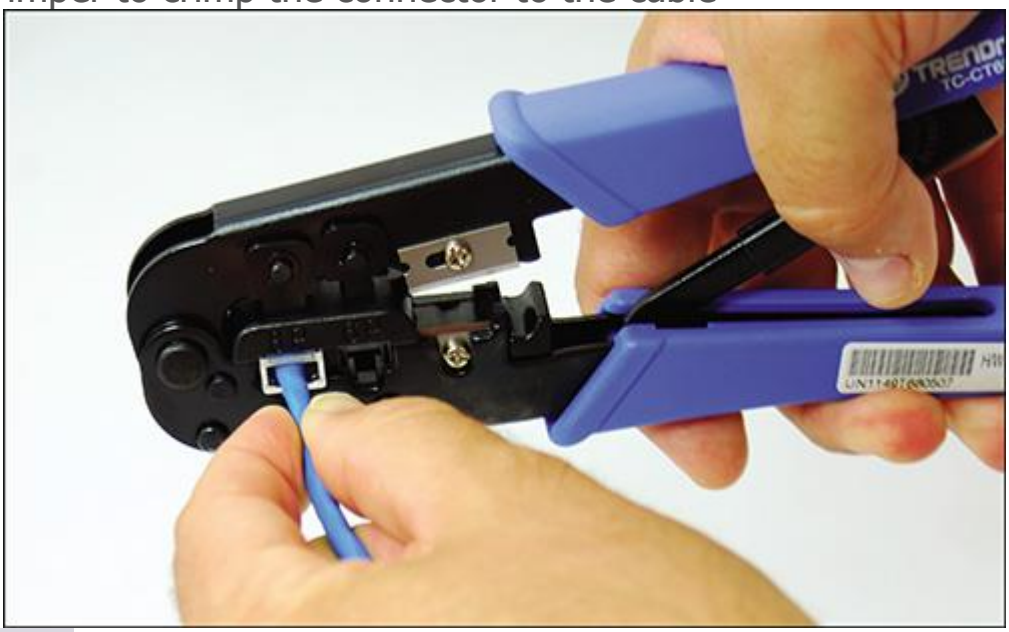
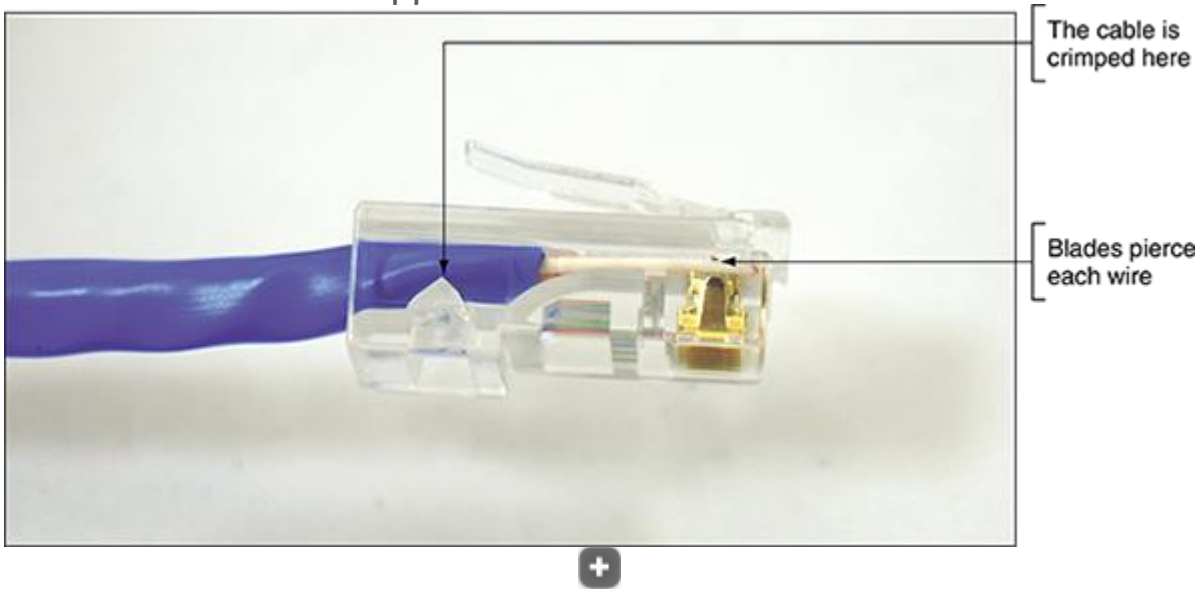


Figure 8-49

The crimper crimps the cable and cable jacket, and eight blades pierce the jacket of each individual copper wire



9. 9

Slide the boot into place over the connector. Now you're ready to terminate the other end of the cable. Configure it to also use the T568B wiring arrangement. Figure 8-50 shows the straight-through cable with only one boot in place.

Figure 8-50

A finished patch cable with one boot in place

10. 10

Use a cable tester to make sure the cable is good.

Note 6

According to networking standards for wiring a keystone RJ-45 jack and a straight-through cable, you can avoid crosstalk by removing the cable jacket to expose no more than three inches of twisted-pair wires, and you should untwist exposed twisted-pair wires no more than a half inch.

8-3dWi-Fi Networking

Core 1 Objective

- 2.3

Compare and contrast protocols for wireless networking.

Wi-Fi, or wireless fidelity, networking uses radio frequencies to transmit and receive data between the wireless access point and the device connected to the network. Recall from the module "Networking Fundamentals" that you need the wireless network name, called the SSID, to join the wireless network.

As shown in Table 8-1 at the beginning of this module, each 802.11 standard can transmit on different frequencies: 2.4 GHz or 5 GHz (gigahertz). By using

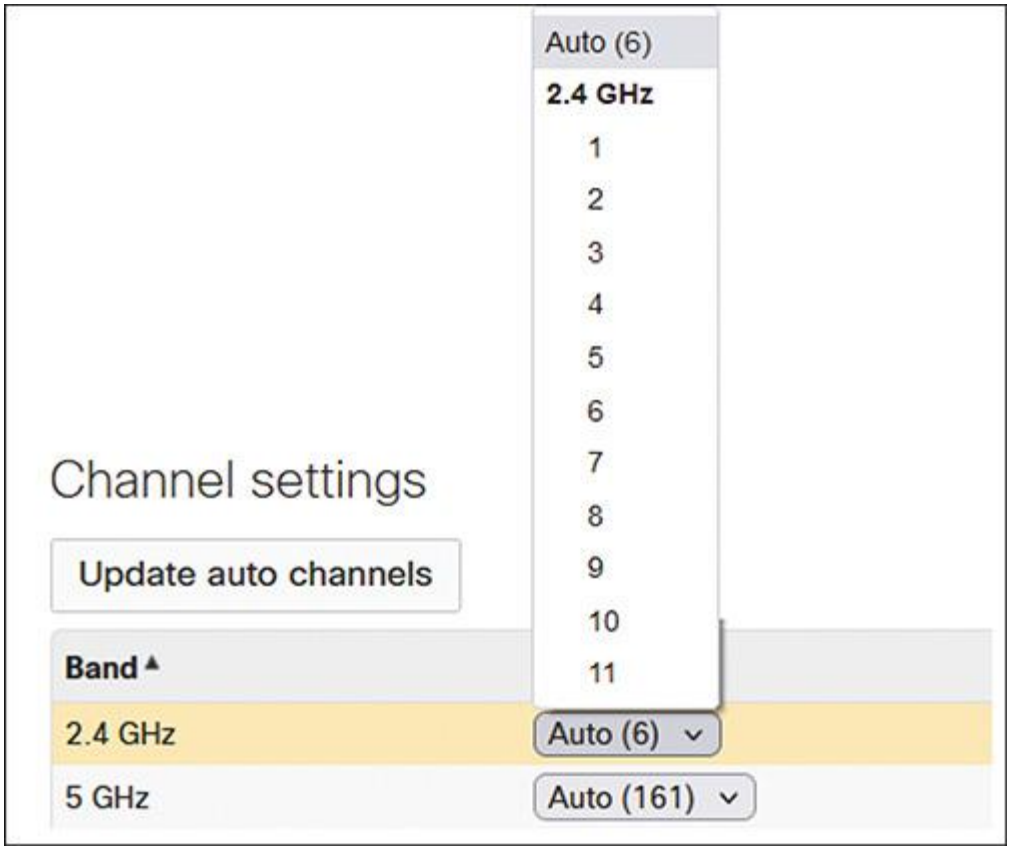
these radio frequencies, we can transmit data between devices easily because these frequencies are reserved for this special purpose. The 2.4 GHz frequency provides a longer transmit distance but has a slower speed when compared to the short distance, high-speed connections provided by 5 GHz. Refer to Table 8-1 for the maximum transmit speed for each Wi-Fi standard.

Wi-Fi Channels

A **channel** is a specific radio frequency within a broader frequency. For example, 2.412 GHz and 2.437 GHz are two channels in the 2.4 GHz band. In the United States, the FCC, which regulates Wi-Fi, has made 11 channels available for wireless communication in the 2.4 GHz band. 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, although 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 one router, the Wi-Fi Settings page provides a dropdown menu to select a specific channel or to allow the router to automatically select the least busy channel (see Figure 8-51).

Figure 8-51

Wi-Fi channel selection can be set to auto or manually select a specific channel



Source: Meraki

8-4 Troubleshooting Network Connections

Core 1 Objective

- 5.7

Given a scenario, troubleshoot problems with wired and wireless networks.

Troubleshooting networks is one of the primary tasks a help desk associate will be assigned in the course of their job. You may be asked to resolve issues caused by a simple loss of power or connectivity or those resulting from a broken network adapter or cable. Being able to quickly and thoroughly troubleshoot issues so employees and clients can continue their own work is important. In this section of the module, you learn to troubleshoot several network issues.

