13

Networking

In this chapter you will learn:

> To identify common network cables and connectors

> About Ethernet networks

> About the OSI and TCP/IP models, different networking protocols, differences between TCP and UDP, and important TCP or UDP port numbers

> To identify MAC, IPv4, and IPv6 addresses

> To set up wired and wireless networks

> Common network troubleshooting tools

> To configure and access a network printer

> Important network servers

> The basics of SDN

> To share data using a network

> How to be a proactive technician

CompTIA Exam Objectives:

✓ 1101-2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

✓ 1101-2.2 Compare and contrast common networking

✓ 1101-2.3 Compare and contrast protocols for wireless

✓ 1101-2.4 Summarize the services provided by networ

- ✓ 1101-2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
- ✓ 1101-2.6 Compare and contrast common network configuration concepts.
- ✓ 1101-2.7 Compare and contrast Internet connection types, network types, and their features.
- ✓ 1101-2.8 Given a scenario, use networking tools.
- ✓ 1101-3.1 Explain basic cable types and their connectors, features, and purposes.
- ✓ 1101-3.4 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1101-3.6 Given a scenario, deploy and configure multifunction devices/printers and settings.
- ✓ 1101-5.5 Given a scenario, troubleshoot common issues with mobile devices.
- ✓ 1101-5.7 Given a scenario, troubleshoot problems with wired and wireless networks.
- ✓ 1102-1.1 Identify basic features of Microsoft Windows editions.
- ✓ 1102-1.2 Given a scenario, use the appropriate Microsoft command-line tool.
- ✓ 1102-1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
- ✓ 1102-1.5 Given a scenario, use the appropriate Windows settings.
- ✓ 1102-1.6 Given a scenario, configure Microsoft Windo tures on a client/desktop.
- ✓ 1102-2.1 Fassen Sie verschiedene Sicherheitsmaßnah Zwecke zusammen.

- ✓ 1102-2.2 Vergleichen und kontrastieren Sie drahtlose Sicherheitsprotokolle und Authentifizierungsmethoden.

- ✓ 1102-2.9 Konfigurieren Sie in einem bestimmten Szenario die entsprechenden Sicherheitseinstellungen in drahtlosen und kabelgebundenen Netzwerken (Small Office/Home Office).

- ✓ 1102-3.2 Behandeln Sie in einem bestimmten Szenario häufige Sicherheitsprobleme für PCs (PC).

- ✓ 1102-3.4 Behandeln Sie in einem bestimmten Szenario häufige Probleme mit mobilen Betriebssystemen und Anwendungen.

Netzwerkübersicht

Netzwerke sind überall um uns herum. Einige Beispiele sind die folgenden:

- Ein Netz von Straßen und Autobahnen
- Ein Telefonnetz
- Das Stromnetz, das unsere Häuser mit Strom versorgt
- Das Mobilfunknetz, das es Mobiltelefonen / Smartphones ermöglicht, sich untereinander sowie mit dem kabelgebundenen Telefonnetz und dem Internet zu verbinden
- Das Flugsicherungsnetz
- Ihr Netzwerk von Freunden und Familie

Ein Netzwerk in Bezug auf Computer besteht aus zwei oder mehr Geräten, die miteinander kommunizieren und Ressourcen gemeinsam nutzen können. Ein Netzwerk ermöglicht es Computerbenutzern, Dateien gemeinsam zu nutzen. per E-Mail zu kommunizieren; im Internet surfen; einen Drucker oder Scanner freigeben; und greifen Sie auf Anwendungen und Dateien zu. Netzwerke können je nach Größe und Art des Netzwerks in Hauptkategorien unterteilt werden. Tabelle 13.1 beschreibt diese verschiedenen Netzwerke.

Tabelle 13.1 Arten von Netzwerken

Netzwerktyp	Beschreibung

Netzwerktyp	Beschreibung
Persönliches Netzwerk (PAN))	Ein PAN besteht aus persönlichen Geräten wie Tastatur, Maus, Fernseher, Mobiltelefon, Laptop, Desktop, Mobilgerät und Taschenvideospielen, die in unmittelbarer Nähe über ein kabelgebundenes oder drahtloses Netzwerk kommunizieren können. Eine Bluetooth-Tastatur, die mit einem PC verbunden ist, ist ein Beispiel für ein PAN.
Lokales Netzwerk (LAN))	Ein LAN ist eine Gruppe von Geräten, die Ressourcen in einem einzelnen Bereich, z. B. in einem Raum, zu Hause oder in einem Gebäude, gemeinsam nutzen können. Die gebräuchlichste LAN-Technologie ist Ethernet. Die Computer in einem kabelgebundenen vernetzten Klassenzimmer sind ein Beispiel für ein LAN.
Wireless LAN (WLAN)	Ein drahtloses Netzwerk wird in Heim- und Geschäftsnetzwerken verwendet und umfasst Geräte wie Laptops, Tablets, Smartphones und Smart-Home-Geräte, die Daten über die Luft übertragen. Eine drahtlose Bridge kann verwendet werden, um Geräte zwischen zwei Gebäuden zu verbinden.
Metropolnetz (MAN))	Ein MAN bietet Konnektivität zwischen Standorten innerhalb derselben Stadt und mehreren LANs. Es kann drahtlos sein oder Glasfaserkabel verwenden. Zum Beispiel können mehrere College-Campus, die innerhalb einer Stadt verbunden sind, verbunden sein, um einen MAN zu bilden.
Wide Area Network (WAN))	Ein WAN bietet Konnektivität zwischen Standorten in großem geografischer Maßstab Standorte, die als Teil des Unterne miteinander verbunden sind, sind

Netzwerktyp	Beschreibung
Wireless WAN (WWAN)	A WWAN provides wireless connectivity for a larger geographic area, using a mix of technologies, such as cellular or long-range fixed wireless.
Wireless mesh network (WMN)	A WMN provides wireless connectivity that is especially good in emergency situations because WMNs pass data between peer radio devices and can be used over large distances.
Storage area network (SAN)	A SAN is a collection of storage devices that are used by multiple servers/network devices and centrally managed.

Let's go into a few of these network types a little deeper so the acronyms can bring visuals to your mind.

Bluetooth PAN

A PAN is a network that has components that are in close proximity to one another. The most common type of PAN uses a technology called **Bluetooth**. Bluetooth devices include audio/visual products, automotive accessories, keyboards, mice, phones, game controllers, cameras, wireless cell phone headsets, sunglasses with radios and wireless speakers, and other small wireless devices.

Bluetooth works in the 2.4 GHz range, similarly to business wireless networks. Traditional Bluetooth has three classes of devices (1, 2, and 3) that have a range of less than 30 feet (less than 10 meters), 33 feet (10 meters), and 328 feet (100 meters), respectively, and a maximum transfer rate of 24 Mbps. Bluetooth version 5 introduced a second type of Bluetooth called Bluetooth Low Energy (BLE) that supports longer distances for speeds up to 2 Mbps. Vendors tout ranges o
meters), although such distances are not defined in th
good for Internet of Things (IoT) devices such as sens
cameras, a stove, or lights within a home. The BLE sta

patible with the classic Bluetooth standard, but smartphones or other devices might have the capability of using both.

Up to eight Bluetooth devices can be connected in a piconet or PAN (a small network). Bluetooth has always had security features integrated into it, including 128-bit encryption (for scrambling of data). Figure 13.1 shows a Bluetooth connection between a cell phone mounted on a runner's arm and a fitness device on the wrist so that the phone app can be used to configure the device and download the activity data.

Figure 13.1 Bluetooth connectivity

A Bluetooth network provides computer-to-computer connectivity between Bluetooth devices. Each computer must support a PAN to join the network. In Windows, use *Settings* > *Devices* > *Bluetooth & other devices*. Review Chapter 10, "Mobile Devices," for complete installation steps.

LANs

LANs can be wired or wireless, but a LAN that is wireless is called a WLAN. Let's focus on the wired type first. A LAN is tw
connected via wiring. You can actually connect two d
between their NICs to form a LAN, but most LANs tod
LANs. An **Ethernet** LAN has a central device called a
Ethernet cable connects an RJ45 port on the network

or hub, as shown in Figure 13.2. The hub or switch typically has 2 to 48 ports on the front.

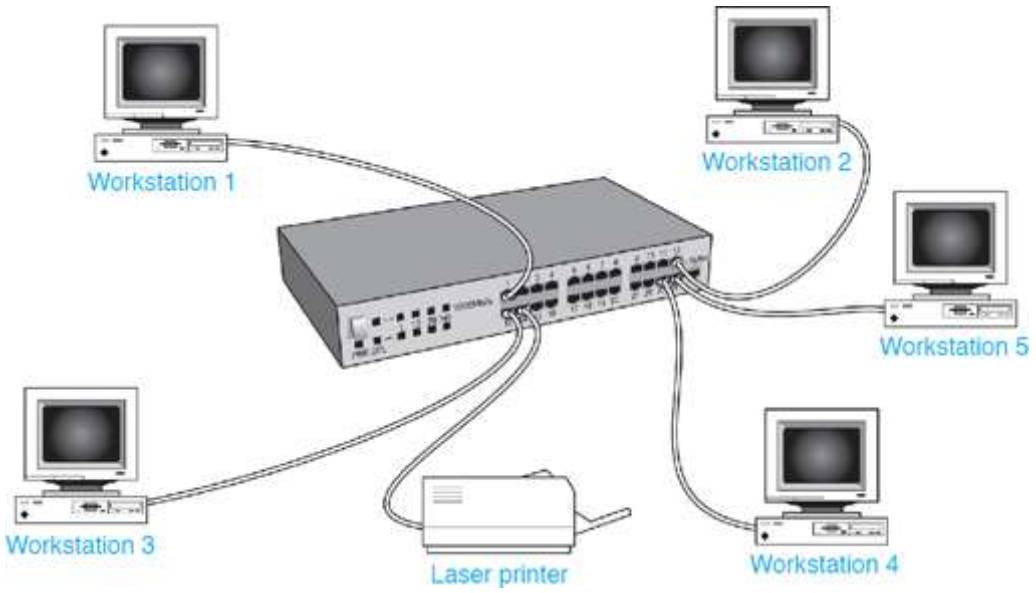


Figure 13.2 Ethernet LAN

A hub is not as intelligent as a switch. A switch examines each data frame as it comes through the switch. A hub cannot do this. You sometimes have to look at the model number/description to tell the difference between a hub and a switch because they are similar in appearance.

'ech Tip Why a switch is better than a hub

When a workstation sends data to a hub, the **hub** broadcasts the data out all ports except for the port that received the original data (the port the data came in on). A better solution is a switch. A **switch** keeps a table of addresses. When a switch receives data, the switch looks up the destination MAC address (an address burned into a NIC) in the switch table and forwards the data out the port for which it is destined.

When a hub is used, collisions may occur because two devices can place data onto the network at the same time. Every device has to delay sending data for a period of time, and then transmiss
This isn't an inefficient use of bandwidth. A switch el
and is therefore a better network device to use.

Switches can be either managed or unmanaged. A **managed switch** has an IP address assigned and can be configured, modified, and monitored through a corporate network. An **unmanaged switch** simply connects devices so that they form a network. This would be like a switch you might have in a home or small business wired network.

'ech Tip Ethernet networks are physically wired in a star

The most common network topology used today is the star topology, which is used with Ethernet networks.

In a star topology (refer to Figure 13.2), each network device has a cable that connects between the network interface card (NIC) on the device and the hub or switch. If one computer or cable fails, all other devices continue to function. However, if the hub or switch fails, the network goes down.

Star topologies are easy to troubleshoot. If one network device goes down, the problem is in the device, cable, or port on the hub/switch. If a group of network devices goes down, the problem is most likely in the device that connects them together (the hub or switch).

Table 13.2 lists the different types of Ethernet networks. In the term 100BaseT, the *100* means that the network runs at 100 Mbps. The *T* at the end of 100BaseT means that the computer uses twisted pair cable. The *1000* in 1000BaseT means that 1,000 Mbps is supported. *Base* means that the network uses baseband technology. Baseband describes data that is sent over a single channel on a single wire. In contrast, broadband is used in cable TV systems, and it allows multiple channels using different frequencies to be covered over a single wire.

Table 13.2 Ethernet standards

Ethernet type	Description
10BaseT	10 Mbps over Cat 3 or Cat 5 UTP c

Ethernet type	Description
100BaseT	100 Mbps over Cat 5 or higher UTP cable
1000BaseT	Also known as Gigabit Ethernet; 1,000 Mbps or 1 Gbps over Cat 5 or higher UTP cable
1000BaseSX	1 Gbps using multi-mode fiber (a type of cable made of plastic or glass that carries data using light)
1000BaseLX	1 Gbps using single-mode fiber
2.5G/5GBaseT	2.5 or 5 Gbps over Cat 6 or higher cable
10GBaseSR	10 Gbps over multi-mode fiber
10GBaseLX4	10 Gbps over multi-mode or single-mode fiber
10GBaseLR	10 Gbps up to 6.2 miles (10 km) using single-mode fiber
10GBaseER	10 Gbps up to 24.85 miles (40 km) using single-mode fiber
10GBaseT	10 Gbps over UTP (Cat 6 or higher) or STP cable
25GBaseLR	25 Gbps over fiber up to 6.2 miles (10 km)
25GBaseER	25 Gbps over fiber up to 24.85 miles (40 km)
40 Gigabit Ethernet	40 Gbps over single-mode fiber or 23 feet (7 m) using copper
100 Gigabit Ethernet	100 Gbps over multi-mode or sing

LANs typically are based on one of two models: a workgroup model or a domain model. A **workgroup** LAN is used in a wired home or small business network. A **domain** is used in a corporate environment and usually contains multiple networks. A domain typically contains servers, databases, and shared resources that are centrally managed. Table 13.3 compares the two types.

Table 13.3 Workgroup and domain network characteristics

Workgroup	Domain
Small number of devices (typically fewer than 20)	Typically more than 20 devices
All devices are usually on one network	Contains multiple networks
Each network device must have user accounts configured	User accounts are centrally managed
More of a security risk	Security is centrally managed with security policies applied
Might contain a web server, file server, or network-attached storage (NAS) but may have no servers	Storage is centralized, and multiple servers are usually involved
Easier to implement	Any change requires planning
Each PC uses a workstation OS	Each server requires a network operating system (NOS)
Requires fewer resources	Network resources are centralized, located in cloud based, or these

Figure 13.3 shows the type of wired and wireless connectivity used in a workgroup. Figure 13.4 shows the kind of connectivity that can be used in a network domain.

Figure 13.3 Wired and wireless connectivity in a workgroup network

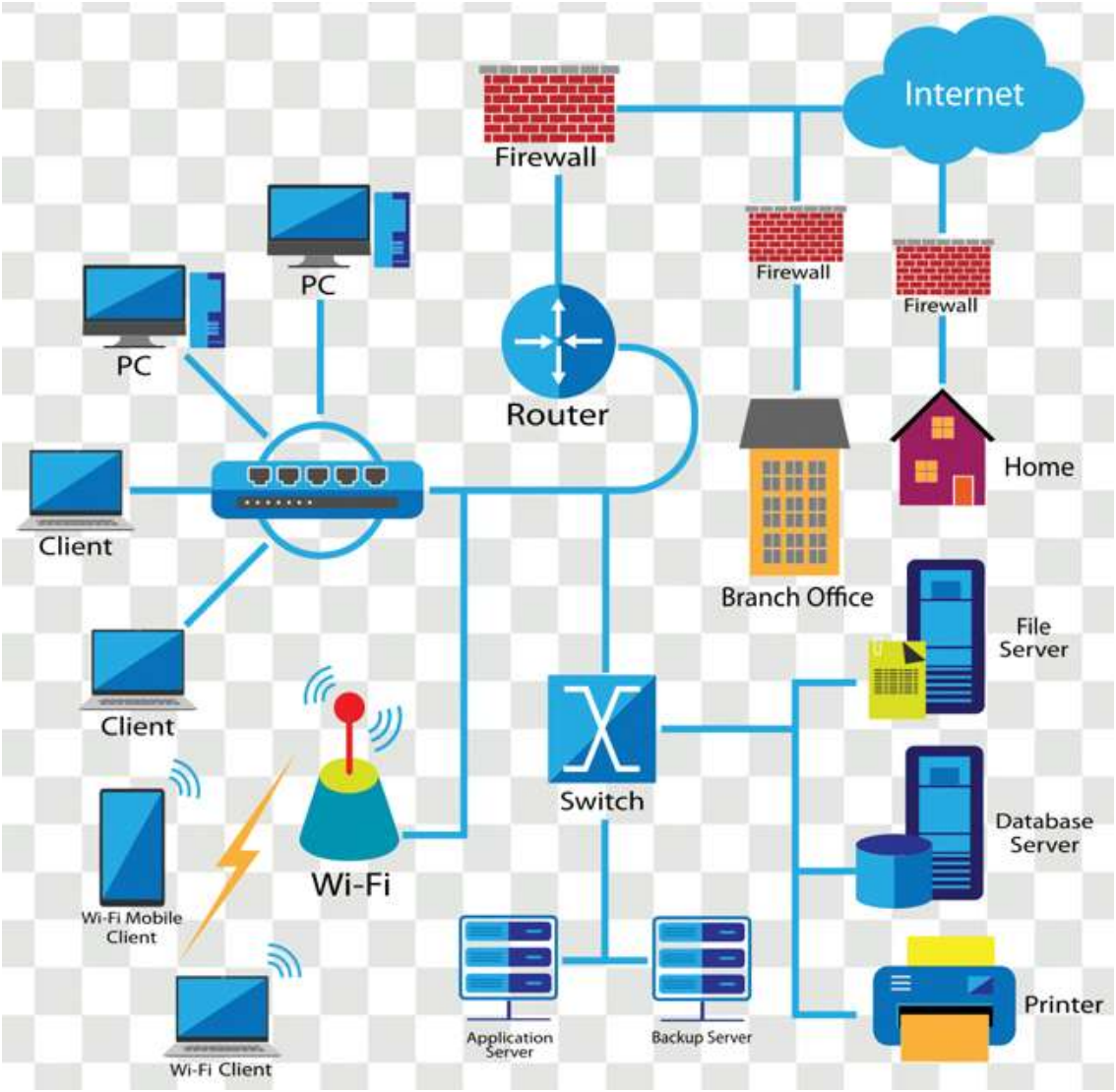


Figure 13.4 Domain network

Figure 13.5 shows the type of equipment found in a network operations center (NOC) that could be used with a domain-based network.

Figure 13.5 Network operations center (NOC)

When you attach to a wired LAN and are using a Microsoft operating system, you are presented with three or four choices, depending on the OS you are using: workgroup network, guest network, public network, private network, or domain. A home or work environment is considered a **private network**, and private addresses are used. Characteristics of your computer can be seen or discovered by other devices. A **public network** is like when you are using a computer in the community library or at a hotel. With a public network, Windows does not allow discovery of the device even though it is connected to a network. The option chosen defines, to some extent, the type of network you could configure. Table 13.4 describes the basic choices.

Table 13.4 Windows network options

Network option	Description
Workgroup	Used to configure a device participating in a small home or business network. Use the S Panel to select this option.

Network option	Description
Domain	Used to configure a device in an enterprise corporate environment where policies are enforced and deployed. Use the System Control Panel to select this option.
Private	Used when you are on a trusted network such as a home or corporate network. Use *Network & Internet* > *Ethernet* Settings option to select for a wired network or select the wireless network > *Properties* option.
Public	Used to configure a device on a network where the other devices are unknown. Network discovery is disabled. Use *Network & Internet* > *Ethernet* Settings option to select for a wired network or select the wireless network > *Properties* option.

WLANs

WLANs (sometimes called Wi-Fi networks) are popular in homes and businesses for connecting devices. WLANs connect wireless devices like phones, tablets, laptops, TVs, and smart speakers/devices, using a specific range of radio frequencies, as shown in Figure 13.6.

Figure 13.6 WLAN connectivity

SANs

A storage area network (SAN) has a large number of hard drives mounted in a unit that attaches to the network, and that storage is centrally managed. Figure 13.7 shows a person installing a server, and behind him is a SAN.

Figure 13.7 Storage area network (SAN)

If a PC needed to access data on a SAN, it could just do so through the normal LAN, but the PC might also contain a special NIC to connect to the SAN **iSCSI** or Fibre Channel (**FC**) connections (look back at Figure 2.40 in Chapter 2, "Connectivity," to see fiber connectors), as shown in Figure 13.8. Connectivity between a SAN and servers also is accomplished using these connectivity methods, as shown in Figure 13.9.

Figure 13.8 SAN fiber connectivity

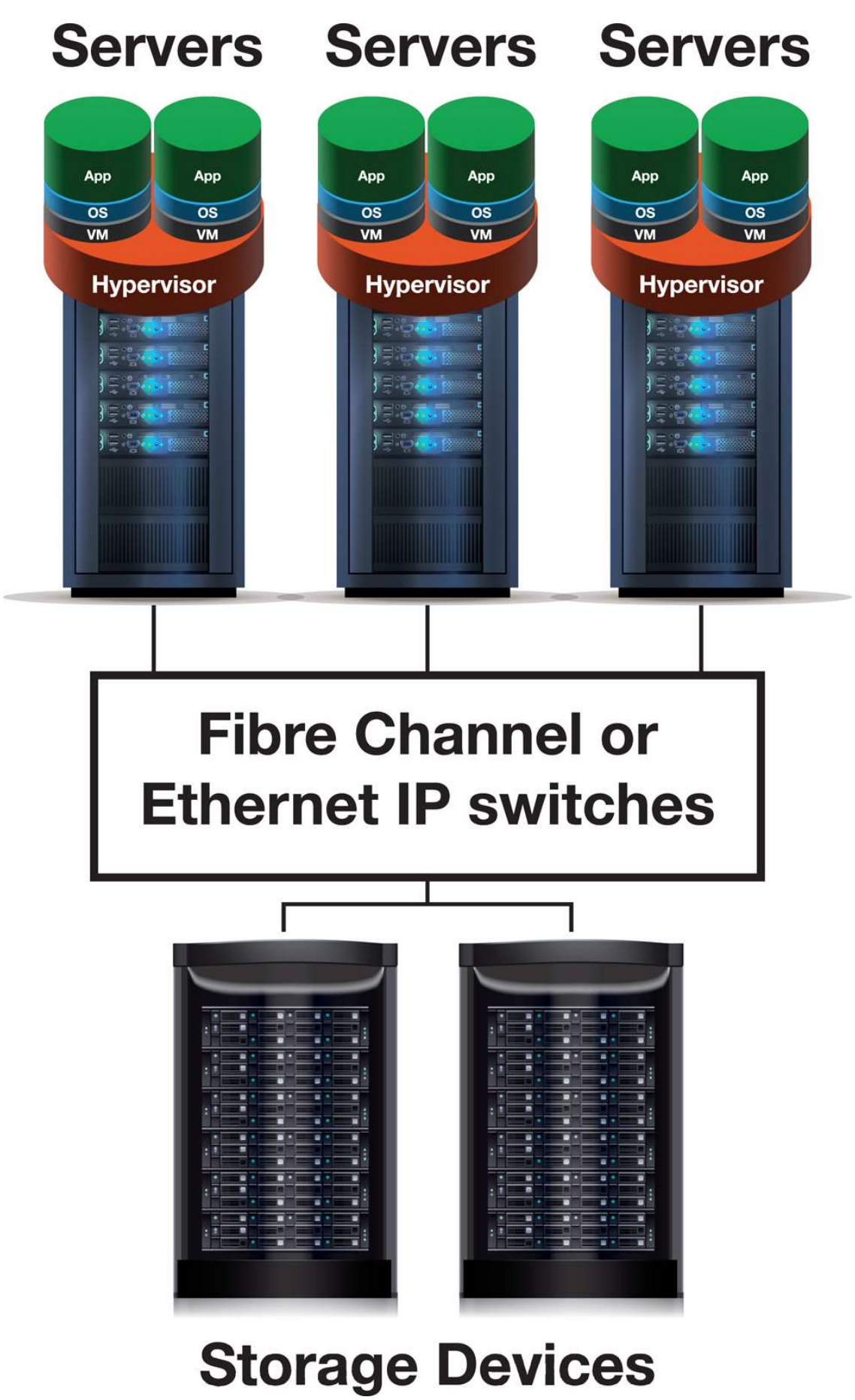


Figure 13.9 SAN connectivity to servers

Today, networks are vital to businesses. They can
many homes. A technician must have a basic underst
vices that make up networks and their roles. No matt
you are aspiring toward, you will have to deal with these concepts.

Network Media Overview

A network requires some type of medium to transmit data. This medium is normally some type of cable or air (wireless using radio, microwave, and electromagnetic signals). The most common types of cable are coax, twisted pair copper and fiber-optic cable. Air is used in wireless networking when data is sent over radio frequencies.

Copper Media

Copper media is the most common cabling used to connect devices to a network. Copper media comes in two major types: twisted pair and coaxial.

Twisted Pair Cable Overview

Twisted pair cable comes in two types: shielded and unshielded. The acronyms used with this type of cable are STP (shielded twisted pair) and UTP (unshielded twisted pair). The most common type of copper media used with computer networking and phone cabling is **UTP** cable. **Twisted pair cable** has four pairs of conductors entwined around each other—hence its name. Figure 13.10 shows the physical properties of an unshielded twisted pair cable.

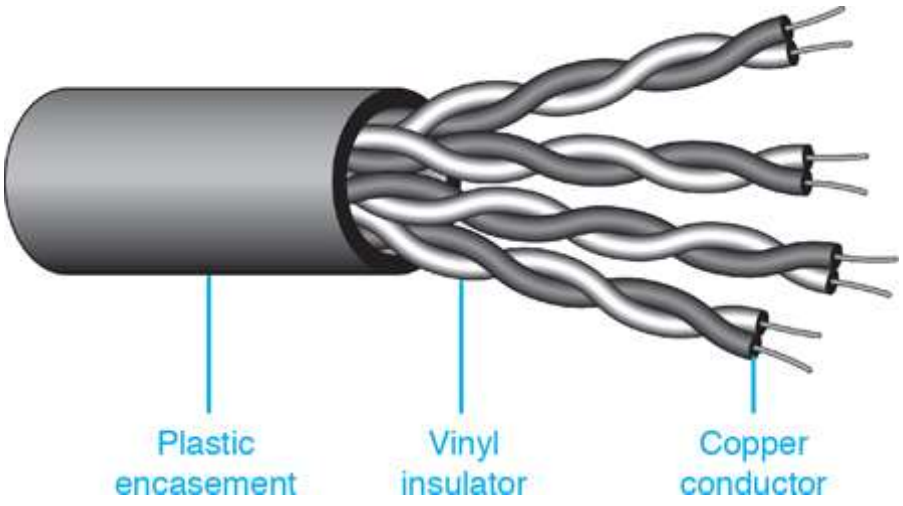


Figure 13.10 UTP cable

STP cable has extra foil that provides more shield
pair cable is used in industrial settings, such as factor
shielding is needed to prevent outside interference fr
ing the data on the cable. It is also used with **direct b**

derground outdoor cabling that has waterproofing and extra insulation so tubing or pipes are not required.

UTP cable is measured in gauges. The most common sizes of UTP cable are 22-, 23-, 24-, and 26-gauge cables. UTP cables come in different specifications called categories. The most common are Categories 5e, 6, 6a, and 7. People (and cable manufacturers) usually shorten the name *Category* to *Cat*, so Category 6 is spoken of as Cat 6. Table 13.5 shows some of the categories of UTP cable. You can also refer to Table 2.6 in Chapter 2 for a recap of the major Ethernet characteristics.

Table 13.5 UTP cable categories

Category	Description
Cat 5	No longer a recognized standard; replaced by Cat 5e.
Cat 5e	Known as Cat 5 enhanced. Can be used with 10BaseT, 100BaseT, and 1000BaseT (Gigabit) Ethernet networks. Cables are rated to a maximum of 328 feet (100 meters). Supports frequencies up to 100 MHz per pair (speeds up to 1 Gbps).
Cat 6	Supports Gigabit Ethernet better than Cat 5e but uses larger-gauge (thicker) cable. Supports frequencies up to 250 MHz per pair (speeds up to 1 Gbps). More stringent specifications to prevent crosstalk (signals from one wire going over into another wire). Commonly used in industry.
Cat 6a	Supports 10GBaseT Ethernet and frequencies up to 500 MHz (speeds up to 10 Gbps).
Cat 7	Backward compatible with Cat 5e and 6. Supports 10GBaseT Ethernet and frequencies up (speeds up to 10 Gbps).

Category	Description
Cat 8	Allows speeds up to 40 Gbps using only STP at time of press.

A special type of UTP or STP cable is plenum cable. A *plenum* is a building's air circulation space for heating and air conditioning systems. **Plenum cable** is treated with Teflon or some other fire-retardant materials to reduce its fire risk. Plenum cable produces less smoke and is less toxic when burning than regular networking cable.

The alternative to plenum cable is polyvinyl chloride (**PVC**) cable, which has a plastic cable insulation or jacket. PVC is cheaper than plenum cable, and it can have flame retardant added to make the cable flame retardant if necessary for compliance with building codes. PVC is usually easier to install than plenum cable.

Terminating Twisted Pair Cable

Twisted pair network cable has an RJ45 connector that has a tang (a plastic clip) to securely insert the connector into an RJ45 jack, as shown in Figure 13.11. Tangs frequently get broken, and sometimes a technician must make an Ethernet cable. If a tang breaks off, the RJ45 connector is cut off and a new RJ45 connector attached. This is known as *terminating* a cable. To create a new cable, you purchase a spool of twisted pair cable, cut off a suitable length, and add an RJ45 connector to each end.

Figure 13.11 UTP connector with tang

Twisted pair cable uses either an **RJ45** (8 conductor) or **RJ11** (4 conductor) connector. RJ45 connectors are used with networks and RJ11 connectors with phone cabling. Twisted pair network cable has eight copper wires. The wires are grouped in colored pairs (see Figure 13.12). Each pair is twisted together to prevent crosstalk, which occurs when a signal on one wire interferes with the signal on an adjacent wire.