8-4a Limited or Slow Wired Connectivity

Core 1 Objective

- 5.7

Given a scenario, troubleshoot problems with wired and wireless networks.

Limited or slow wired connectivity to the network can be caused by many factors. When trying to resolve these types of network connectivity issues, check the following:

- Hardware configuration errors, such as speed or duplex settings on the network interface card.
- Switch port settings, which should be verified with network administrator.
- High usage by other network clients or users. Network monitoring software such as Wireshark (wireshark.org) or other software applications can be used to capture and analyze traffic.
- Configuration issues with a router or modem. Solving this type of issue may require calling your ISP for assistance.

Exam Tip

Some skills mentioned in this section, such as using Wireshark or configuring a managed switch, are described so you have an idea of what to expect when troubleshooting a network. You learn to do these skills in later networking classes. For the A+ Core 1 exam, you are expected to only know about these skills and tools—not necessarily how to use them.

8-4b Port Flapping

Core 1 Objective

- 5.7

Given a scenario, troubleshoot problems with wired and wireless networks.

Port flapping occurs when a particular interface or port on a switch is continually going up and down. This rapid switching between statuses, or flapping, prevents devices from communicating on the network. When port flapping occurs, check the following:

- The most likely cause of port flapping is a misconfiguration on the switch. To correct the problem, a technician should verify the configuration with the network administrator.
- Another cause of port flapping is bad cables. Check that cable connections to the port are solid. Try exchanging the cables.
- The SFP card that provides SFP ports on the switch might be bad. An SFP (small form-factor pluggable) card provides various SFP card ports, such as the four ports shown in Figure 8-52. One slot has a card

already installed in it. Verify cable connections are solid, and try exchanging cables or exchanging the SFP card with a known good one.

Figure 8-52

A fiber-optic SFP port with an LC fiber cable attached

- Check for updates to the switch firmware. Sometimes outdated firmware can cause problems.

8-4c Network Jitter and High Latency

Core 1 Objective

- 5.7

Given a scenario, troubleshoot problems with wired and wireless networks.

Network jitter, or fluctuations in latency on your network, can cause network communication disruptions. Recall that latency is the measurement of time between when a packet is sent and when it is finally received by the end device. **High latency** situations can occur because of high network use or because of the technology your network uses for Internet connectivity. Satellite and wireless networks tend to have higher latency than a wired network. If the network is experiencing jitter, try the following:

- Check network cable connections at both the local workstation and at the wall jack and from the wall jack to the patch panel.
- Check for connectivity and activity lights on physical interfaces (the network ports on the computer, the switch, or the SOHO router). For

wireless connectivity, check for signal strength on the connected network.

- Check connectivity between network infrastructure, such as connections between a switch and a router on the network. For a managed switch, verify with the network administrator how ports, including SFP interfaces, are configured.
- To check for connectivity, use the ping command. You can ping another computer on the network or on the Internet. For example, to check for connectivity on the Internet, ping a Google DNS server using its IP address:

```
ping 8.8.8.8
```

8-4d VoIP Call Quality

Core 1 Objective

- 5.7

Given a scenario, troubleshoot problems with wired and wireless networks.

VoIP (voice over IP) phones require high throughput in order to ensure high quality of service (QoS)—which, in turn, ensures that your phone calls are loud and clear, without echoing, delay, or static. Low QoS issues may be caused by the following:

- Other services being prioritized over the phone call
- Lack of bandwidth
- Misconfiguration of the phone system

To troubleshoot VoIP issues, check to make sure the VoIP phone system is correctly configured. You may want to isolate the phones to their own VLAN or subnet. You can also configure QoS settings on your network to prioritize the VoIP applications and devices over other applications and devices using the network. Recall that to implement QoS, priorities must be set on every device using the network, including the SOHO router and each network adapter and OS on the network.

8-4e Intermittent Wireless and External Interference

Core 1 Objective

- 5.7

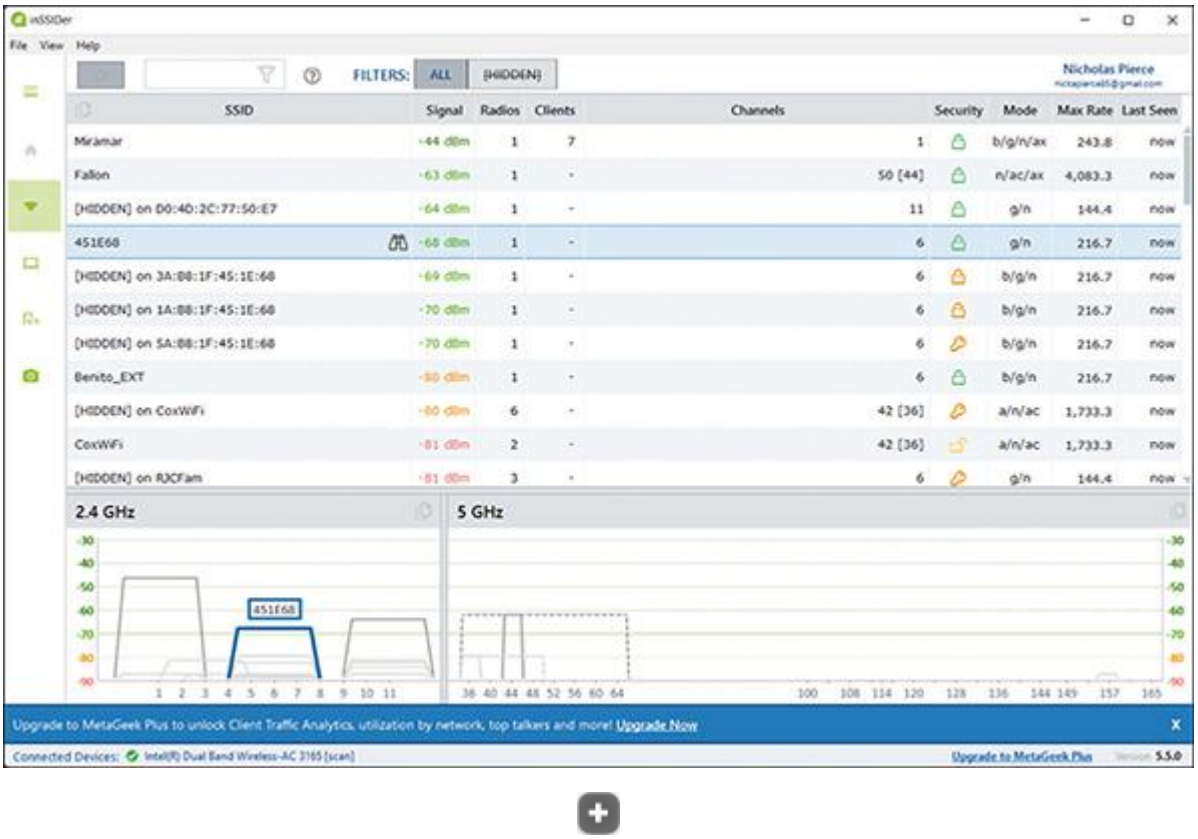
Given a scenario, troubleshoot problems with wired and wireless networks.

Because wireless networks are susceptible to interference from a variety of sources—including neighboring wireless networks, other RF devices such as cordless phones or radios, microwaves, or walls—these types of issues can cause even experienced technicians to scratch their heads. The use of a

wireless network analyzer—such as inSSIDer, shown in Figure 8-53—or an RF spectrum analyzer device, such as the one shown in Figure 8-54—can help identify the source of interference.

Figure 8-53

Wi-Fi analyzer software, such as inSSIDer, can be used to see details of nearby wireless networks



Source: inSSIDer

Figure 8-54

An RF spectrum analyzer can help identify the source of interference

Source: Amazon.com, Inc.

Now that you have learned some basics of fixing problems with a network, let's look at how technology has evolved to allow for two or more systems to use the same physical hardware with virtualization.

8-5 Client-Side Virtualization

Core 1 Objectives

- 4.1

  Summarize cloud-computing concepts.

- 4.2

  Summarize aspects of client-side virtualization.

Virtualization in computing is when one physical machine hosts multiple activities that are normally done on multiple machines. Desktop virtualization, also called **virtual desktop infrastructure (VDI)**, is when one computer provides multiple desktops for users. Each **virtual desktop**, or instance, is contained in its own virtual machine.

Note 7

When a user ends a session with a VDI virtual desktop, the user can request that changes they made to the virtual machine be saved until the next session. When changes are saved, the virtual desktop is said to be persistent and working in a persistent environment. If each time the user starts a new session, the virtual desktop resets to its default configuration and settings, the virtual desktop is said to be nonpersistent.