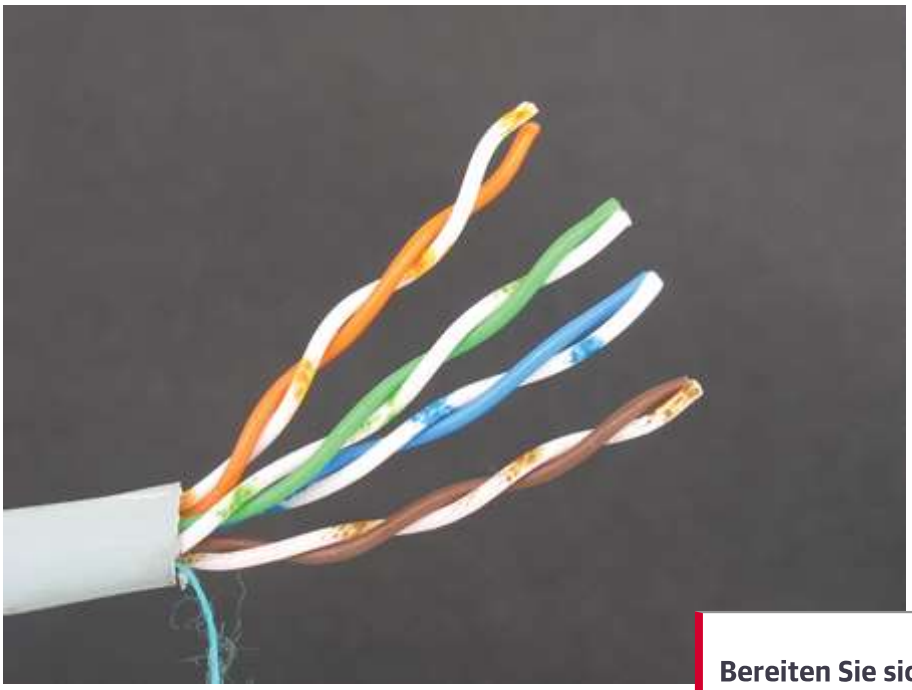
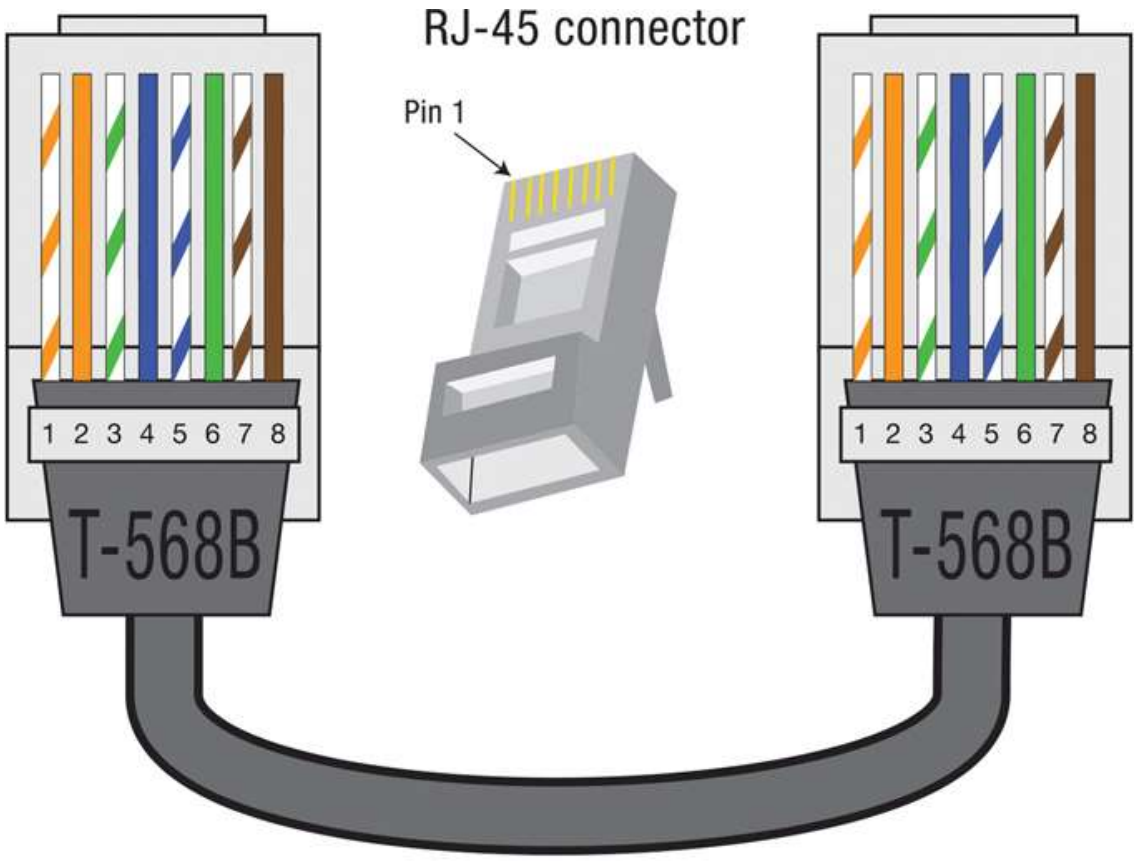


Figure 13.12 UTP color pairs

To connect a computer to a switch or network wall outlet, a **straight-through cable** (also known as a patch cable) is used. Both ends of the cable would be wired to the **T568A** standard, or both ends of the cable would be wired to the **T568B** standard (the more popular method). When connecting two computers (or two switches) together, a **crossover cable** is used. A crossover cable has one RJ45 connector created to the T568A standard and the other end created to the T568B standard. Figure 13.13 shows the color codes associated with the T568A and T568B standards. Figure 13.14 shows the location of pin 1 on an RJ45 port and on a connector. Notice in both figures how the tang is pointing down toward the floor.



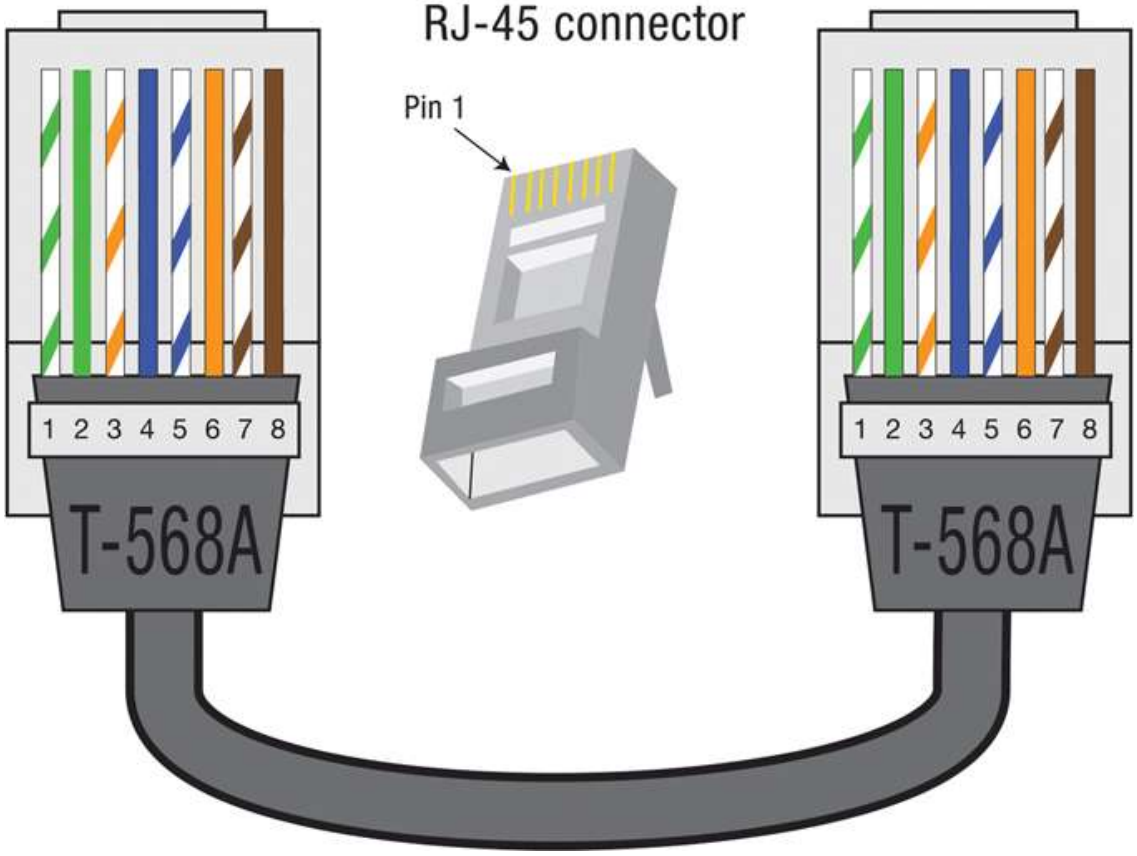


Figure 13.13 UTP cabling by color and wiring standards

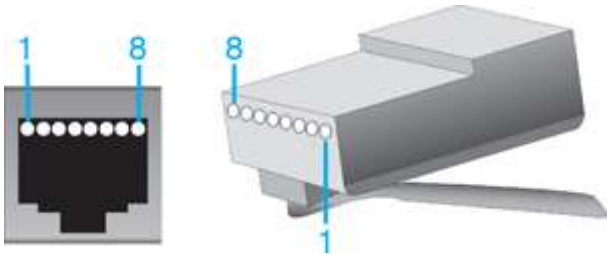


Figure 13.14 Pin 1 on an RJ45 port and connector

'ech Tip Networking two PCs without a switch or hub

If you have two PCs with Ethernet NICs installed, you can connect them with a crossover cable attached to the RJ45 jack on each NIC.

To start creating your own cable, the plastic encasement must be stripped away with a **cable stripper** (also known as a wire stripper and shown in Figure 13.15) to expose approximately 1 inch (2 centimeters) of the vinyl insulator that covers the copper conductors. Look back to Figure 13.12 to see the exposed conductors after the insulator has been stripped.

Figure 13.15 Cable stripper

A **crimper**, which is used to secure a cable to an RJ45 connector, may include a blade and/or a cable stripper. In the first photo in Figure 13.16, the cable is being stripped of the plastic encasement. The second photo in Figure 13.16 shows the vinyl insulator stripped away.

Figure 13.16 Crimper used as a wire stripper

After the plastic encasement is removed, untwist the cable pairs and place them in the proper color order. Wiggle each cable back and forth to make it more pliable. Cut the cables straight across, leaving 1/2 inch (1 centimeter) of cable. Insert the cables into the RJ45 connector in the correct color order. Ensure that the tang points toward the floor.

A common mistake when making a cable is not pushing the wires to the end of the RJ45 connector. Before crimping, look at the end of the RJ45 connector. You should see each wire jammed against the end of the RJ45 connector. You should see what looks like a set of eight gold dots staring at you when you turn the connector end toward you to verify that the conductors are pushed far enough into the connector before crimping.

Another check to do before crimping is ensure that the plastic encasement is inside the RJ45 connector. You do not want the vinyl insulator outside the connector, or data errors can occur. Notice in Figure 13.17 how the blue plastic encasement is in the wider part of the RJ45 connector. No unprotected wires are outside the RJ45 connector.

'ech Tip Push the cable firmly into the jack

It is important to fully insert a UTP cable into an RJ45
dardized order. A common mistake new technicians

the RJ45 connector upside down.

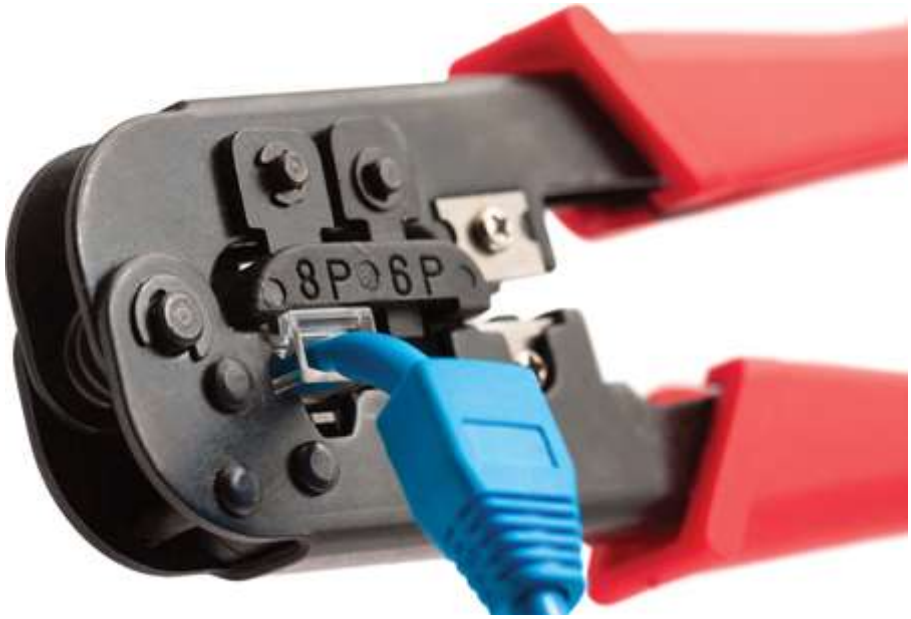


Figure 13.17 Crimping an RJ45 connector

When you have verified the color order, ensured that the eight gold connectors are pushed to the end, and verified the plastic encasement inside the RJ45 connector, you are ready to crimp. Crimping involves carefully inserting the RJ45 connector into the crimper (while keeping the wires pushed firmly into the connector) and pressing the crimper handles together firmly until the cable clicks and releases. Figure 13.17 shows a store-bought Ethernet cable that probably had a broken tang that required the RJ45 connector to be replaced. Notice how the cable has a protective sleeve that normally is positioned over the plastic part of the RJ45 connector. You must move the sleeve back before you can cut off the damaged RJ45 connector and replace it. You then slide the sleeve back over the RJ45 connector when crimping is complete.

After crimping, you must use a **cable tester** to ensure that the cable is ready for use. Figure 13.18 shows a cable tester. Plug one end of the cable into the RJ45 jack on the main tester piece (yellow case) and the other end into the RJ45 cap. Each cable tester is different, so review the instructions, if necessary.

Figure 13.18 Cable tester

Twisted Pair Cable in the Corporate Environment

With twisted pair cable, all network devices connect to one central location, such as a patch panel, hub, or switch. Refer to Figure 13.2 to see how straight-through cables connect each network device to a switch. In a corporate environment, a patch panel is used. A **patch panel**, which mounts in a network wiring rack, has network ports on the front of it and wiring connected to the back of it to provide network connectivity. In Figure 13.19, the first photo shows the front of the patch panel, and the second photo shows the back.

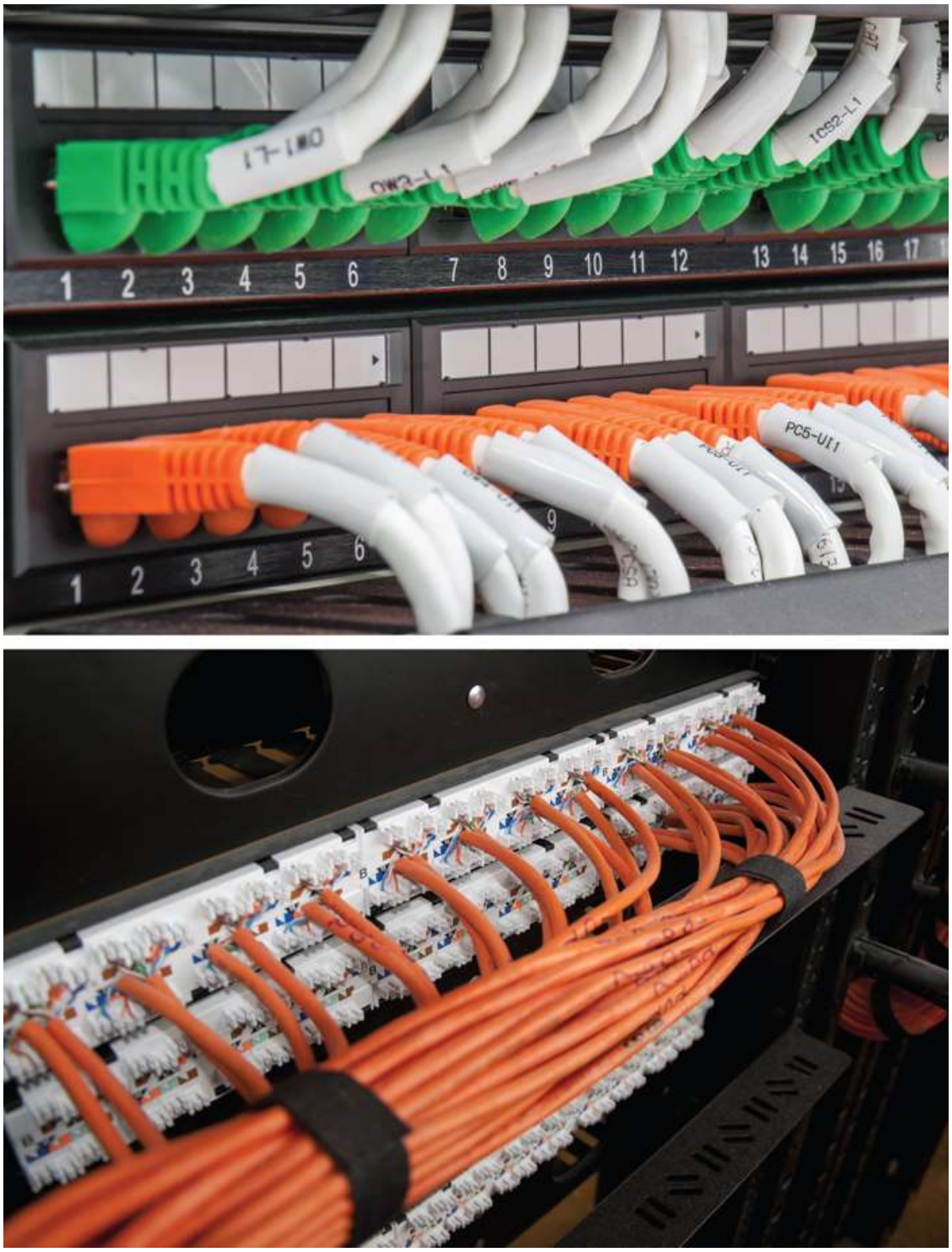


Figure 13.19 Front and back of a patch panel

A UTP cable connects from a network device to an RJ45 wall jack. That wall jack has UTP cabling (see Figure 13.20) that goes from the back of the wall jack to the back of a patch panel, as shown in Figure 13.21. A switch mounts in a wiring rack, along with a patch panel. A straight-through UTP patch cable connects from a port on the front of the patch panel to a switch located in the same network rack. Figure 13.2
bling from PCs to a switch in a corporate environmer

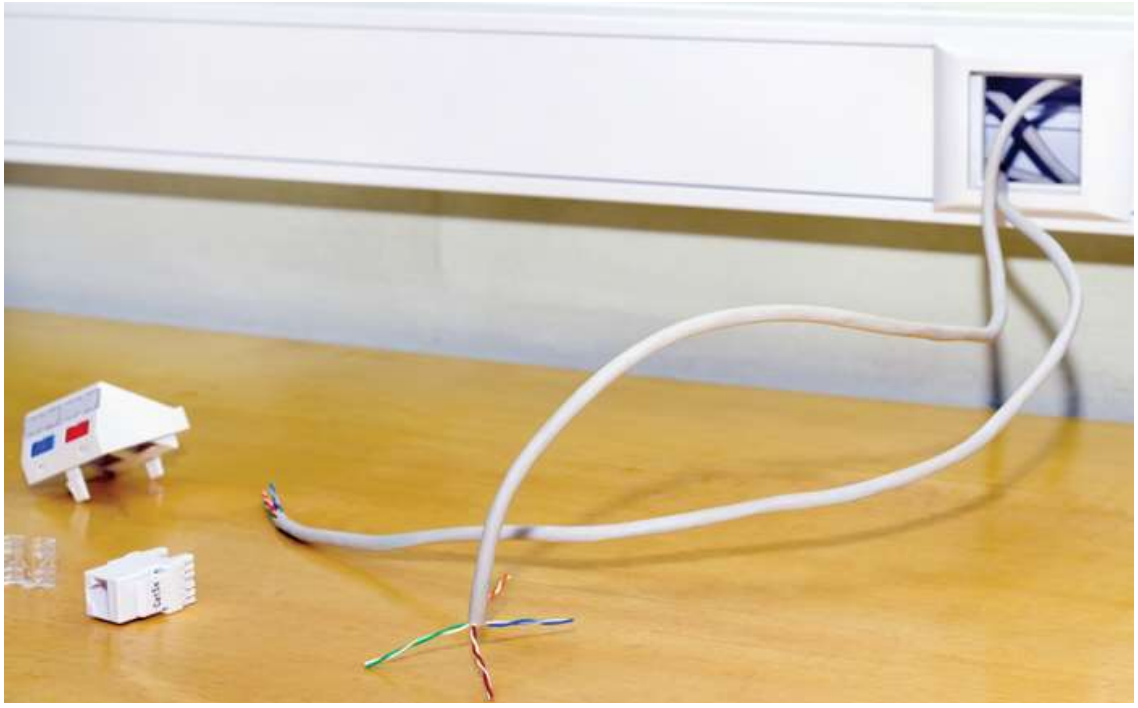


Figure 13.20 Network wall jack

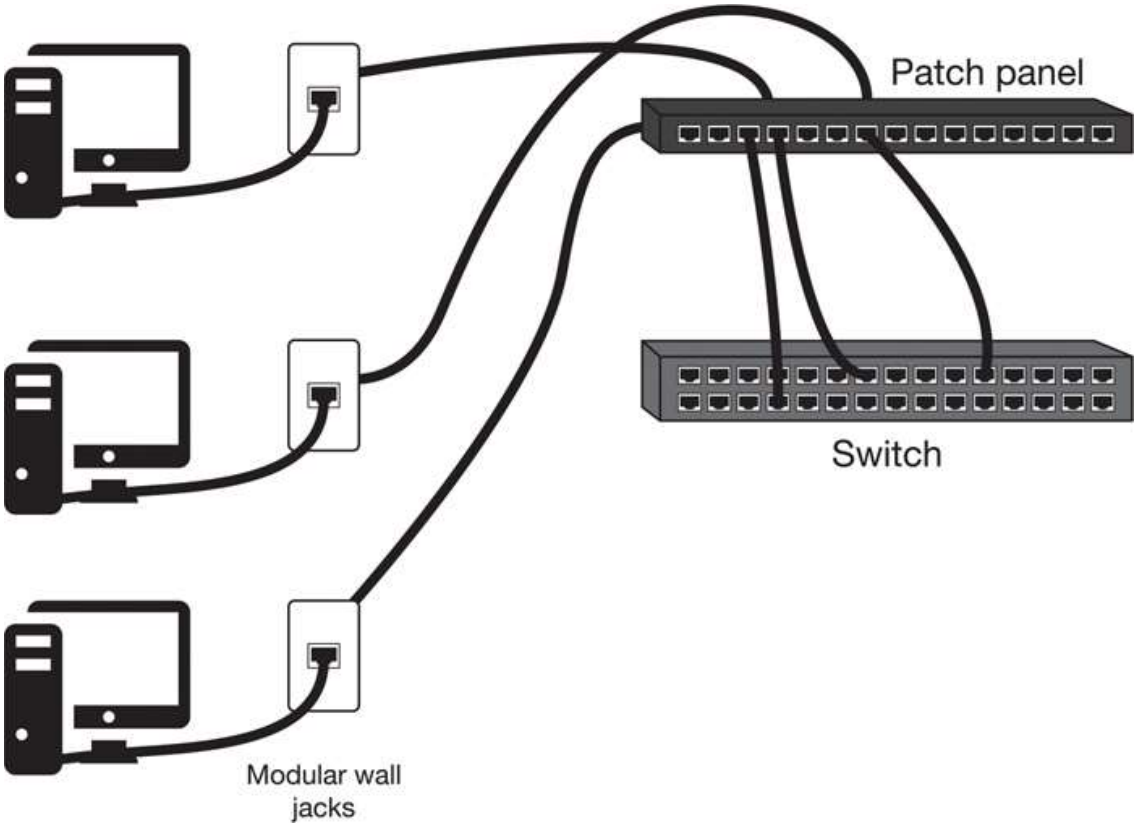


Figure 13.21 Corporate network connectivity from PCs to a switch

Ethernet cabling from the end device to the switch normally consists of three runs: (1) the cable from a patch panel to the wall at a maximum of 295 feet (90 meters), (2) the 16-foot (5 meter) maxi from the wall to a network device, and (3) a 16-foot (5 cable from a patch panel to a switch. The total length to patch panel can be 328 feet (100 meters).

'ech Tip Label both cable ends

When installing any type of network cable, you should label both ends with a unique identifier that normally includes the building and/or room number.

Power over Ethernet (PoE)

Corporate phones, IP cameras, projectors, wireless access points, and even audio systems or monitors can be powered through a technology called Power over Ethernet (**PoE**). There are different standards for PoE, and they are summarized in Table 13.6.

Table 13.6 PoE standards

Common name	IEEE standard	Description
PoE Standard (Type 1)	802.3af	2 pairs of UTP provide up to 15.4W of power to a port and 12.95W and 48V to power a device such as a voice over IP (VoIP) phone, wireless AP, or camera.
PoE Plus (PoE+ or Type 2)	802.3at	4 pairs of UTP provide up to 30W of power to a port and 25.5W and 50V to 57V to power a device such as an alarm system or a motion-tracking camera.
PoE++ (Type 3)	802.3bt	4 pairs of UTP provide up to 60W of power to the port and 51W and 50V to 57V to power a device such as a video phone or a door access reader.

Common name	IEEE stan-dard	Description
PoE++ (Type 4)	802.3bt	4 pairs of UTP provide up to 100W of power to the port and 71W and 52V to 57V to power a device such as a monitor, laptop, or point-of-sale register.
POH (Power over HD-Base-T)	802.3at	4 pairs of UTP provide up to 100W of power to the port and 100W and 52V to 57V to power a device due to the end device being able to de-termine cable length and draw.

Power can be provided to a device via PoE through a switch that has PoE capability (called a **PoE switch**), a PoE patch panel, or a **PoE injector** (sometimes called a power injector) to inject DC voltage power. Figure 13.22 demonstrates these concepts.

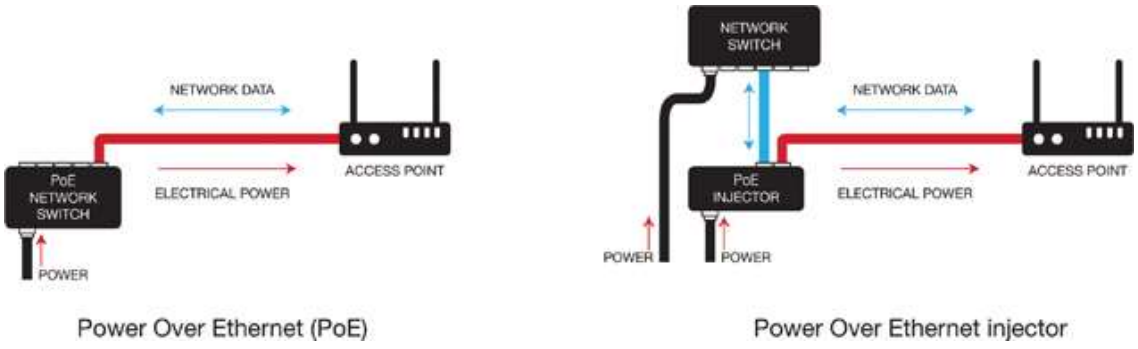


Figure 13.22 Access point with PoE and PoE injector

Ethernet Over Power

One way to create an Ethernet network without swit
crossover cable between two PCs is to use electrical c
over Power (EoP) (also known as *powerline commun*

work data to EoP modules plugged in to power outlets to extend an Ethernet network. Some EoP modules support wireless connectivity as well. To use EoP, you need a minimum of two EoP modules. One module plugs in to a power outlet near the internet modem/router. An Ethernet cable attaches from the internet modem/router to the EoP module. A second EoP module connects somewhere else in the home or business, near a device that has trouble connecting to the internet due to the absence of Ethernet wiring or weak wireless RF signal. Attach an Ethernet cable between the stranded device and the EoP module, and the device will have internet access. Figure 13.23 shows this concept.

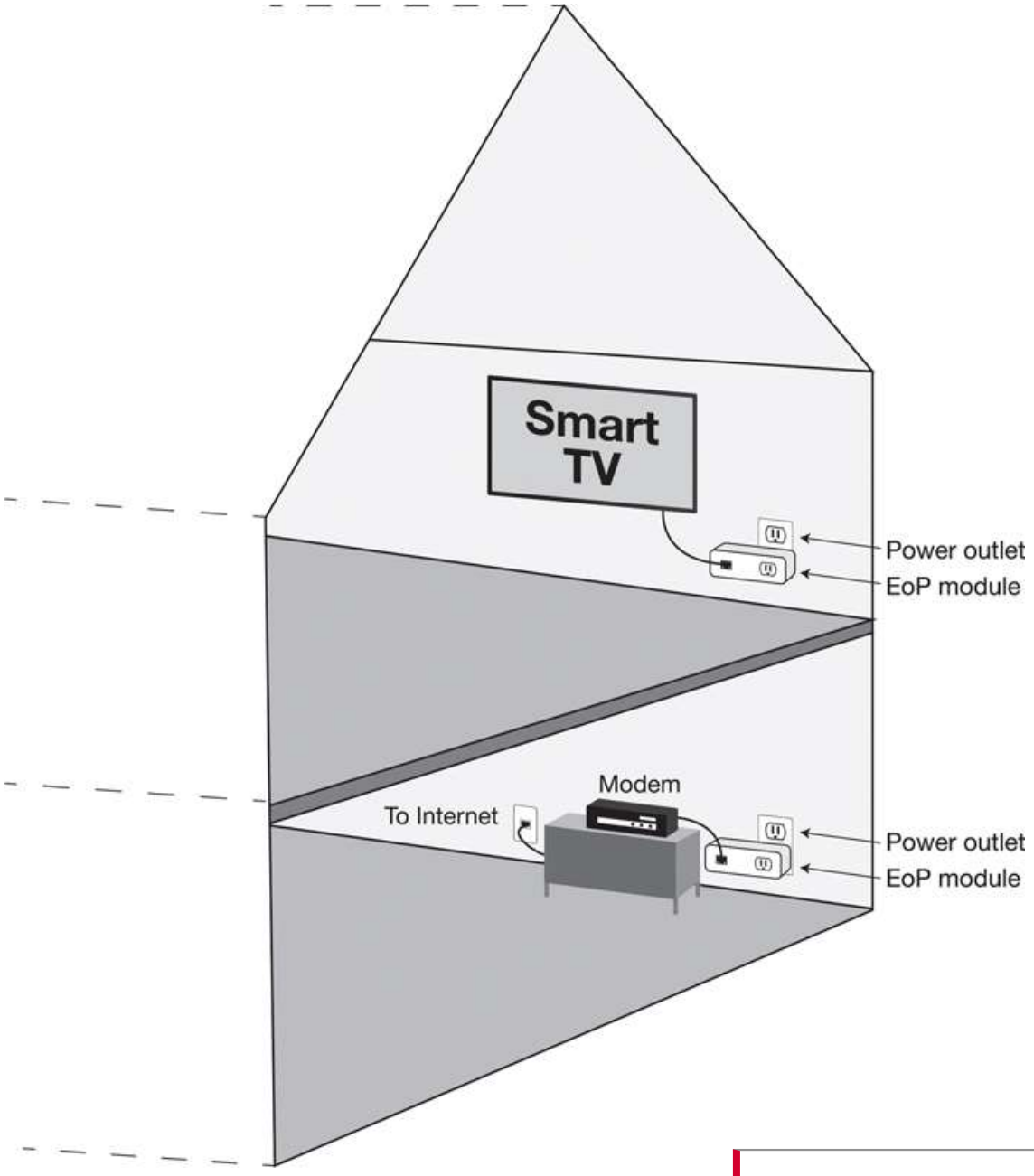


Figure 13.23 Ethernet over Power connectivity

Protecting Your Network and Cable Investm

IT professionals are charged with protecting cabling investments as well as ensuring that cabling does not cause personal safety risks. Network devices should be locked in a secure room or cabinet when possible. Figure 13.24 shows network cabinets that have network devices as well as cabling installed inside them.

Figure 13.24 Network cabinets

Network racks, such as the one shown inside the cabinet in Figure 13.24, require grounding so that all of the equipment mounted to the rack is the same potential. Electrical codes indicating how this is to be done vary by country and state. On painted racks, it is important to remove the paint from a small section and attach a ground cable that connects from the rack to building ground or an electrical panel; electricians commonly do this. You might also see a ground wire connected to a UPS that provides backup power to network equipment.

Network cable can be pulled through walls and over ceilings but should be installed in conduit or raceways (mesh racks or ladder racks that keep the cable away from other things), if possible. A professional **cable management system** can help keep network c
Ensure that network cabling is not a trip or other saf
cation. Of course, this increases the cost of the netwo
protects the network cabling and people. Figure 13.2

closet that is typical of the closets in many companies. Figure 13.26 shows a network wiring rack with a cable management system.

Figure 13.25 Messy network wiring rack

Figure 13.26 Cable management system

A ladder rack is a network cable accessory that holds multiple cables going across a room or from one side of a room to a network rack that is located away from the wall. Figure 13.27 shows a network cable ladder rack with bundles of cables.

Figure 13.27 Network cable ladder racks

Network Cabling and Troubleshooting Tools

Table 13.7 and Figure 13.28 describe and show network-related tools used in making cable and troubleshooting cable issues.