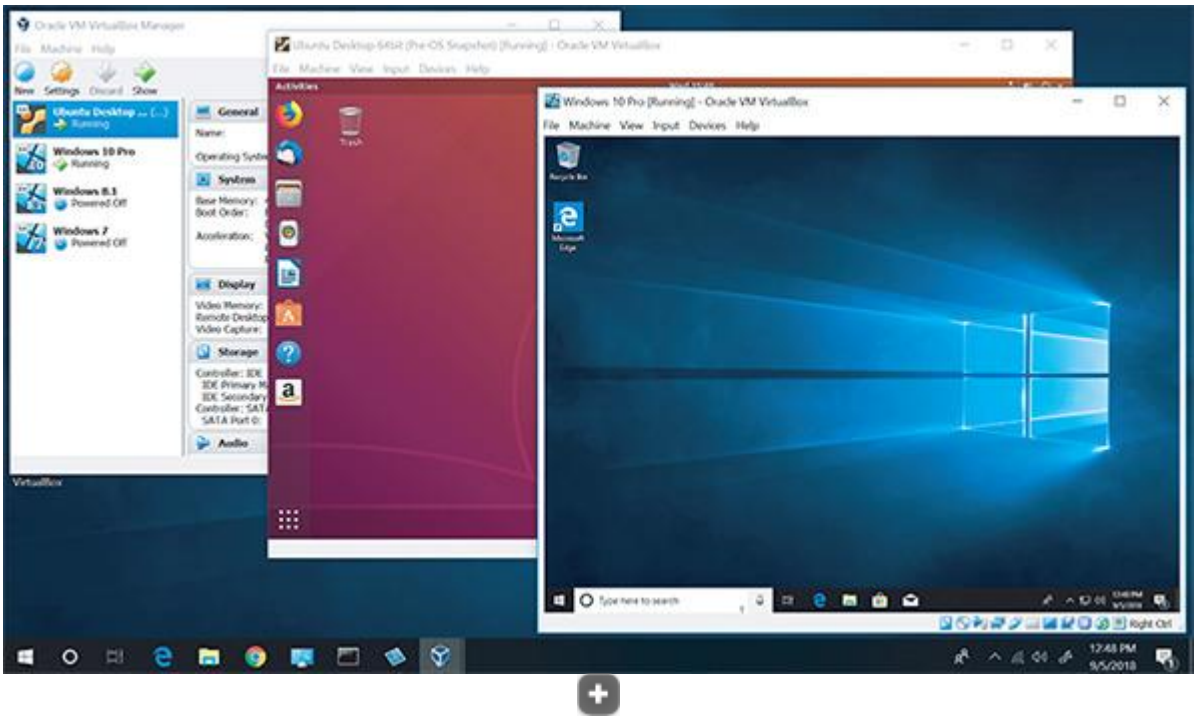
With desktop virtualization, software called a **hypervisor** creates and manages the virtual machines (VMs). Each VM that is managed by a hypervisor has its own virtual hardware (virtual motherboard, processor, RAM, hard drive, NIC, and so forth) and

acts like a physical computer. After an OS is installed in a VM, applications can be installed.

Figure 8-55 shows a Windows 10 Professional desktop with two virtual machines running that were created by Oracle VirtualBox, which is hypervisor software. One VM is running Windows 10 and the other VM is running Ubuntu Desktop, which is a Linux OS. You'll learn about Linux in the Core 2 module "Linux and Scripting." In the Core 2 module "Installing Windows," you will complete an activity that involves installing Windows in a VM.

Figure 8-55

Two virtual machines running on a Windows 10 host, each with its own virtual hardware and OS (Windows 10 and Ubuntu Linux)



Source: Oracle Corporation

Virtualization can be used for many purposes, including the following:

- **Cross-platform virtualization.** With **cross-platform virtualization**, you install a different operating system in a VM than the one installed on your host machine supporting the VM. One reason to use cross-platform virtualization is when you install Linux in a VM on your Windows 10 laptop so that you can learn to use this OS.
- **Application virtualization.** You can run an application in a VM that is not meant for your normal operating system or platform, a practice referred to as **application virtualization**. For example, if you need to run an old application compiled for Windows 95, you can install Windows 95 in a VM on your Windows 10 desktop and run the **legacy software** in the Windows 95 VM. In another example, you can create a VM on your Windows 10 desktop, install Linux in the VM, and install Apache HTTP Server (a web server) in Linux.

- **Sandboxing.** A **sandbox** is an isolated environment where users and developers can learn and experiment safely without affecting the live environment. VMs are a popular sandboxing method for researching, experimenting, and testing. Researching computer security issues such as examining the latest malware within a virtual machine can help isolate the malware from the rest of your network and system. Software and app developers may use sandboxing in a VM for **test development** before publicly publishing it.

8-5a Setting Up Client-Side Virtualization

Core 1 Objective

- 4.2

Summarize aspects of client-side virtualization.

Desktop virtualization can be implemented in the cloud or on premises. On premises, an IT support technician might be called on to set up client-side virtualization on a workstation to host multiple VMs. The first step is to make sure the workstation can support the hypervisor and VMs.

Customize a Virtualization Workstation

Here are the requirements for a workstation that will host multiple virtual machines:

- **Maximum CPU cores.** Each VM has its own virtual processor, so it's important that the host's processor is a multicore processor. All dual-core or higher processors sold today support hardware-assisted virtualization (HAV), which is a technology that enhances the processor support for virtual machines. For Intel processors, this feature is called Intel VT. For AMD processors, the technology is called AMD-V.
- **The motherboard BIOS/UEFI.** Most of today's motherboards support HAV, and it must be enabled in the BIOS/UEFI setup. Figure 8-56 shows the UEFI setup screen for one motherboard where the HAV feature is called Intel Virtualization Technology. When you enable the feature, also verify that all subcategories are enabled under the main category for hardware virtualization.

Figure 8-56

A UEFI setup screen to enable hardware virtualization

Source: American Megatrends, Inc.

- **Maximum RAM.** Some hypervisors are designed so that each VM that is running ties up all the RAM assigned to it. Therefore, you need large amounts of RAM when a computer is running several VMs.
- **Lots of storage space.** Each VM has its own virtual hard drive (VHD), which is a file stored on the physical hard drive that acts like an independent hard drive, complete with its own boot sector and file systems. You can configure this VHD to be a fixed size or dynamically expanding. The fixed size takes up hard drive space whether the VM uses the space or not. A dynamically allocated VHD increases in capacity as the VM uses the space. Each VM must have an operating system installed, which takes about 20 GB for a Windows 10 installation. In addition, each application installed in a VM requires storage space. Make sure you have adequate storage space for all the VMs the customer plans to create. See the requirements provided by the hypervisor manufacturer for additional recommendations.
- **Network requirements.** If multiple VMs on the workstation will be running at the same time, you'll need a fast network connection; make sure the NIC supports Gigabit Ethernet. Later, when you set up the workstation, it might require a static IP address so others on the network can reach the VMs. Also consider using two NICs in the

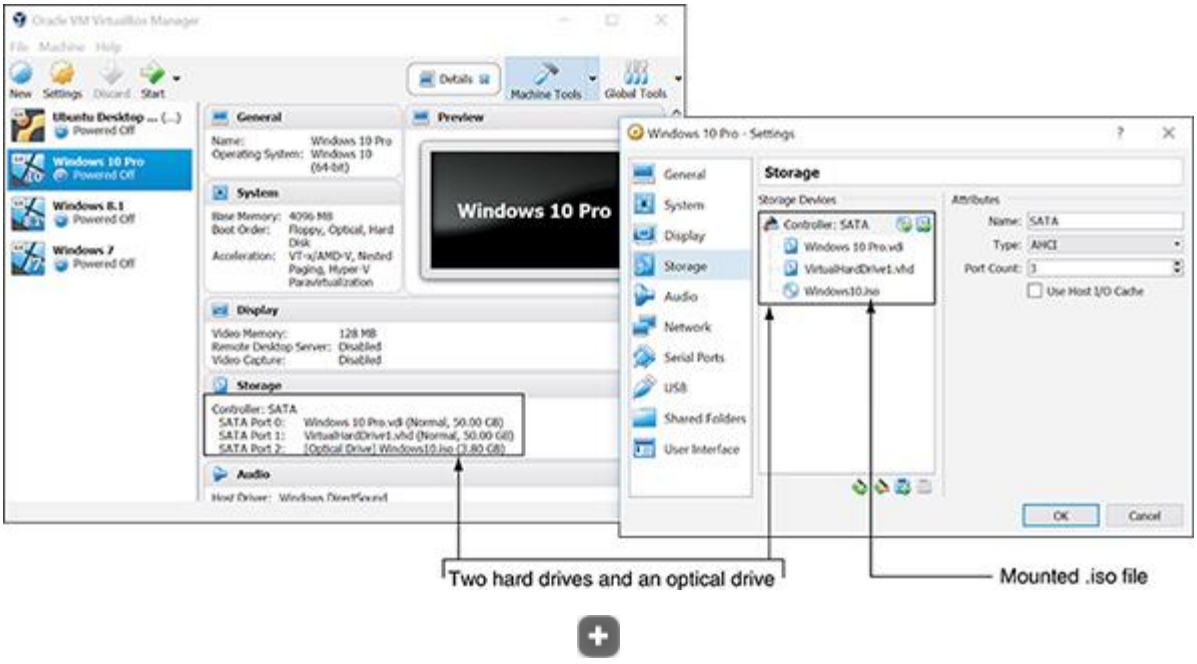
workstation: The hypervisor can run all the VMs through one NIC that has the static IP address assignment, and the other NIC is used for other network activity on the host workstation. Some network administrators may also choose to set up the VMs in their own VLAN. When deciding how to use the overall budget for a virtualization workstation, prioritize the number of CPU cores and the amount of installed RAM.

Install and Configure a Hypervisor

A hypervisor offers a way to configure each VM, including which virtual hardware is installed. For example, when you launch **Oracle VirtualBox**, the VirtualBox Manager window shown on the left side of Figure 8-57 appears. To create a new VM, click **New** in the upper-left corner, and follow the directions on-screen. To change the configuration of a VM, select the VM in the left pane and click **Settings**. In the Settings dialog box, click **Storage**, as shown on the right side of Figure 8-57, to install and uninstall virtual hard drives and optical drives in the VM.