Table 13.7 Network cabling tools

Tool	Description
Cable stripper	Creates straight-through UTP patch cables or cross-over cables. (Refer to Figures 13.15, 13.16, and 13.28.) Also called a wire stripper.
Cable tester	Checks coaxial and UTP cable (dep model). (Refer to Figures 13.18 and

Tool	Description
Crimper	Permanently attaches an RJ45 or RJ11 connector to cable. (Refer to Figure 13.17.)
Loopback plug	Attaches to a specific port and tests the port or communications circuitry to see if a signal can be sent out and received. If the test succeeds, the port and communications circuits are good.
Multimeter	Takes voltage, resistance, and current readings. Can be used to check if data racks are grounded. (Refer to Figures 5.22, 5.23, and 5.24 in Chapter 5, "Disassembly and Power.")
Punchdown tool	Connects network cables to a patch panel (see Figure 13.28, 13.29, and 13.30) or phone cables to a punchdown block (see Figure 13.30).
Tone generator and probe	Used to identify cables when they are not labeled or are labeled incorrectly. A **tone generator** connects to a cable or is inserted into a network jack. The tone generator injects a tone down the cable. The **toner probe** (see Figure 13.28) is touched to the other end of a cable to identify it.
Network tap	Also known as a breakout tap, monitors/copies network data and can be a hardware device, done on some corporate switch models, or done through software. If hardware, think of a T-shaped device. The device typically has two ports that are used to allow the data to come in and then flow out. One or more additional ports are used to send the data that flowed through the first two ports out to a tures the data for further analysis.

Figure 13.28 Network tools

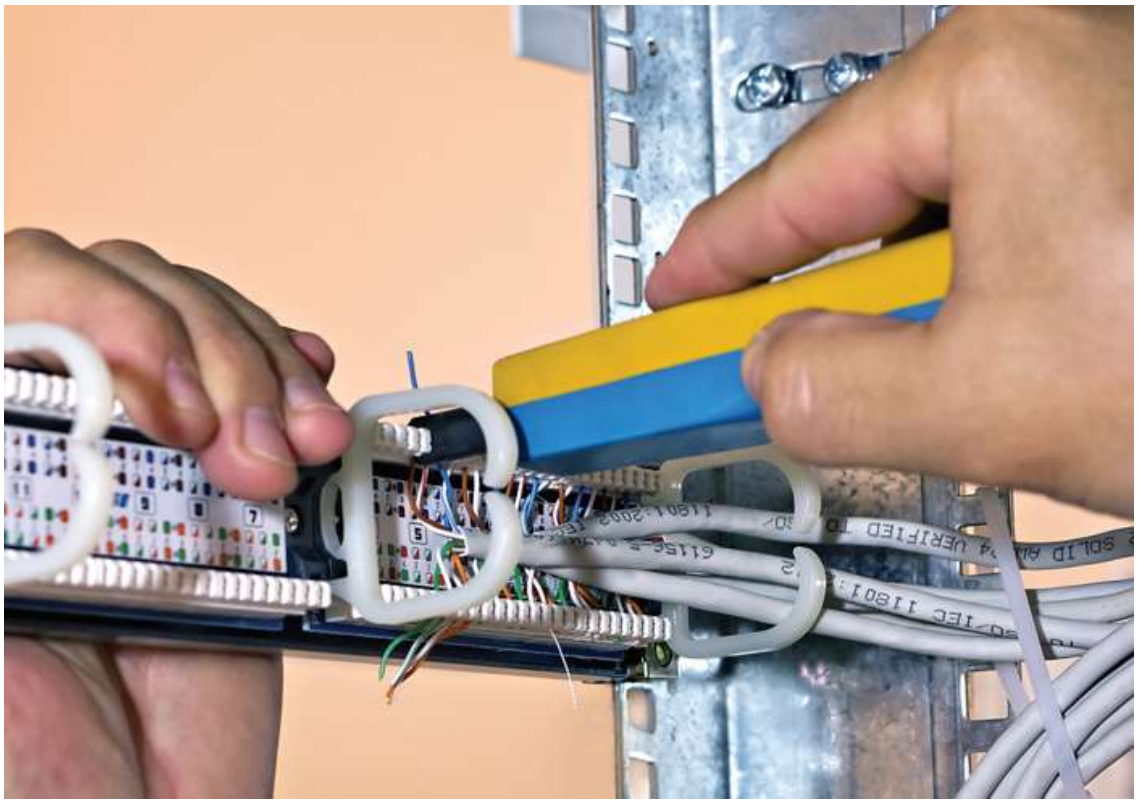


Figure 13.29 Punchdown tool with a network patch panel

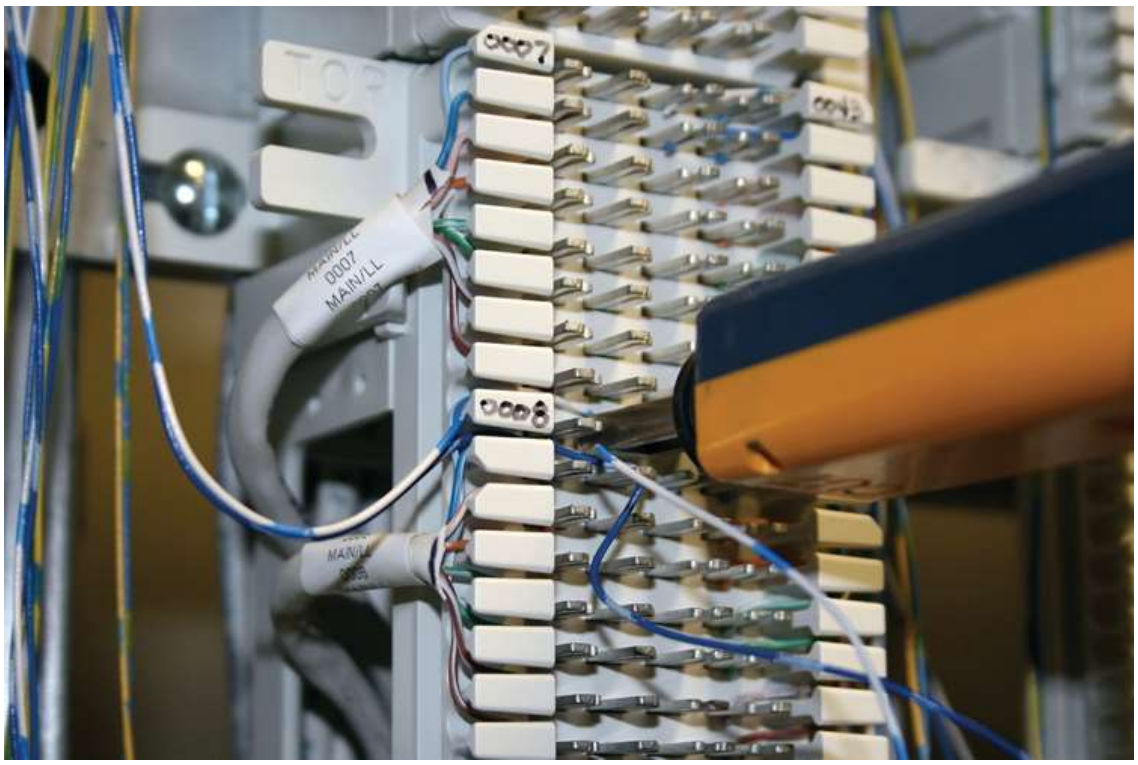


Figure 13.30 Punchdown tool with a phone punchdown block

The OSI Model

The International Organization for Standardization (ISO) developed a model for network communications known as the OSI (Open Systems Interconnect) model. The **OSI model** is a standard for information transfer across the network. All network communication must be handled by a set of rules, and the OSI model provides a structure into which these rules fit.

Can you imagine a generic model for building a car? This model would state that you need some means of steering, a type of fuel to power the car, a place for the driver to sit, safety standards, and so forth. The model would not say what type of steering wheel to put in the car or what type of fuel the car must use but would just be a blueprint for making the car. The OSI model is a similar model in networking.

The OSI model divides networking into different layers so that it is easier to understand (and teach). Dividing the network into distinct layers also helps manufacturers. If a particular manufactur[illegible] network device that works on Layer 3, the manufactu[illegible] cerned only with Layer 3. This division helps networ[illegible] emerge much faster.

The layers of the OSI model (starting from the top and working down) are application, presentation, session, transport, network, data link, and physical (see Figure 13.31).

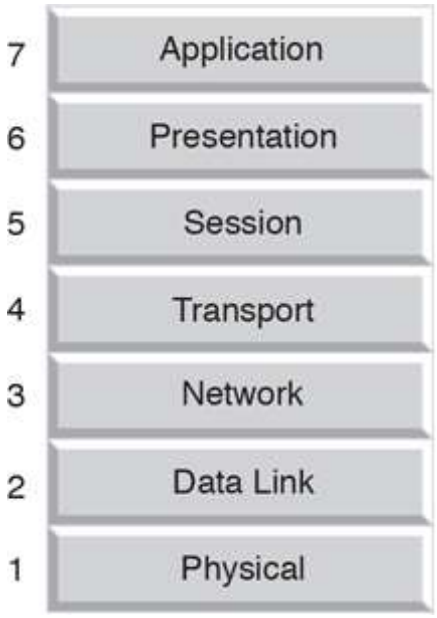


Figure 13.31 OSI model layers

Each layer of the OSI model uses the layer below it (except for the physical layer, which is at the bottom). Each layer provides some function to the layer above it. For example, the data link layer cannot be accessed without first going through the physical layer. If communication needs to be performed at Layer 3 (the network layer), the physical and data link layers must be used first.

'ech Tip OSI mnemonic

A mnemonic to help remember the OSI layers is Active People Seldom Take Naps During Parties. For example, A in Active reminds you of the application layer, P in People reminds you of the presentation layer, and so on.

Each layer of the OSI model from the top down (except for the physical layer) adds information to the data being sent across
Sometimes, this information is called a *header*. Figur
header is added as a packet travels down the OSI mo
ing computer receives the data, each layer removes t

tion. Information at the physical layer is normally called *bits*. When referring to information at the data link layer, use the term *frame*. When referring to information at the network layer, use the term *packet*.

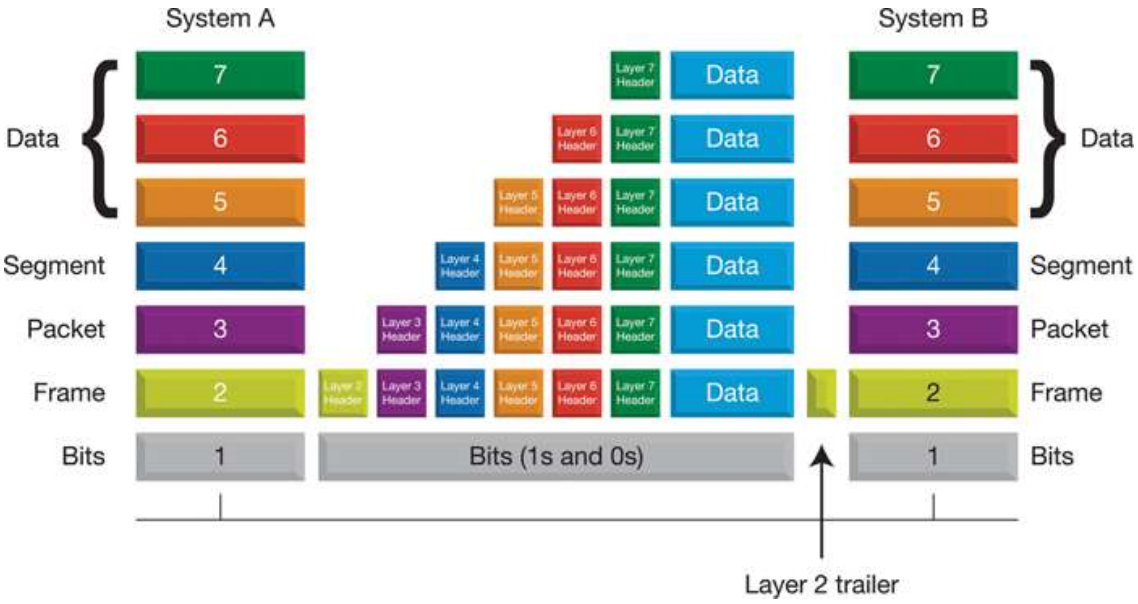


Figure 13.32 OSI peer communication

Each of the seven OSI model layers performs a unique function and interacts with the layers surrounding it. The bottom three layers handle the physical delivery of data across the network. The top four layers handle the ins and outs of providing accurate data delivery between computers and their individual processes, especially in a multitasking operating system environment.

The OSI model can be confusing when you first learn about networking, but it is important. Understanding the model helps when troubleshooting a network. Knowing where a problem occurred narrows the field of possible solutions. Table 13.8 describes the layers of the OSI model.

Table 13.8 OSI model

OSI model layer	Description
Application	Provides network services (file, print, and messaging) to any software application running on the network. **Firewalls** (devices or software that inspect data for security purposes and filter traffic based on networking protocols and rules established by a network administrator) operate at this layer and can also inspect Layer 4, 3, and 2 data as well.
Presentation	Translates data from one character set to another.
Session	Manages communication and synchronization between network devices.
Transport	Provides mechanisms for how data is sent, such as reliability and error correction.
Network	Provides path selection between two networks. **Routers** reside at the network layer and send data from one network toward the destination network. Encapsulated data at this layer is called a *pack*et. Multilayer switches can operate at this layer.
Data link	Encapsulates bits into frames. Can provide error control. A MAC address is at this layer. Layer 2 switches operate at this layer.
Physical	Defines how bits are transferred and received. Defines the network media, connectors, and voltage levels. Data at this level is called bits. Hubs, cables, and NICs operate at this level.

The TCP/IP Model

A **network protocol** is a data communication language. A protocol suite is a group of protocols that are designed to work together. Transmission Control Protocol/Internet Protocol (**TCP/IP**) is the protocol suite used in networks today. It is the most common network protocol suite and is required when accessing the internet. Most companies and homes use TCP/IP as their network standard. The TCP/IP protocol suite consists of many protocols, including Transmission Control Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP), to name a few. These will be explained as we go along. The TCP/IP model describes how information flows through a computer when TCP/IP-based protocols are used. The TCP/IP model has only four layers, in contrast to the seven layers in the theoretical OSI model. Because there are fewer layers and because the TCP/IP model consists of protocols that are in production, it is easier to study and understand networking from the perspective of the TCP/IP model. Figure 13.33 shows the TCP/IP model and message formatting, and Table 13.9 describes the layers.

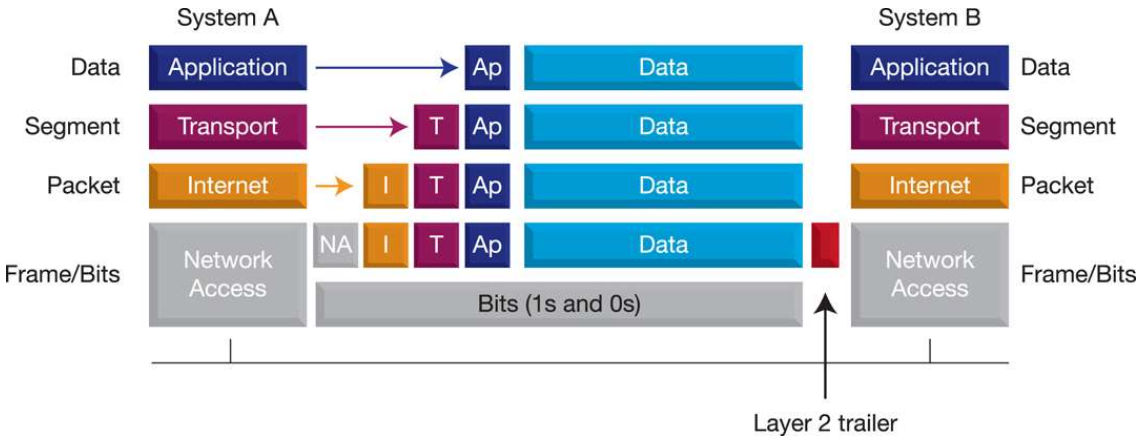


Figure 13.33 TCP/IP model and message formatting

Table 13.9 **TCP/IP model layers**

TCP/IP model layer	Description

TCP/IP model layer	Description
Application	TCP/IP-based application layer protocols format data for specific purposes; equivalent to the application, presentation, and session layers of the OSI model. Protocols include HTTP, Telnet, DNS, HTTPS, FTP, TFTP, TLS, SSL, POP, SNMP, IMAP, NNTP, and SMTP.
Transport	Transport layer protocols add port numbers in the header, so a computer can identify which application sends the data. When data returns, this port number allows the computer to determine into which window on the screen to place the data. Protocols include TCP and UDP.
Internet	Sometimes called the internetwork layer, IP is the most common internet layer protocol. IP adds source and destination IP addresses to uniquely identify the source and destination network devices. An **IP address** is a unique 32- or 128-bit number assigned to a NIC.
Network access	This layer was called the link layer in the original RFC (request for comments). It defines how to format the data for the type of network used. For example, if Ethernet is used, an Ethernet header, including unique source and destination MAC addresses, will be added here. A **MAC address** is a unique 48-bit hexadecimal number burned into a chip on the NIC. The network access layer would define the type of connector used and put the data onto the network, whether it be voltage levels for 1s and 0s on the copp of light for fiber.