Figure 8-57

Emulated (virtual) hard drives and an optical drive are installed in a VM on VirtualBox



Source: Oracle Corporation

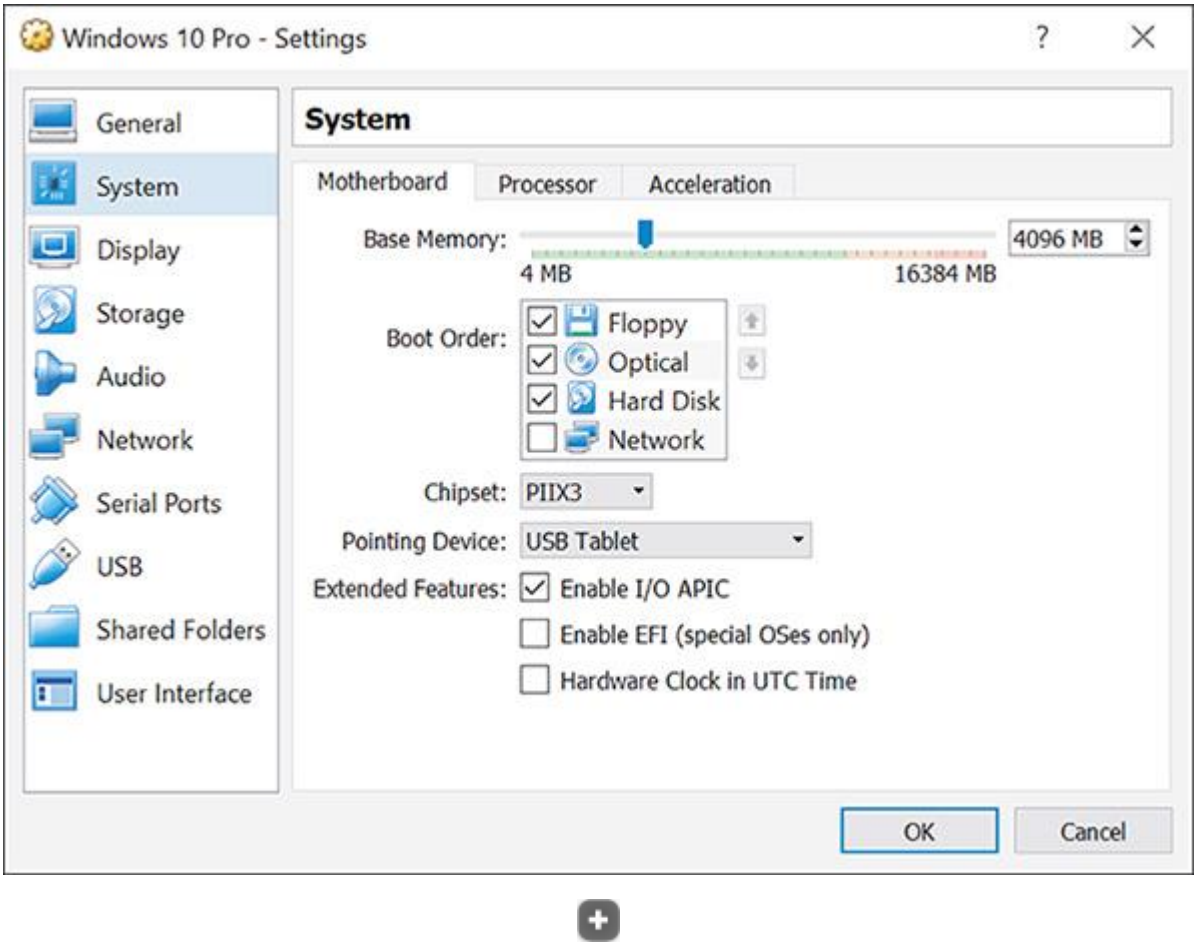
Notice in the Settings dialog box in Figure 8-57 that the VM, which does not yet have an OS installed, has two hard drives and an optical drive. The virtual hard drive named *Windows 10 Pro.vdi* is connected to SATA port 0 and will contain the Windows 10 installation. *VirtualHardDrive1.vhd*, a backup hard drive for this VM, is the same size (50 GB) and is connected

through SATA port 1. The virtual optical drive is connected to SATA port 2 and holds the Windows 10 ISO file, ready for installation on the VM. An ISO file holds the image of a CD or DVD and can be used to provide Windows installation files. When you mount this file to the VM, you can install Windows in the VM from this virtual DVD; many hypervisor programs will perform this step for you during setup of a new VM.

In the Settings dialog box, click **System** to configure motherboard settings, such as boot order and memory (see Figure 8-58). Also consider network requirements for the VM. A VM can have one or more virtual network adapters, called a **virtual NIC**. Click **Network** (see Figure 8-59) to change adapter settings.

Figure 8-58

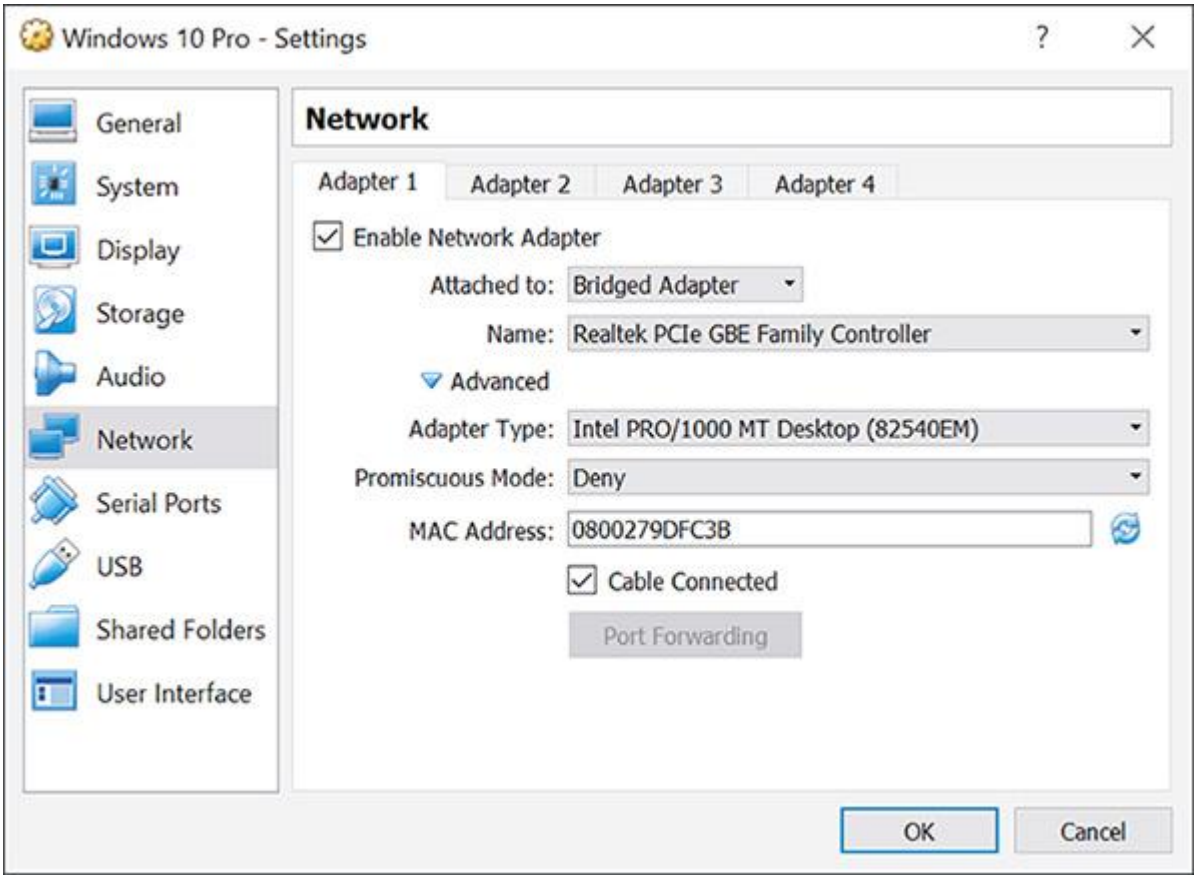
Configure motherboard settings in the VM to change the boot order



Source: Oracle Corporation

Figure 8-59

Configure up to four network adapters for a VM in Oracle VirtualBox



Source: Oracle Corporation

A VM can connect to a local network in the same way as other computers using the host computer's network interface, and it can share and use shared resources on the network. Alternatively, you can keep the VM isolated from the physical network while connected to other VMs on the host computer, or you can keep it completely isolated from all physical and virtual networks. In the Network pane of the Settings dialog box, you can control the number and type of installed network adapters—up to four adapters for this hypervisor, as shown in Figure 8-59.

To boot up a VM, select it in the left pane, and click **Start** in the menu. The VM boots up and works the same way as a physical computer.

8-5b Securing a Virtual Machine

Core 1 Objective

- 4.2

Summarize aspects of client-side virtualization.

Just like a physical machine, a virtual machine is susceptible to hackers and malware. When supporting a VM that holds sensitive data and has network

and Internet connectivity or is in a public area, keep these points in mind for securing VM resources:

- **Secure the VM within the VM.** Using the OS installed in the VM, follow all the security measures you are learning throughout this text. For example, be sure to configure the OS firewall in the VM, keep updates current, install and run anti-malware software, require passwords for all user accounts in the VM, and encrypt data folders.
- **VMs should be isolated for best security.** One major advantage of using VMs on a workstation is that a VM on one workstation is better isolated from a VM on another because the workstations provide an extra layer of protection. Also, the host workstation for VMs should not be used for web surfing or other activities that might compromise its VMs. If a workstation has more than one NIC, a VM that should be kept especially secure can be isolated by dedicating a NIC solely to this VM and putting this NIC on its own subnet.
- **Secure the files that hold a VM.** You can move a VM from one computer to another by moving the files that contain the VM. Be sure these files that hold the VM are secured with permissions that allow access only to specific local or network users and apply file encryption to the files.
- **Secure the host computer.** Protect your VMs by applying security measures to protect the host computer that holds the VMs. For example, run anti-malware, keep Windows updated, require password authentication to sign in to the host computer, harden the host computer's firewall, and isolate it on the network in a protected subnet.

Exam Tip

The A+ Core 1 exam might give you a scenario that requires you to secure a virtual machine installed on a host computer.

Just as virtualization can be set up on your own hardware, let's look how virtualization can be expanded across the Internet using a third party's hardware for your own computing needs. To the cloud we go!

8-6 Cloud Computing

Core 1 Objective

- 4.1

Summarize cloud-computing concepts.

In the module "Networking Fundamentals," you learn about server resources available on a network, and in this module, you learn some ways to virtualize network resources. Not all a network's resources reside on the

local network. **Cloud computing** is when a vendor or corporation makes computing resources available over the Internet. For example, Google Drive, iCloud Drive, Dropbox, and OneDrive are cloud file storage services that allow you to store your files in the cloud. These services work with synchronization apps on mobile devices and computers to sync data and settings under a user account—such as a Google, Apple, or Microsoft account—between the cloud and devices using the account. Cloud computing can also provide many other types of services and resources, including applications, network services, websites, database servers, specialized developer applications, and virtual desktops in VMs.

The current trend for both small and large businesses is to use cloud computing rather than local computing resources to expand current and future computing needs. As an IT technician, you need to understand how cloud computing works and how to support it.

8-6a Deployment Models for Cloud Computing

Core 1 Objective

- 4.1

Summarize cloud-computing concepts.

Cloud computing services are delivered by a variety of deployment models, depending on who manages the cloud and who has access to it. The main deployment models you are likely to encounter are as follows:

- **Public cloud.** In a **public cloud**, services are provided over the Internet to the general public. Google or Yahoo! email services are examples of public cloud deployment.
- **Private cloud.** In a **private cloud**, services are established on an organization's own servers or established virtually for a single organization's private use. For example, an insurance company might have a centralized data center that provides private cloud services to its branch offices throughout the United States.
- **Community cloud.** In a **community cloud**, services are shared among multiple organizations with a common interest, but the services are not available publicly. For example, a medical database might be shared among all hospitals in a geographic area, or government agencies might share regulatory requirements. In these cases, the community cloud could be hosted internally by one or more of the organizations involved or hosted externally by a third-party provider.

- **Hybrid cloud.** A **hybrid cloud** is a combination of public, private, and community clouds used by the same organization. For example, a company might store inventory databases in a private cloud but use a public cloud email service.

8-6b Characteristics of Cloud Computing

Core 1 Objective

- 4.1

Summarize cloud-computing concepts.

Regardless of the service provided, all cloud computing service models incorporate the following elements:

- **Elastic services and storage. Rapid elasticity** refers to the service's ability to be scaled up or down as the need level changes for a particular customer without requiring hardware changes that could be costly for the customer. Layers of services—such as applications, storage space, or number of users—can be added or removed when requested. Services can also be adjusted automatically, depending on the options made available by the service vendor.
- **Metered utilization.** Resources offered by a cloud computing vendor—such as storage, applications, bandwidth, and other services—are measured, or **metered**, for billing purposes and/or for the purpose of limiting any customer's use of that resource according to the service agreement.
- **Shared resources.** By enabling multiple customers to share the use and cost of cloud resources, a cloud service provider assists in reducing the cost of ownership for themselves and their customers.
- **High availability.** Cloud resources are considered highly available because they can be configured and turned on at a moment's notice. These services can be replicated, or copied, to data centers around the globe to ensure they are available even if one data center suffers an outage.
- **File synchronization.** Just as the services within the cloud are highly available, data files can be synchronized across the network to ensure all systems and users are working with the same versions of the same files.

8-6c Cloud Computing Service Models

Core 1 Objectives

- 2.2

  Compare and contrast common networking hardware.

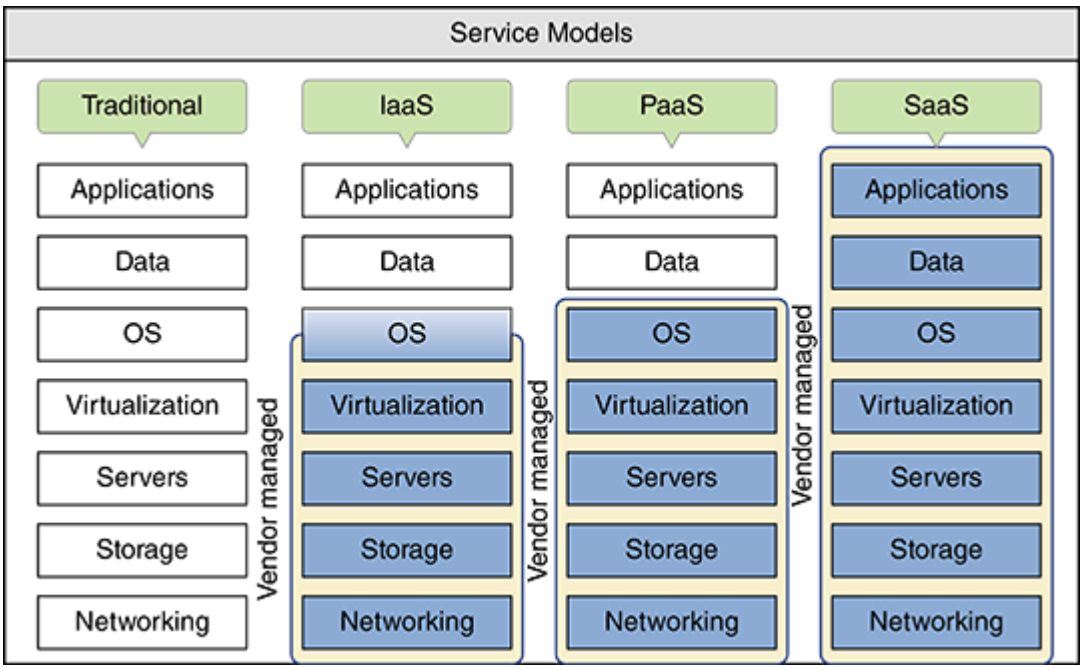
- 4.1

  Summarize cloud-computing concepts.

  Cloud computing service models are categorized by the types of services they provide. The National Institute of Standards and Technology (NIST) has developed a standard definition for each category, which varies by the division of labor implemented. For example, as shown on the left side of Figure 8-60, an organization is traditionally responsible for its entire network, top to bottom. In this arrangement, the organization has its own network infrastructure devices, manages its own network services and data storage, and purchases licenses for its own operating systems and applications. The three cloud computing service models illustrated on the right side of Figure 8-60 incrementally increase the amount of management responsibilities outsourced to cloud computing vendors.

Figure 8-60

At each progressive level, the vendor takes over more computing responsibility for the customer



The following list describes these service models:

- **IaaS.** With **IaaS (Infrastructure as a Service)**, the customer rents hardware—including servers, storage, and networking—and can use these hardware services virtually. Customers are responsible for their own application installations, data management, and backup. In most situations, customers are also responsible for their own operating systems. For example, customers might rent several VMs and use them for servers by installing an OS in each VM and hosting applications such as web servers, email servers, DNS servers, or DHCP services, or by hosting productivity software such as Microsoft Office for employees. IaaS is ideal for fast-changing applications, to test software, or for startup businesses looking to save money by not having to invest in hardware. Examples of IaaS providers are Amazon Web Services (aws.amazon.com), Windows Azure (azure.microsoft.com), and Google Compute Engine (cloud.google.com).
- **PaaS.** With **PaaS (Platform as a Service)**, a customer rents hardware, operating systems, and some applications that might support other applications the customer may install. PaaS is popular with software developers who require access to multiple platforms during the development process. A developer can build and test an application on a PaaS virtual machine made available over the web, and then throw out the machine and start over with a new one with a few clicks in their browser window. Applications that a PaaS vendor might provide to a developer are tailored to the specific needs of the project, such as an application to manage a database of test data. Examples of PaaS services include Google Cloud Platform and Microsoft Azure.
- **SaaS.** With **SaaS (Software as a Service)**, customers use applications hosted on the service provider's hardware and operating systems, and typically access the applications through a web browser. Applications are provided through an online user interface and are compatible with a multitude of devices and operating systems. Online email services, such as Gmail and Yahoo!, are good examples of SaaS. Google offers an entire suite of virtual software applications through Google Cloud and its other embedded products. Except for the interface itself (the device and whatever browser software is required to access the website), the vendor provides every level of support from network infrastructure through data storage and application implementation.
- **XaaS.** In the **XaaS (Anything as a Service or Everything as a Service)** model, the "X" represents an unknown, just as it does in algebra. Here, the cloud can provide any combination of functions, depending on a customer's exact needs. The XaaS model is not shown in Figure 8-60.

As you have seen in this module, networks can be small and housed within a single building or extend around the globe, like the Internet. You can use various types of hardware and cables to set up, manage, and expand your network to meet your changing requirements. Expanding your software systems using virtualization and the cloud can also help you meet those changing needs.

8-7a Module Summary

Types of Networks and Network Connections

- Networks are categorized by size as a PAN, LAN, WLAN, MAN, or WAN. A SAN is a specialized, high-speed network for storing and sharing files.
- Performance of a network technology is measured in bandwidth and latency.
- Ways to connect to the Internet include satellite, fiber optic, cable, DSL, cellular, and WISP.

Identifying Network Hardware and Infrastructure

- Networking hardware used on local networks can include switches, routers, wireless access points, cables, and connectors.
- Switches can be unmanaged or managed, which allows for configuration.
- Most wired local networks use twisted-pair cabling that can be unshielded twisted-pair (UTP) cable or shielded twisted-pair (STP) cable. Twisted-pair cable is rated by category, with the most common being CAT-5, CAT-5e, CAT-6, and CAT-6A.
- Fiber-optic cables can use one of the following connectors: ST, LC, or SC. Connectors should be selected to match the equipment being connected.
- Power over Ethernet (PoE) sends power over Ethernet cables for supported devices.
- IoT devices increase quality of life and convenience by connecting home and appliances to the Internet.
- SDN, SCADA systems, UTM technologies, and load balancers all can be integrated into a network to expand its functionality, increase security monitoring, and optimize the availability of the network.