Table 13.10 shows what devices operate at the OSI and TCP/IP model layers. Wireless devices are covered later in this chapter.

Table 13.10 Devices and the OSI and TCP/IP models

Network devices	OSI layer	TCP/IP layer	Description
Router, wireless router	Network	Internet (inter-net-work)	A router connects two or more networks.
Switch, wireless access point, wireless bridge	Data link	Network access	A switch connects devices to a LAN and learns MAC addresses. An access point connects wireless devices to form a WLAN. A wireless bridge connects two networks.
Hub, wireless antenna, cable, connectors	Physical	Network access	A hub connects devices to a LAN. An antenna receives wireless signals. A cable connects a device to a wired network. A connector attaches to a cable.

Network Addressing

A network adapter normally has two types of addresses assigned to it: a MAC address and an IP address. A MAC address is a 48-bit unique hexadecimal number that is burned into a chip located on a NIC. A MAC address is unique for every computer on a network. The first 24 bits represent the manufacturer and the remaining 24 bits are
dress is known as a Layer 2 address or a physical add
is normally shown in one of the formats listed in Tab

Table 13.11 MAC address formats

Address format	Description
00-11-11-71-41-10	Groups of two hexadecimal digits are separated by hyphens.
01:11:11:71:41:10	Groups of two hexadecimal digits are separated by colons.
0111.1171.4110	Groups of four hexadecimal digits are separated by periods.

IP addressing provides a much more organized way of addressing a computer, and an IP address is sometimes known as a Layer 3 address, in reference to the OSI network layer. There are two types of IP addresses: IPv4 (IP version 4) and IPv6 (IP version 6). **IPv4** is the most common IP addressing used on LANs. An IPv4 address is a 32-bit number that is entered into a NIC's configuration parameters. This address is used when multiple networks are connected and when accessing the internet. An IPv4 address is shown using dotted decimal notation, such as 192.168.10.4.

'ech Tip What is in an IPv4 address?

An IPv4 address is separated into four sections called octets. The octets are separated by periods, and each one represents 8 bits. The numbers 0 to 255can be represented by 8 bits.

IPv6 addresses are 128 bits in length and shown in hexadecimal format. IPv6 addresses are used by corporate devices and by most internet service providers. Today, a computer has both an IPv4 address and an IPv6 address assigned. An example of an IPv6 address is fe80::13e:4586:5807:95f7. Each set of four digits repre
an octet contains just three digits (for example, 13e),
zero in front that has been omitted from the octet (01
(::) in an IPv6 address represents a string of zeros tha

Only one set of double colons is allowed in an IPv6 address. Many network cards are assigned IPv6 addresses, even when IPv6 is not used.

One IPv6 address assigned to a NIC is a link-local address. An IPv6 **link-local address** is used to communicate on a particular network. This address cannot be used to communicate with devices on a different network. A link-local address can be manually assigned or, more commonly, may be automatically assigned. Figure 13.34 shows a home computer that has an IPv6 link-local address that has been automatically assigned. You can also see the IPv4 address in this figure.

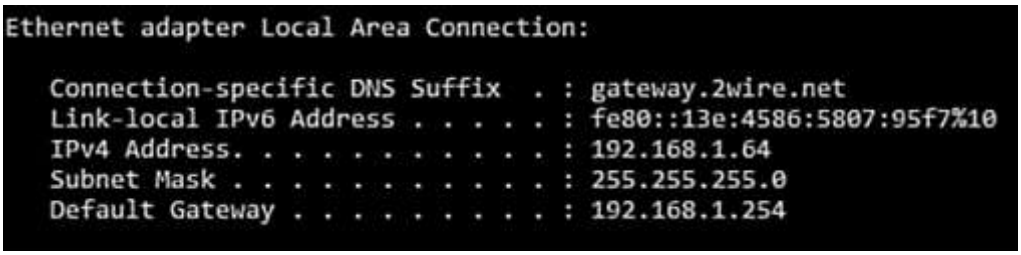


Figure 13.34 IPv6 link-local address and IPv4 address

IPv4 addresses are grouped into five classes: A, B, C, D, and E. Class A, B, and C addresses are used by network devices. Class D addresses are used for multicasting (sending traffic to a group of devices such as in a distributed video or a web conference session), and Class E addresses are used for experimentation. It is easy to tell which type of IP address is used by a device: You just need to look at the first number shown in the dotted decimal notation. Table 13.12 shows the common classes of addresses.

Table 13.12 Classes of IPv4 addresses

Class	First octet (number) of the IP address
Class A	0 to 127
Class B	128 to 191
Class C	192 to 223

The IP address 12.150.172.39 is a Class A address b
number is 12. The IP address 176.10.100.2 is a Class B

first number is 176. The IP address 200.1.1.1 is a Class C address because the first number of 200 is within the range of 192 to 223.

IP addresses are also classified as public addresses and private addresses. A **private IP address** is used inside a home or business. This address is not allowed to be transmitted across the internet. The service provider or company translates the address to a **public IP address** that is seen on the internet. Table 13.13 shows the private IP address ranges for the IPv4 classes.

Table 13.13 IPv4 private IP addresses

Class	First octet (number) of an IP address
Class A	10.*x*.*x*.*x* (where the *x* represents any number from 0 to 255), or 10.0.0.0 through 10.255.255.255
Class B	172.16.*x*.*x* through 172.31.*x*.*x*, or 172.16.0.0 through 172.31.255.255
Class C	192.168.*x*.*x*, or 192.168.0.0 through 192.168.255.255

More IPv4 Addressing

An IP address is broken into two sections: the network number and the host address. The **network number** is the portion of an IP address that represents which network the computer is on. All computers on the same network have the same network number. The **host address** (or host portion of the address) represents the specific computer on the network. All computers on the same network have unique host numbers; if they didn't, they could not communicate.

The number of bits that represent the network nu
number depends on which class of IP address is used
dresses, the first 8 bits (the first number) represent th
and the remaining 24 bits (the last three numbers) re
number. With Class B IP addresses, the first 16 bits (t

bers) represent the network portion, and the remaining 16 bits (the last two numbers) represent the host number. With Class C IP addresses, the first 24 bits (the first three numbers) represent the network portion, and the remaining 8 bits (the last number) represent the host number. Figure 13.35 illustrates this point.

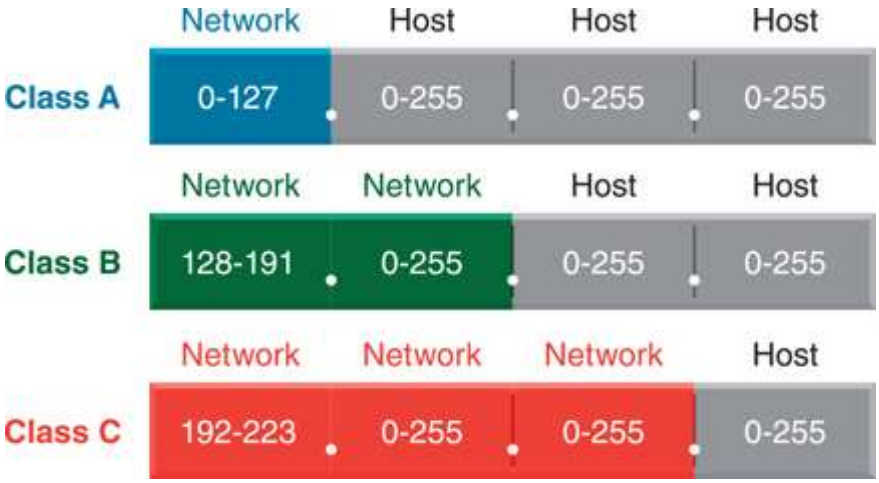


Figure 13.35 IP addressing (network and host portions)

To see how IP addressing works, say that a business has two networks connected with a router. On each network, there are computers and printers. Each of the two networks must have a unique network number. For this example, one network has the network number 192.168.151.0, and the other network has the network number 192.168.152.0. Notice that each network number is a Class C IP address because the first number is 192.

With a Class C IP address, the first three numbers represent the network number. The first network uses the numbers 192.168.151. to represent the network part of the IP address. The second network uses the numbers 192.168.152. in the network part of the address. Remember that each network must have a different network part of t
any other network in the organization. This is part of
scheme designed by a network engineer and implem
cians. Almost all organizations and home networks u
(refer to Table 13.13) for their IP addressing scheme.

The last part of the IP address (the host portion) will be used to assign a number to each network device. On the first network, each device will have a number that starts with 192.168.151. because that is the network part of the number, and it stays the same for all devices on that network. Each device will then have a different number in the last portion of the IP address—for example, 192.168.151.1, 192.168.151.2, 192.168.151.3, 192.168.151.4, and so on (as shown in Figure 13.36).

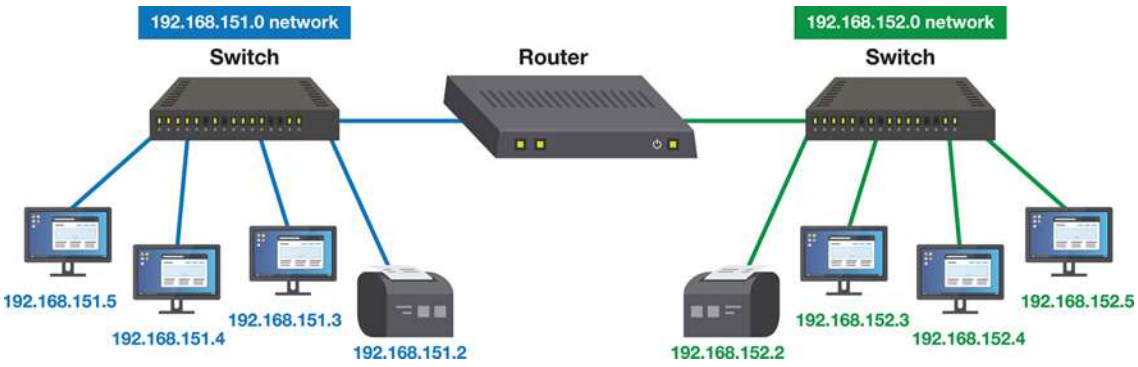


Figure 13.36 IP addressing (two networks example)

On the second network, each device will have a number that starts with 192.168.152. because that is the network part of the IP address. The last number in the IP address changes for each device. In this example, no device can have a host number that has 0 in the last octet because that number represents the network. In addition, no device can have an IP address where the last octet in the host portion of the address is 255 because that represents the **broadcast address**, which is the IP address used to communicate with all devices on a particular network.

In this example, no network device can be assigned the IP addresses 192.168.151.0 or 192.168.152.0 because these numbers represent the two networks. Furthermore, no network device can be as
dresses 192.168.151.255 or 192.168.152.255 because t
sent the broadcast address used with the 192.168.151
192.168.152.0 network. An example of a Class B broa

172.16.255.255. An example of a Class A broadcast address is 10.255.255.255.

VLANs

Another way of creating networks is by using VLANs. Creating a virtual local area network (**VLAN**) involves creating multiple networks within a switch. For example, IP phones, PCs, and printers typically connect to a switch, and companies that have switches that support VLANs tend to create separate networks for different types of devices or for devices in particular locations. For example, if you had two IP phones, three PCs, and a printer connected to the same switch, you might configure the switch ports that connect to the IP phones as VLAN 17, the switch ports that connect to the PCs as VLAN 18, and the port that connects to the printer as VLAN 19. The IP addressing schemes used within a company commonly include the VLAN number as part of the IP addressing. Notice in Figure 13.37 that the phones have IP addresses 192.168.17.*x* (where *x* is a unique number) and that the PCs have IP addresses 192.168.18.*x*. The printer has the IP address 192.168.19.3.

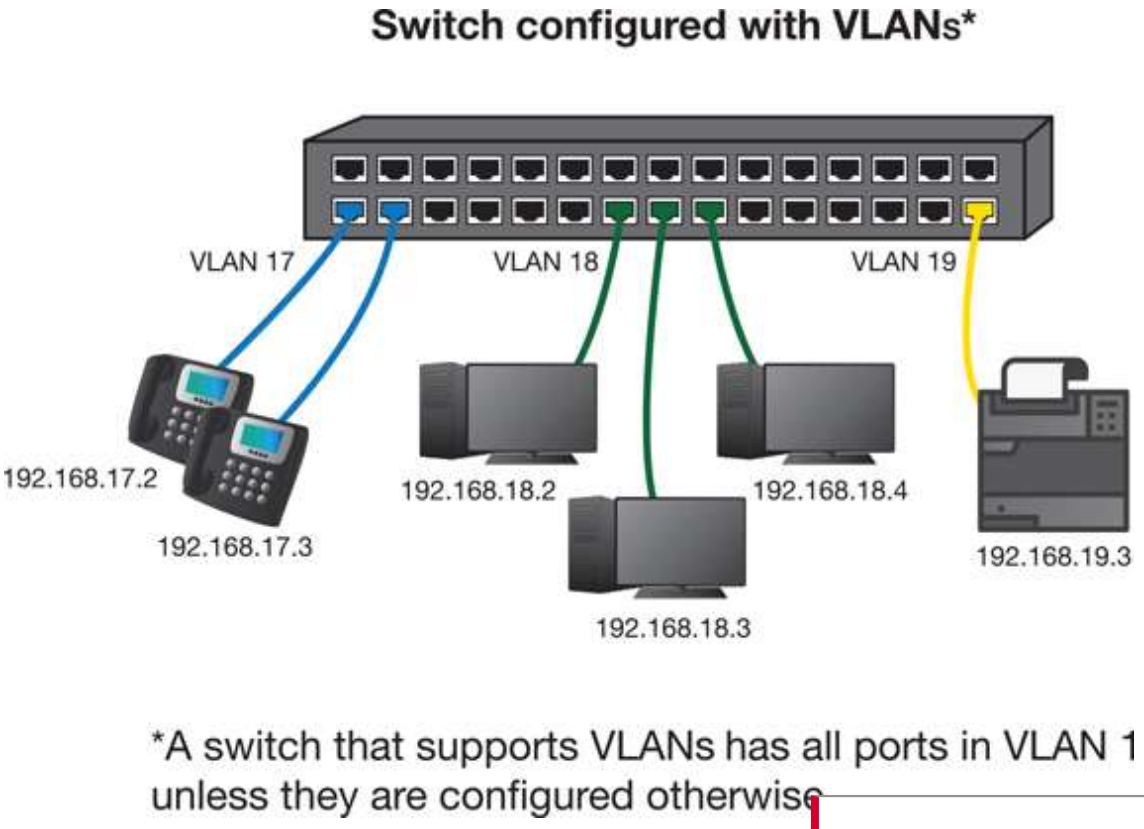


Figure 13.37 VLANs

Not all switches can be configured with VLANs, but on a switch that does support VLANs, all ports are assigned to VLAN 1 by default. If a switch does not support VLANs, then all ports need to be considered to be in the same network, and all devices connected to the switch will be in the same network.