Configuring Network Infrastructure

- Tools used to manage and troubleshoot network wiring and connectors include a loopback plug, cable tester, Wi-Fi analyzer, toner probe, cable stripper, crimper, punchdown tool, and network tap.
- The RJ-45 connector has eight pins. Four pins (pins 1, 2, 3, and 6) are used to transmit and receive data using the 10BaseT and 100BaseT speeds. Using 1000BaseT speed, all eight pins are used for transmitting and receiving data.
- Two standards used to wire network cables are T568A and T568B. The difference between the two standards is that the orange twisted-pair wires are reversed in the RJ-45 connector from the green twisted-pair wires.
- Either T568A or T568B can be used to wire a network. To avoid confusion, don’t mix the two standards in a building.
- Use wire strippers, wire cutters, and a crimper to make network cables. A punchdown tool is used to terminate cables in a patch panel or keystone RJ-45 jack. Be sure to use a cable tester to test or certify a cable you have just made.

- Wi-Fi, or wireless fidelity, networking uses radio frequencies to transmit and receive data between the wireless access point and the device connected to the network.

Troubleshooting Network Connections

- Common issues of networks include limited or slow connectivity, port flapping, jitter or latency issues, quality of service issues for VoIP connections, and interference issues for wireless networks.
- Troubleshooting steps should include checking hardware and software configurations, allocation of bandwidth for high QoS services such as VoIP, and monitoring for interference from other networks or devices that are nearby.

Client-Side Virtualization

- Client-side virtualization is done by creating multiple virtual machines, each with its own virtual desktop, on a physical machine using a hypervisor.
- Virtualization can be used to allow for cross-platform virtualization, for application virtualization for support, or even to set up a sandbox environment to experiment with different operating systems or develop software.
- Considerations for virtualized systems include ensuring enough physical hardware resources are allocated for each virtual machine and ensuring the environment is maintained securely.

Cloud Computing

- Cloud computing is providing computing resources over the Internet to customers.
- A public cloud service is available to the public, and a private cloud service is kept on an organization's own servers or made available by a vendor only for a single organization's private use. A community cloud is shared between multiple organizations, and a hybrid cloud is any combination of these deployment models.
- All cloud computing service models incorporate rapid elasticity, metered utilization, resource sharing, high availability, and file synchronization.
- Cloud computing service models—including IaaS, PaaS, SaaS, and XaaS—are categorized by the types of services they provide and the degree that a third-party service or vendor is responsible for the resources.

8-7c Thinking Critically

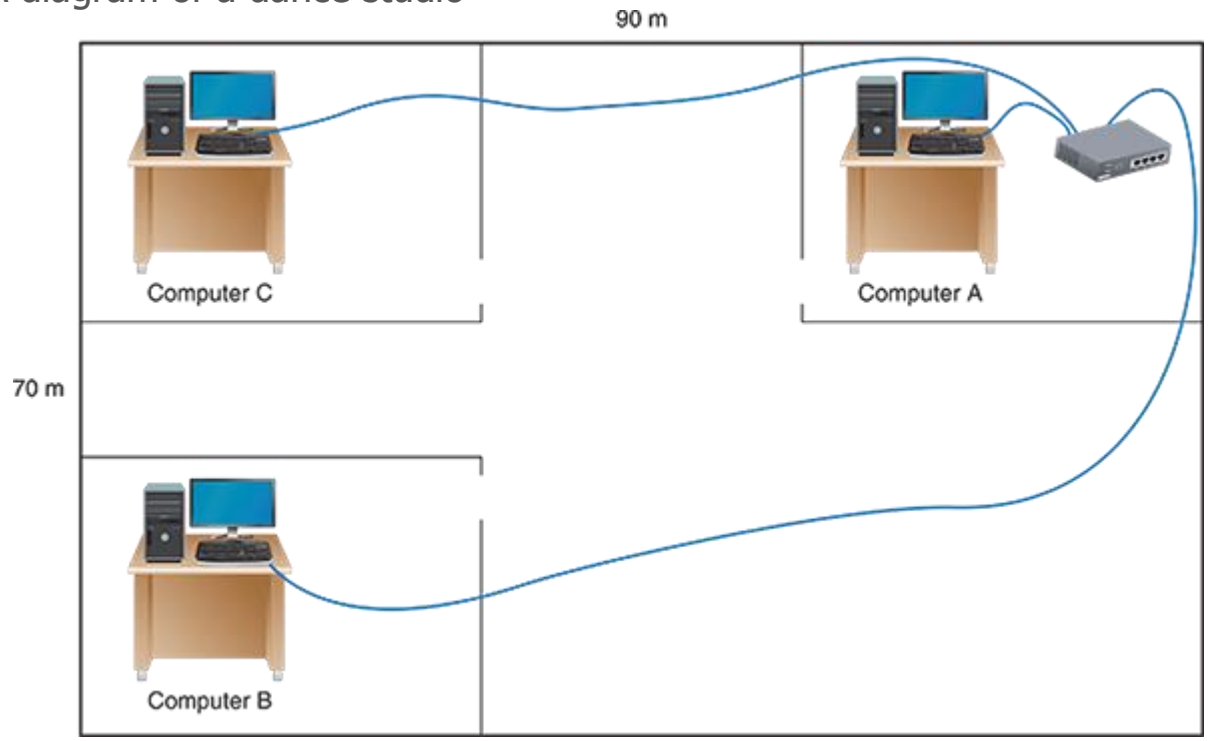
These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. Your customer, Miranda, recently installed a new router in her dance studio, as shown in the diagram in Figure 8-61. She then ran Ethernet cables through the drop ceiling to computers in various offices. Without any further testing, which computers do you suspect are experiencing connection problems? (Choose all that apply.)

    1. Computer A
    2. Computer B
    3. Computer C
    4. None of the answers are correct

Figure 8-61

A diagram of a dance studio



2. Which of the following tools can be used to determine if a network cable is good? (Choose all that apply.)

    1. Cable tester
    2. Crimper
    3. Loopback plug
    4. Patch panel

3. You've been hired to help with installing cable at a new office building for the local college. You're wiring a connection into the first room on your list. List the colors of the wires in the order you should place them into the connector, starting with pin 1.

4. You're setting up some VMs to test an application you're considering making available to employees of the small company you work for. You need to test the app in a variety of OSs, and you don't expect to need these VMs after testing is complete. You'd like setup to be as simple and straightforward as possible without needing to make any changes to the servers on your network. Which of these hypervisors will best serve your needs?

    1. XenServer
    2. Client Hyper-V
    3. Hyper-V
    4. ESXi

5. You have three VMs running on a Windows 10 computer. Two of the VMs—machines A and B—can communicate with the Internet and other network resources, as is the host

Windows 10 machine. However, one VM, machine C, cannot access websites on the Internet. What is the first component you check? The second component?

1. The host machine's network adapter
2. The switch connected to the host machine
3. VM C's virtual NIC
4. The host machine's hypervisor settings

6. You're installing VirtualBox on a Windows 10 Home computer, and you get the following error message:

```
VT-x is disabled in the BIOS for all CPU modes
```

1. What is the problem?
2. How do you fix it?

7. Which component in a thin client might need a higher rating than other components?

1. The CPU, because most of the processing is done on the thin client
2. RAM, because the system must have enough to hold a virtual desktop
3. The hard drive, because a VM takes up a large amount of hard drive space
4. The NIC, because most of the processing is done on the server

8. Your manager has instructed you to set up a virtualization workstation that will provide help desk users with access to Windows 10 Pro and Home, Ubuntu Desktop, Linux Mint, and Android Oreo and Pie. They also want you to use Client Hyper-V as the hypervisor. In what order should you install the operating systems and hypervisor?

1. Ubuntu Desktop, Client Hyper-V, remaining OSs in VMs
2. Client Hyper-V, Windows 10 Pro, remaining OSs in VMs
3. Client Hyper-V, OSs in VMs
4. Windows 10 Pro, Client Hyper-V, remaining OSs in VMs

9. You work for a small startup company that just hired five new employees, doubling its number of team members. In preparation for the new employees' first day in the office, you add five new user accounts to your CRM (customer relationship management) software subscription, a service that is hosted in the cloud. What aspect of cloud computing has worked to your advantage?

1. High availability
2. Rapid elasticity
3. Metered service
4. Resource pooling

10. Doctors at a regional hospital access an online database of patient records that is being developed and tested by a conglomerate of health insurance agencies. The database contains records of hundreds of thousands of patients and is regulated by HIPAA restrictions on protected health information (PHI). What kind of cloud deployment is this database?

11. Office 365 is an example of what type of cloud computing service model?

1. IaaS
2. Application streaming

3. PaaS
4. SaaS

12. Which of the following resources are shared between the host computer and a VM? (Choose all that apply.)

1. NIC
2. Operating system
3. Hard drive
4. Applications

13. A friend of yours is having trouble getting good Internet service. They say their house is too remote for cable TV, and they don't even have a telephone line to their house. They have been very frustrated with satellite service because storms and even cloudy skies can disrupt the signal. They use Verizon for their cell phone, which gets good signal at the house. What Internet service would you recommend they look into getting for their home network?

1. Dial-up
2. LTE installed Internet
3. DSL
4. Cable Internet

14. You recently installed a SOHO router in a customer's home, and the owner has called to say their child is complaining that Internet gaming is too slow on their wireless laptop. Which possibilities should you consider to speed up the gaming experience? (Choose all that apply.)

1. Verify that the wireless connection is using the fastest wireless standard the router supports.
2. Disable encryption on the wireless network to speed up transmissions.
3. Suggest they use a wired Gigabit Ethernet connection to the network for gaming.
4. Enable IPv6 for the laptop.

15. Which of the following tools can be used to monitor network traffic by a monitoring system such as an IDS or IPS?

1. Crimper
2. Tone generator and probe
3. Cable tester
4. Network tap

16. A power-over-Ethernet (PoE) switch provides power to end devices. What is the maximum voltage provided by a PoE+ switch port to the device?

1. 25.5 watts
2. 17 watts
3. 34 watts
4. 15.4 watts

17. Cable and fiber-optic modems are increasing in popularity with ISPs across the United States. While these are great for stationary connections to the Internet, travelers need another option for connectivity. Which of the following can provide a cost-effective solution for connectivity?

1. Satellite
2. Long-range fixed wireless
3. Cellular WAN
4. DSL

18. Alicía is having trouble browsing the Internet on the wireless network from the employee lunchroom on her lunch break. You check her connection, and it appears that the connection works for a few minutes but then disconnects. The NIC settings show the correct IP address and Wi-Fi settings, but you continue to see the up/down on the connection. Which of the following could best explain why Alicía is having problems?

1. The wireless NIC is broken.
2. The WAP is configured wrong.
3. The microwave in the lunchroom is causing interference.
4. The computer OS needs upgrades.

Main content

Module Review

8-7d

Hands-On Projects

Hands-On Project 8-1

Researching a Network Upgrade

- **Est. Time:** 30 minutes
- **Core 1 Objectives:** 2.2,2.3,2.7,3.1

An IT support technician is often called on to research equipment to maintain or improve a computer or network and make recommendations for purchase. Suppose you are asked to upgrade a small network that consists of one switch and four computers from 100BaseT to Gigabit Ethernet. The switch connects to a router that already supports Gigabit Ethernet. Do the following to price the hardware needed for this upgrade:

1. Find three switches by different manufacturers that support Gigabit Ethernet and have at least five ports. Save or print the webpages describing each switch.
2. Compare the features and prices of the three switches. What additional information might you want to know before you make your recommendation for a small business network?
3. Find three network adapters by different manufacturers to install in the desktop computers to support Gigabit Ethernet. Save or print webpages for each NIC.
4. Compare features of the three network adapters. What additional information do you need to know before you make your recommendation?
5. Make your recommendations based on the moderate (middle-of-the-road) choices. What is the total price of the upgrade, including one switch and four network adapters?
6. What is one more question you need to have answered about other equipment before you can complete the price of the upgrade? Explain how you would find the answer to your question.

Hands-On Project 8-2

Wiring a Keystone Jack

- **Est. Time:** 15 minutes
- **Core 1 Objectives:** 2.8,3.1

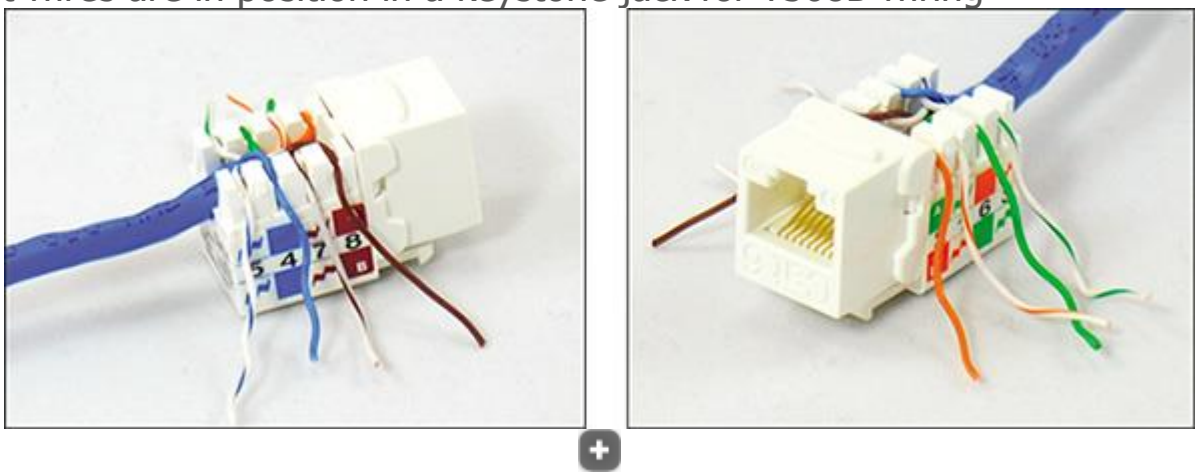
A keystone RJ-45 jack is used in a network wall jack. To practice wiring a keystone jack, you'll need a wire stripper, wire cutter, twisted-pair cabling, keystone jack, and punchdown tool. Here are the instructions to wire a keystone jack:

1. 1
   Using a wire stripper and wire cutter, strip and trim back the jacket from the twisted-pair wire, leaving about two inches of wire exposed. Untwist the wires only so far as necessary so each wire can be inserted in the color-coded slot in the jack. The untwisted wire should be no longer than a half inch. Why are twists so important when wiring connectors and jacks?

2. 2
   Insert each wire into the appropriate slots for either the T568A or the T568B standard, depending on the network where you might use this keystone jack. Figure 8-62 shows the wires in position for T568B wiring. Notice how the cable jacket goes into the keystone jack. Which wiring standard did you use? How did you choose that standard?

Figure 8-62

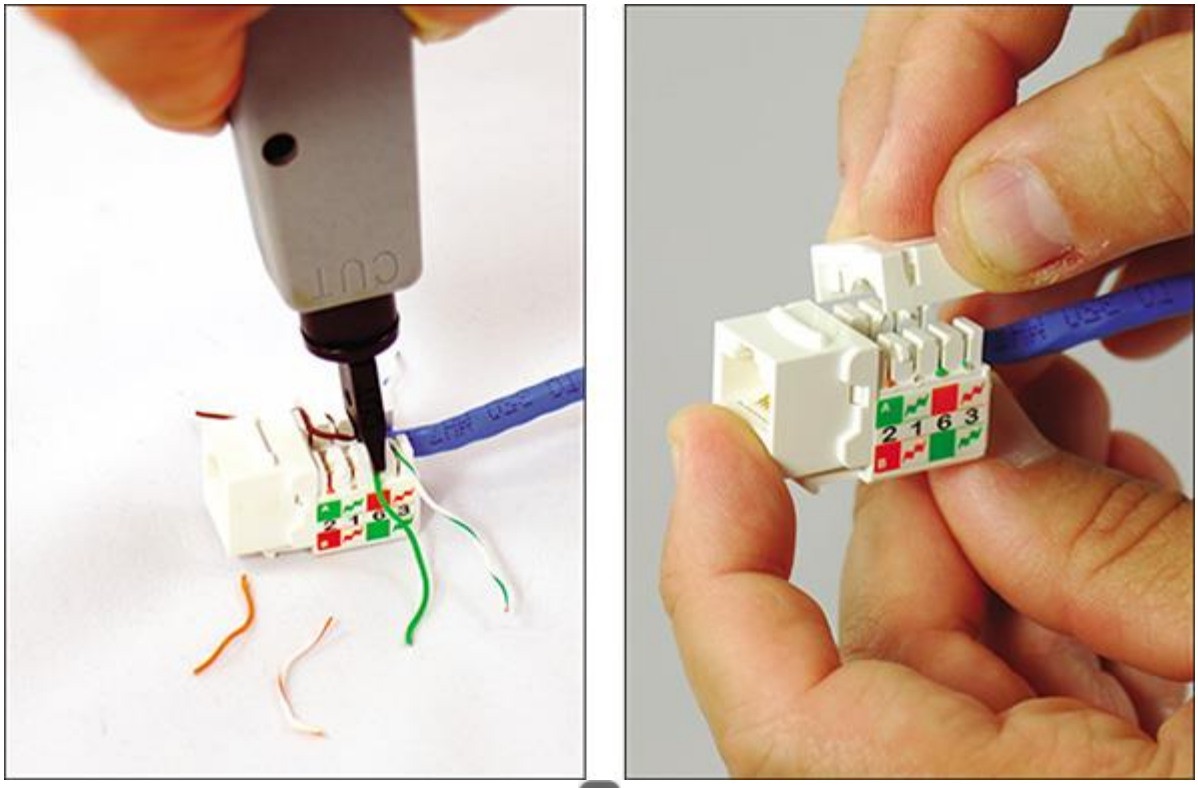
Eight wires are in position in a keystone jack for T568B wiring



3. 3
   Using the punchdown tool, make sure the blade side of the tool is on the outside of the jack. (The punchdown tool has "Cut" embedded on the blade side of the tool.) Push down with force to punch each wire into its slot and cut off the wire on the outside edge of the slot. It might take a couple of punches to do the job. See the left side of Figure 8-63. Place the jack cover over the jack, as shown on the right side of Figure 8-63.

Figure 8-63

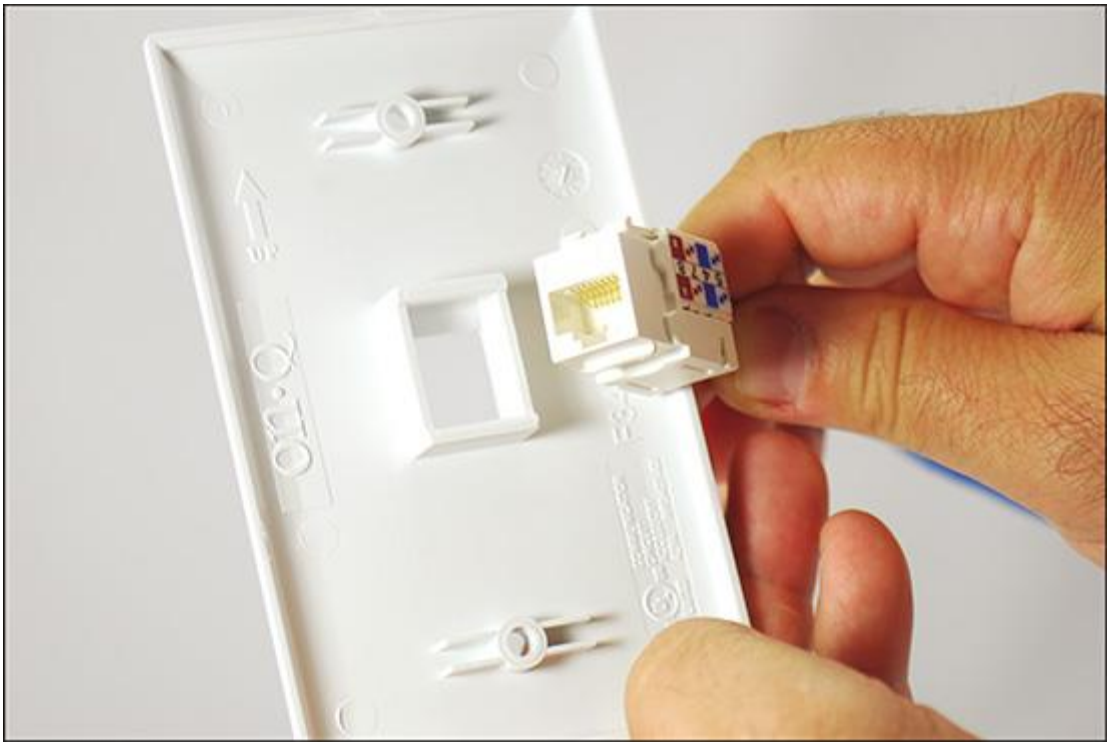
Use a punchdown tool to punch the wires into the keystone jack, and then place the cover in position