Benefits of VLANs include the following:

- Separation of networks at Layer 2
- Reduced broadcast messages
- Ease of applying security
- Facilitates the use of quality of service (QoS)

Subnet Masks

In addition to assigning a computer an IP address, you must also assign a computer a subnet mask. A **subnet mask** (sometimes shortened to *mask*) is a number that a computer uses to determine which part of the IP address represents the network and which portion represents the host. The default subnet mask for a Class A IP address is 255.0.0.0, the default subnet mask for a Class B IP address is 255.255.0.0, and the default subnet mask for a Class C IP address is 255.255.255.0. Table 13.14 recaps this important information.

Table 13.14 IP address information

Class	First number	Network/host number	Subnet mask
A	0–127	*N.H.H.H**	255.0.0.0
B	128–191	*N.N.H.H**	255.255.0.0
C	192–223	*N.N.N.H**	

*N = network number; H = host number

Sometimes subnet masks are shown with a slash (/) followed by a number. The number represents how many consecutive 1s are in the subnet mask. For example, /8 indicates that there are eight consecutive 1s in the subnet mask, or 11111111.00000000.00000000.000000000. Notice that the subnet mask is all 0s after the eight 1s are shown. This is known as prefix notation format. A technician might have to refer to network documentation, and the subnet mask to use will be shown in prefix notation format. The prefix notation format for a Class A address is /8, Class B is /16, and Class C is /24.

A subnet mask does not always have to follow classful boundaries. Sometimes, a technician might see a subnet mask that looks like the following examples: 255.255.254.0 or /23, 255.255.255.192 or /26, and 255.255.255.240 or /28. These are known as classless inter-domain routing (CIDR) subnet masks. **CIDR** (pronounced “cider”) is a method of allocating IP addresses based on the number of host addresses needed for a particular network. Because the subnet mask dictates where the network portion ends and where the host portion begins, CIDR subnet masks are different from the standard 255.0.0.0, 255.255.0.0, and 255.255.255.0 subnet masks.

To help you better understand the concept, let’s look at how a /23 subnet mask becomes 255.255.254.0. The /23 means there are 23 1s in a row in the subnet mask, with the rest of the numbers being 0s; keep in mind that there are just eight 1s in each of the subnet mask sections where you enter the number. Write down the 23 1s with only eight digits in each section. Place 0s after the 1s for the remaining digits, keeping in mind that the subnet mask, like an IP address, has 32 bits. Then you perform simple binary-to-decimal conversion to get the subnet mask in dotted decimal notation, as it must be when you enter it on a network device:

11111111.11111111.11111110.00000000

255 . 255 . 254 . 0

Appendix A, “Subnetting Basics,” goes into CIDR in a lot more detail

Wireless Networks Overview

Even though wireless devices are covered elsewhere in the book, a networking chapter would not be complete without discussing wireless networking. Wireless data transfer occurs in both licensed and unlicensed ranges. In one of the licensed wireless ranges, a company or service provider has to obtain a specific frequency, possibly a frequency range, from the Federal Communications Commission (FCC) or its designee. Licensed wireless offers better performance than unlicensed, but it involves costs. Licensed wireless is used for radio and TV, military systems, and cellular communications.

Wireless networks in the home and corporate model are networks that transmit data over air using either unlicensed ranges such as infrared (1 THz to 400 THz range) for things like your TV remote or radio frequencies (the traditional **2.4 GHz** or **5 GHz** range, and the new **6 GHz** range) for wireless networks.

Wireless networks are popular and are great in places that are not conducive to running cabling, such as outdoor centers, convention centers, bookstores, coffee shops, and hotels, as well as between buildings and in between nonwired rooms in homes (as illustrated in Figure 13.38) or businesses. Wireless networks operate at Layers 1 and 2 of the OSI model and can be installed indoors or outdoors.

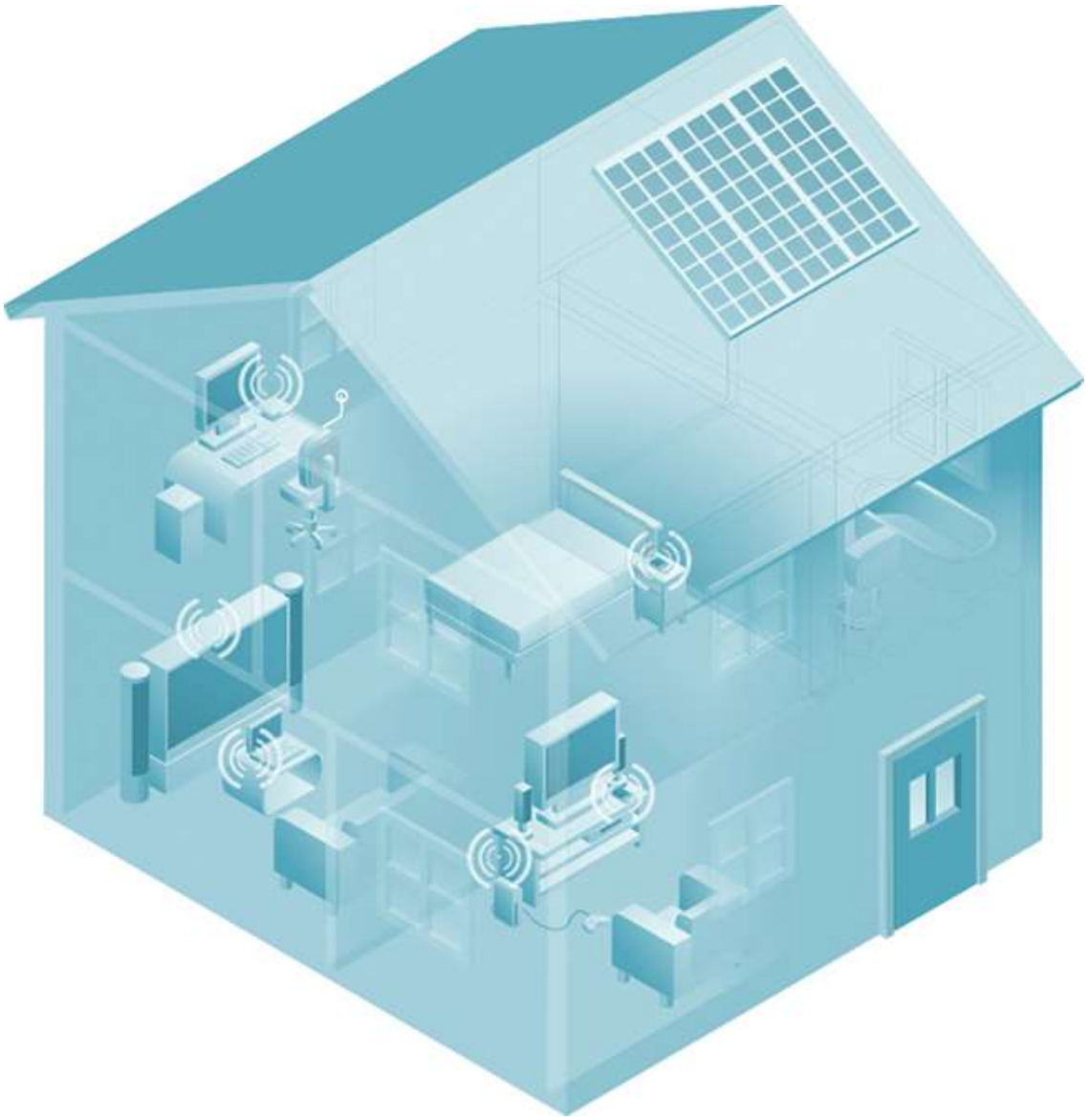


Figure 13.38 Wireless connectivity within a home

'ech Tip What if I want wireless connectivity for my desktop computer?

Desktop workstations usually have integrated RJ45 Ethernet connections, but for wireless networking, a wireless NIC is required and may have to be added.

Laptops and portable devices are frequently used to connect to wireless networks and have wireless capabilities integrated into them. Laptops also normally have wired network connections. A technician must be familiar with installation, configuration, and both wired and wireless technologies.

Wireless Network Standards

The IEEE 802.11 committees define standards for wireless networks, and these standards can be quite confusing. Table 13.15 shows the current and proposed wireless network standards.

Table 13.15 IEEE 802.11 standards

Standard	Purpose
802.11a	Came after the 802.11b standard. Has speeds up to 54 Mbps but is incompatible with 802.11b. Operates in the 5 GHz range.
802.11b	Operates in the 2.4000 and 2.4835 GHz radio frequency ranges, with speeds up to 11 Mbps.
802.11e	Relates to quality of service.
802.11g	Operates in the 2.4 GHz range, with speeds up to 54 Mbps, and is backward compatible with 802.11b.
802.11i	Relates to wireless network security and includes Advanced Encryption Standard (AES) for protecting data.
802.11n	Operates in the 2.4 and 5 GHz ranges and is backward compatible with the older 802.11a, b, and g equipment. Offers speeds up to 600 Mbps using MIMO (multiple input/multiple output) antennas. Makes possible a maximum of four simultaneous data streams.
802.11ac (Wi-Fi 5)	Operates only in the 5 GHz range, which makes it backward compatible with 802.11n and 802.11a. Offers speeds up to 6.93 Gbps. Makes possible a maximum of eight simultaneous data streams using MU-MIMO (multi-user MIMO) antennas.
802.11ad	Also known as WiGig and works in the Offers speeds up to 6.76 Gbps.

Standard	Purpose
802.11ax (Wi-Fi 6)	Operates in the 2.4, 5, and 6 GHz ranges and is backward compatible with 2.4 and 5 GHz devices. Supports multiple wireless devices more efficiently. Makes possible a maximum of eight simultaneous data streams using MU-MIMO antennas.

Wireless Network Components

The most common components of a wireless network are wireless NICs, access points, wireless bridges, and wireless routers. Table 13.16 describes the purposes of these devices.

Table 13.16 Common wireless devices

Wireless device	Description
Access point (AP)	The central connecting point for a wireless network. Coordinates wireless access for wireless devices. May connect to a wired network.
Wireless bridge	A physical device or software that connects two or more networks. Could connect a wireless network to a wired network. An example of a wireless bridge is a building where all devices connect wirelessly to the bridge. The bridge connects to the wired network, which eventually connects to the internet. Many access points or wireless routers can be placed in bridged mode.
Wireless NIC	Integrated into a wireless laptop, smartphone, or tal card or connect via USB.

Wireless device	Description
Wireless router	An AP/router device that normally has both wireless capability and a few wired Ethernet ports. It is a router because it connects multiple networks.
Wireless printer/multifunction device	Most common type of home/small office device today that can print, scan, and copy.

Major types of wireless NICs include integrated ports, USB, and PCIe. Figure 13.39 shows a wireless USB NIC with a detachable antenna.

Figure 13.39 Wireless USB NIC

To determine whether you have a wireless NIC ins
Windows 10/11 device, access *Settings* > *Network* & *in*
pears in the window to the left if you have it installed
not enabled. Use the *Change adapter options* from the
settings section to see all adapters and to see if any ar

Figure 13.40 shows the Network Connections window of a computer that has virtualization enabled, a wired Ethernet port, Wi-Fi, and Bluetooth installed. Note that the wireless NIC is not being used, but it is enabled.

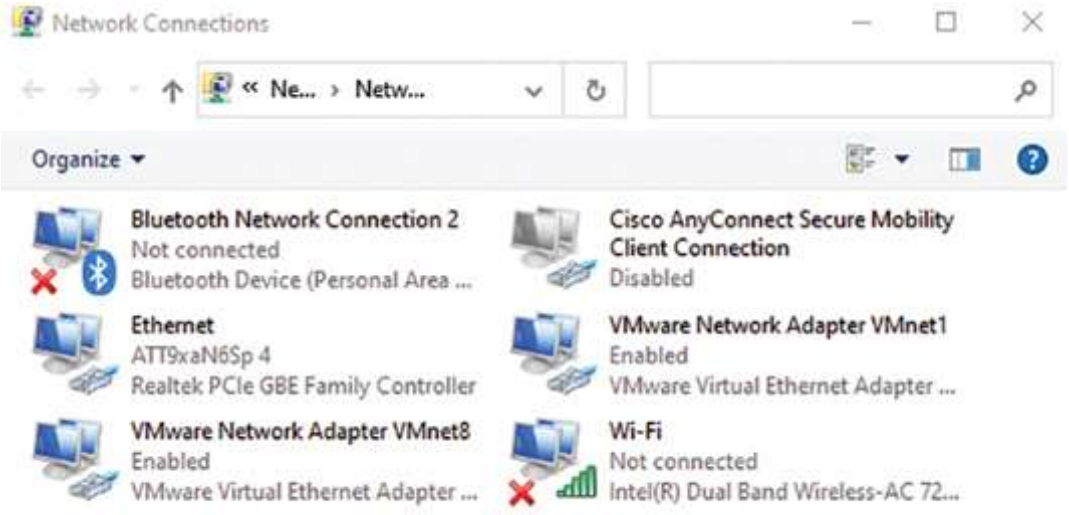


Figure 13.40 Wireless NIC in the Network Connections window

A wireless access point (AP) is a device that receives and transmits data from multiple computers that have wireless NICs installed. The AP can be a standalone unit or can be integrated into a router, as shown in Figure 13.41. It is the wireless AP part of the router that needs the three antennas shown in the figure.

Figure 13.41 Access point integrated with an ADSL router

Wireless routers commonly have switch ports built into them. This is referred to as having router/switch functionality. You might hear a wireless router referred to as a router/switch, but regardless of the name, such a device has switch ports integrated, as shown in Figure 13.42. Much like a wired router, a wireless router is used to connect devices between networks such as a home network and the internet. The switch part of the device is used to create a wired LAN, and each wired device has an Ethernet cable that runs between the device and the switch port on the wireless router.

Figure 13.42 Wireless router with integrated switch ports

Wireless Network Design

Think of an access point like a network hub, but instead of connecting wired devices and sharing bandwidth, the AP connects wireless devices that share bandwidth. Each access point can handle 1 to 100 wireless devices, depending on the wireless standard being used, vendor, environment (wood, drywall, brick, concrete, and so on), amount of usage, and type of data sent.

When designing a wireless network, you need to take into account several factors:

- Which standard you are going to use (802.11n, 802.11ac, 802.11ax, and so on).
- Which frequency range you are going use in a specific location and the type of devices to consider for a specific frequency. For example, you might want to use the 2.4 GHz range as a wireless network for guests and the 5 GHz range for company devices since the 5 GHz range is not as crowded with devices as the 2.4 GHz range is. Another idea would be to design based on the type of equipment, such as use the 2.4 GHz range for PC-based devices and the 5 GHz range for Apple and cellular devices.
- The location of the AP and what interference is around the area where the AP will be installed.

Let's take a look at some of the details involved with design.

Each AP is assigned a service set identifier (**SSID**). It is common for an AP to have a default SSID that can be changed. An SSID is a set of 32 alphanumeric characters used to differentiate between different wireless networks. It is common to have more than one SSID configured on a wireless router/AP, as illustrated in Figure 13.43. Figure 13.44 shows a screen capture of a sample wireless configuration for an 802.11ac TP-Link wireless router.