4. 4
   The jack can now be inserted into the back side of a wall faceplate (see Figure 8-64). Make sure the wires in the jack are at the top of the jack. If you look closely at the faceplate, you can see the arrow pointing up. It's important that the wires in the jack be at the top so dust doesn't settle on these wires over time. Use screws to secure the faceplate to the wall receptacle. Be sure to use a cable tester to check the network cable from its jack to the other end to make sure the wiring is good. When wiring a building, testing the cable and its two connections is called certifying the cable. Use a loopback plug or cable tester with cable to verify your jack works. Is it certified?

Figure 8-64

Insert the jack in the faceplate, making sure the wire connectors are at the top of the jack



Note 8

To see a video by DIY Telecom of using a punchdown tool to make an RJ-45 keystone jack, see youtube.com/watch?v=Xkbz-uywLJs.

Hands-On Project 8-3

Making Network Cables

- **Est. Time:** 15 minutes
- **Core 1 Objectives:** 2.8,3.1

Using the tools and skills you learned about in this module, practice making a straight-through cable and a crossover cable. Use a cable tester to test both cables.

Answer the following questions:

1. Which wiring standard did you use for the straight-through cable? List the pinouts (pin number and wire color) for each of the eight pins on each connector.
2. Will your crossover cable work on a Gigabit Ethernet network? List the pinouts (pin number and wire color) for each of the eight pins on each connector.

Hands-On Project 8-4

Using Google Cloud

- **Est. Time:** 45 minutes
- **Core 1 Objective:** 4.1

Google Cloud Platform is an example of a PaaS. To use the service, do the following:

1. 1

Go to cloud.google.com and click **Get Started for Free**. You will need to sign in using a Google account. If you don't have an account, you can create one with any valid email address. When you first set up an account, you must enter payment information, which Google promises not to use during your free trial period. Create an individual account type, enter your information, and click **START MY FREE TRIAL**.

2. 2
   You begin on the Getting started page for your first project, aptly named "My First Project." Click **COMPUTER ENGINE**, and, if necessary, click the **ENABLE button**. When the system is ready, click **CREATE INSTANCE** in the VM instances box to create a VM. Use the default settings, except the following:

   1. Change the name of the VM to dcserver.
   2. Change the Boot disk to **Windows Server 2019 Datacenter**.

3. 3
   Click **Select**, and then click **Create**. Wait for Google to create the instance.

Note 9

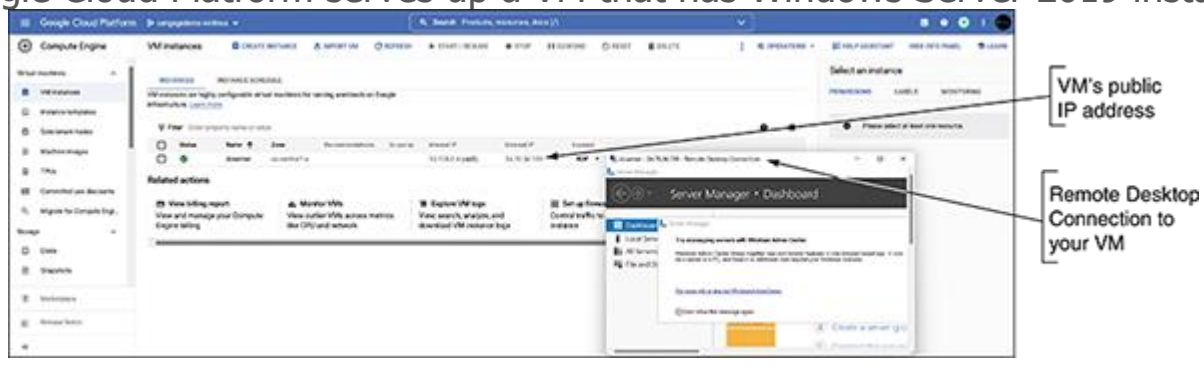
The Microsoft Windows OS selections are not part of the free tier of the Google Cloud Platform. If you want to complete this activity without incurring any associated cost, choose one of the Linux distributions, such as Ubuntu, from the list instead of a Windows OS. All other instructions will still apply. Additional information on costs associated with the Google Cloud Platform can be found at https://cloud.google.com/free/docs/gcp-free-tier/#compute.

1. 4
   In the VM instances list, click the **dcserver** instance, which takes you to the VM instance details page. Click **Set Windows password**, and assign a user name to your VM instance. Note the user name, and click **SET**. Google Cloud assigns a password, which displays on-screen. Copy the password, save it somewhere safe, and then click **CLOSE**.

2. 5
   Note the External IP assigned to the VM instance under the Network Interfaces section, shown near the center of Figure 8-65.

Figure 8-65

Google Cloud Platform serves up a VM that has Windows Server 2019 installed



3. 6
   On your computer, you can use Remote Desktop with screen and file sharing to access your VM. Follow these steps:

   1. Enter the `mstsc` command in the Windows 10 search box. In the Remote Desktop Connection dialog box, enter the External IP address of your VM, which is its public IP address available on the Internet. Click **Connect**.
   2. In the *Enter your credentials* box, your Windows user name appears. If your VM's user name is not the same as your Windows user name, click **More choices** and then click **Use a different account**. You can then enter the VM's user name and password. Click **OK** to connect.

   The bottom window in Figure 8-65 shows the VM in a Remote Desktop Connection window. This Windows Server setup screen is the first screen that appears immediately after the first restart when you've installed Windows Server 2019. Take a few minutes to explore your Windows Server VM.

4. 7
   To avoid accumulating any charges against your free quota, shut down the server VM in the Remote Desktop Connection window. You learn more about Remote Desktop in the module "Network Security and Troubleshooting."

Note 10

You will use the Google Cloud Platform service for other projects in the modules "Securing and Sharing Windows Resources" and "Linux and Scripting." Do not disable your Google Cloud Platform account until after you have completed these projects.

Main content

Module Review

8-7e Real Problems, Real Solutions

Real Problem 8-1

Preparing a Quote for Network Solutions

- **Est. Time:** 30 minutes
- **Core 1 Objectives:** 2.2,2.3,3.1

As a computer and networking consultant to small businesses, you are frequently asked to find solutions to increasing demands for network and Internet access at a business. One business rents offices in a historical building that has strict rules for wiring. They have come to you asking for a solution for providing Wi-Fi access to their guests in the lobby of the building. Research options for a solution and answer the following questions:

1. Print or save webpages showing two options for a Wi-Fi wireless access point (WAP) that can mount on the wall or ceiling. For one option, select a device that can receive its

power by PoE from the network cable run to the device. For the other option, select a device that requires an electrical cable as well as a network cable to the device.
2. Print or save two webpages for a splitter that can be mounted near the second wireless access point and that splits the power from data on the network cable. Make sure the power connectors for the splitter and the access point can work together.
3. To provide PoE on the network cable from the electrical closet to the wireless access point, you can use an injector that injects power into a network cable. Print or save the webpage for such an injector, making sure the voltage and wattage output for the injector are compatible with the needs of both wireless access points.
4. The distance for network cabling from the switch to the wireless access point is about 200 feet (61 meters). What is the cost of 200 feet of PVC CAT-6a cabling? For 200 feet of plenum CAT-6a cabling?
5. Of the options you researched, which do you recommend? Using this option, what is the total cost of the Wi-Fi hotspot?

Real Problem 8-2

Exploring Packet Tracer

- **Est. Time:** 45 minutes
- **Core 1 Objective:** 2.8

In the module "Networking Fundamentals," you installed Packet Tracer and created a very basic network. In this project, you work through three modules of the Packet Tracer Introduction course to take a brief tour of the simulator interface and create a more complex network in Packet Tracer. Notice in the Packet Tracer course that the activities refer to the OSI model instead of the TCP/IP model. Review the section titled "The OSI Model for Network Communication" in the module "Networking Fundamentals" for a brief refresher. Then complete the following steps to access your course:

1. 1
   Return to the Networking Academy website (netacad.com), sign in, and click **Launch Course**. You've already downloaded Packet Tracer, so you can skip chapter 1.

2. 2
   Complete chapters 2, 3, and 4, including the videos and labs, and complete the Packet Tracer Basics Quiz at the end of chapter 4. The other remaining chapters provide excellent information on Packet Tracer but are not required for this project. Answer the following questions along the way:

   1. What is a simple PDU in Packet Tracer?
   2. What is a .pka file?
   3. Which Packet Tracer feature do you think will be most helpful for you in learning how to manage a network?

SOHO router devices offer a lot of options for security, efficiency, and convenience. These features are easy to configure on a consumer grade device—if you know what they are and when to use them. Enterprise-grade devices have similar settings that control how computers can gain access to a network, what they can do while they're on the network, and how the data on the network is managed.