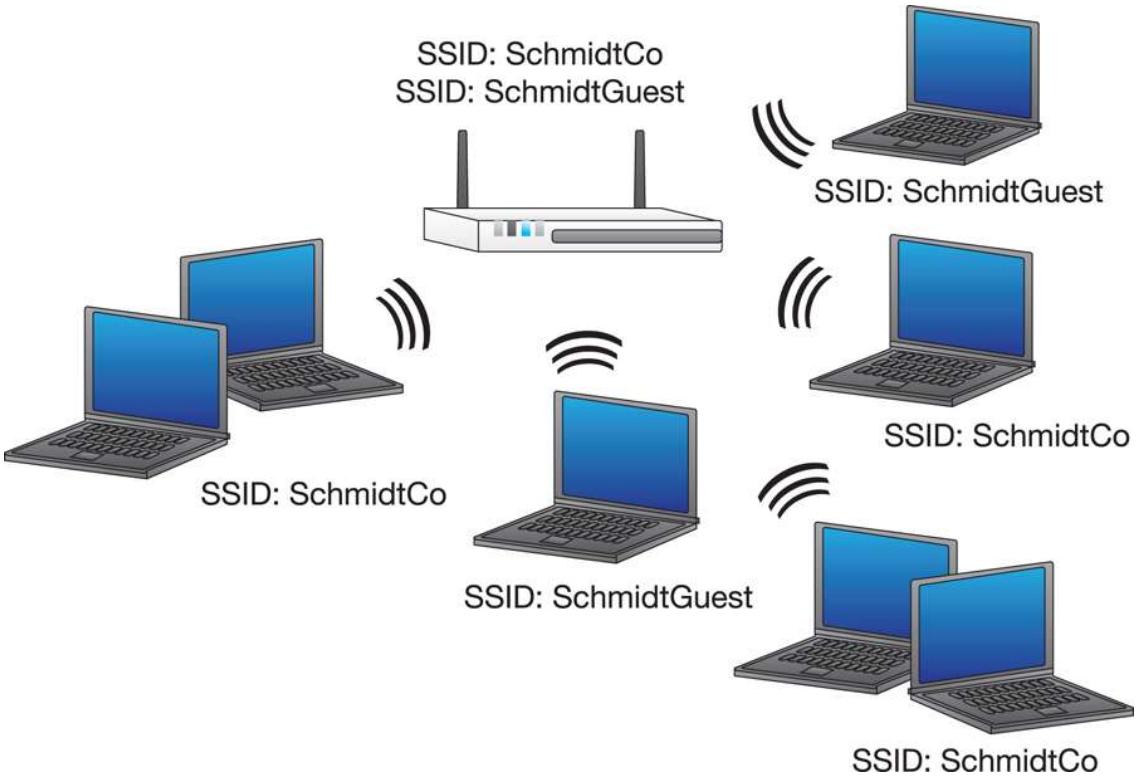


Figure 13.43 Each wireless network has its own SSID

Figure 13.44 Configuring SSIDs and SSID broadcasting on a TP-Link wireless router

An AP broadcasts the SSID by default, but this setting can be changed. When the AP is broadcasting the SSID, wireless NICs can automatically detect that particular wireless network. When the AP is not broadcasting (that is, when the SSID cannot be found in the list of wireless networks), the SSID can be manually configured through the AP's configuration window. Look back at the 2.4 GHz and 5 GHz configurations shown in Figure 13.44. Beside each SSID is a *Hide SSID* checkbox that you can check to disable SSID broadcasting.

An access point can be wired to or can connect wirelessly to another AP, can have a wired or wireless connection to a wireless repeater (also called a **wireless extender**), or can connect to a wired network. The access point can then relay the transmission from a wireless device to another network or to the internet through the wired network. If two access points are used and they connect two different wireless networks, two different SSIDs are used (see Figure 13.45). If two access points connect to the same wireless network, the same SSID is used (see Figure 13.46).

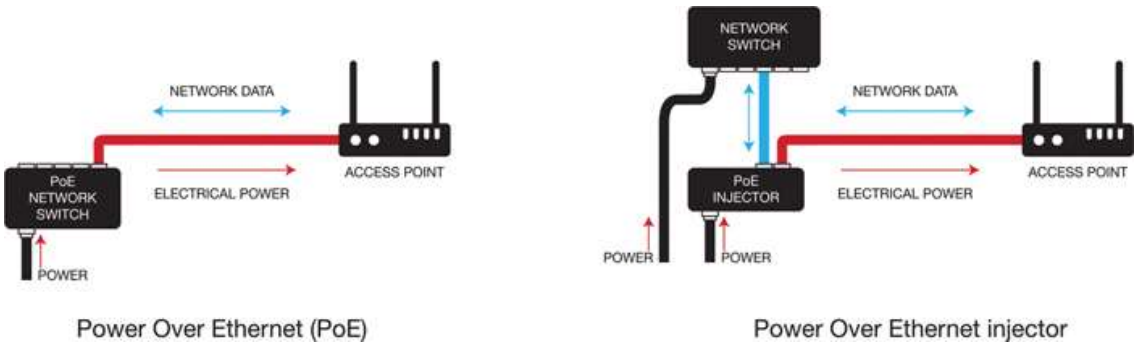


Figure 13.45 Two separate wireless networks with two SSIDs

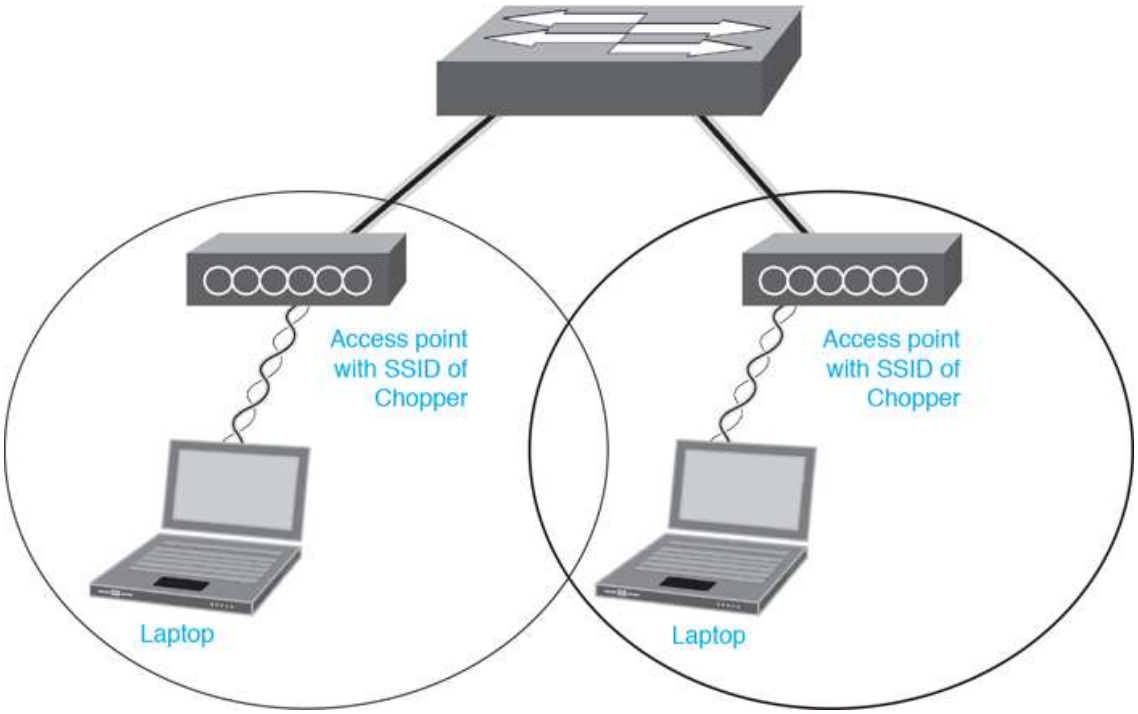


Figure 13.46 One extended wireless network with the same SSID on both APs

A home or small business network can expand its wireless network by using a wireless repeater (also known as a wireless range extender). In such a case, the access point cannot normally be connected to the wired LAN. Instead, the repeater access point attaches to a “root” access point. The repeater access point allows wireless devices to communicate with it and relays the data to the other access point. Both access points have the same SSID (see Figure 13.47)

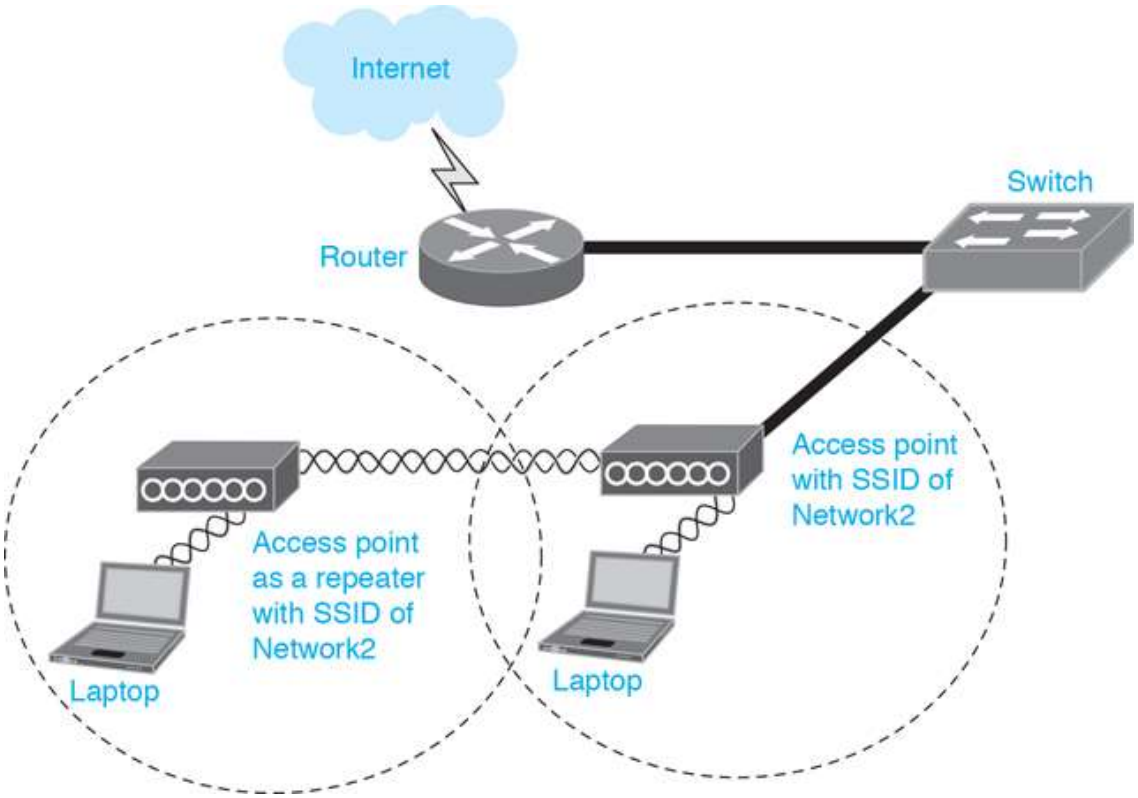


Figure 13.47 Access point as a repeater

Wireless Channel ID

In addition to having an SSID, an access point can be configured with a number known as a channel ID. The **channel**, sometimes called a channel ID, is a specific number that defines at what frequency the access point operates. With an AP that has a 2.4 GHz antenna, up to 14 channels are available, depending on where in the world the wireless network is deployed. In the United States, only 11 channels are used; they are listed in Table 13.17.

Table 13.17 Wireless frequency channels

Channel ID number	Frequency (in GHz)
1	2.412
2	2.417

Channel ID number	Frequency (in GHz)
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

The frequencies shown in Table 13.17 are center frequencies. The center frequencies are spaced 5 MHz apart. Each channel is actually a range of frequencies. For example, the channel 1 range is 2.401 to 2.423, with the center frequency being 2.412.

'ech Tip Channel ID must match

The channel ID (frequency) must be the same between an access point and a wireless NIC for communication to occur between any wireless devices on the network. The wireless NIC can adjust to the same frequency as the AP so communication can occur.

The three commonly used nonoverlapping channe
11. By using these three channel IDs, each of three ac
near one another does not experience interference fr

This is because each center frequency does not overlap with the adjacent frequency channels (see Figure 13.48).

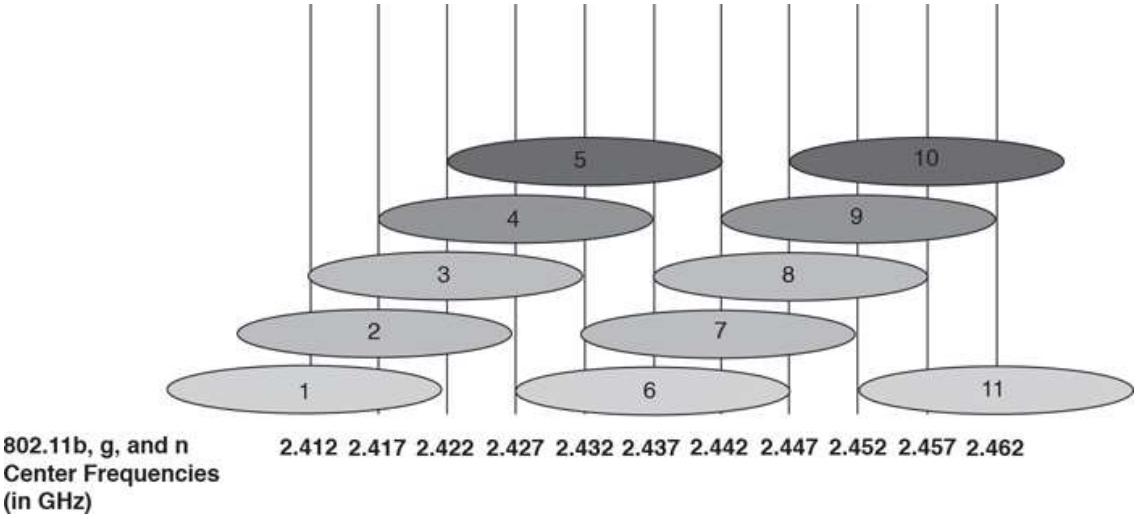


Figure 13.48 802.11b/g/n 2.4 GHz nonoverlapping channels

Notice in Figure 13.48 that each center frequency is 5 MHz from the next center frequency. Also notice that each channel is actually a range of frequencies, as shown by the shaded ovals. Channels 1, 6, and 11 clearly do not overlap and do not interfere with each other. Other nonoverlapping channel combinations could be Channels 2 and 7, Channels 3 and 8, Channels 4 and 9, and Channels 5 and 10. The combination of Channels 1, 6, and 11 is preferred because it gives you three channels with which to work. Figure 13.49 shows a different way of looking at how Channels 1, 6, and 11 do not overlap.

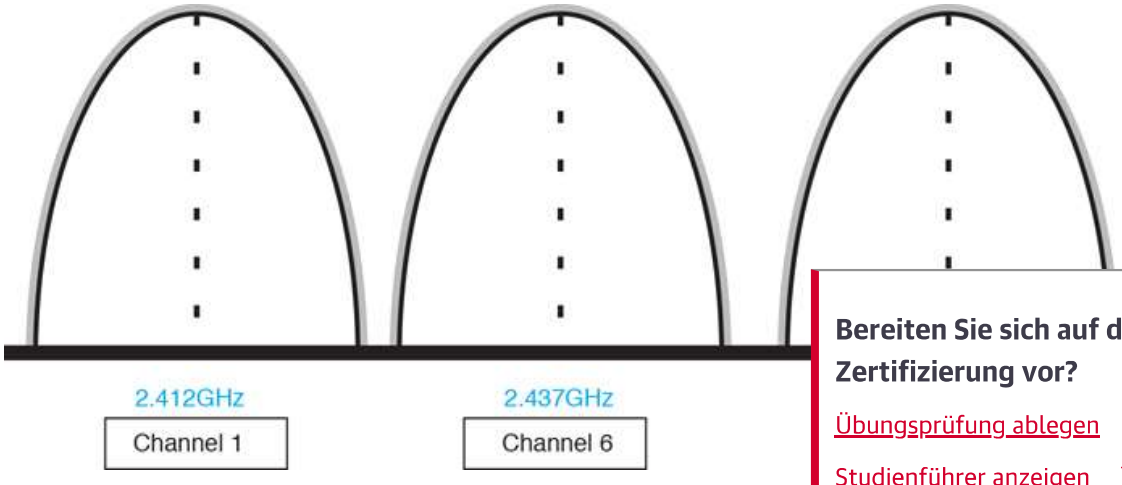


Figure 13.49 2.4 GHz channel IDs 1, 6, and 11

Figure 13.50 shows how the three nonoverlapping channels can be used to attain extended coverage even with multiple access points. Note that where there is blank space between the circles, no wireless coverage exists. The circles can be adjusted so that coverage is complete, but a slight overlap of channels will occur.

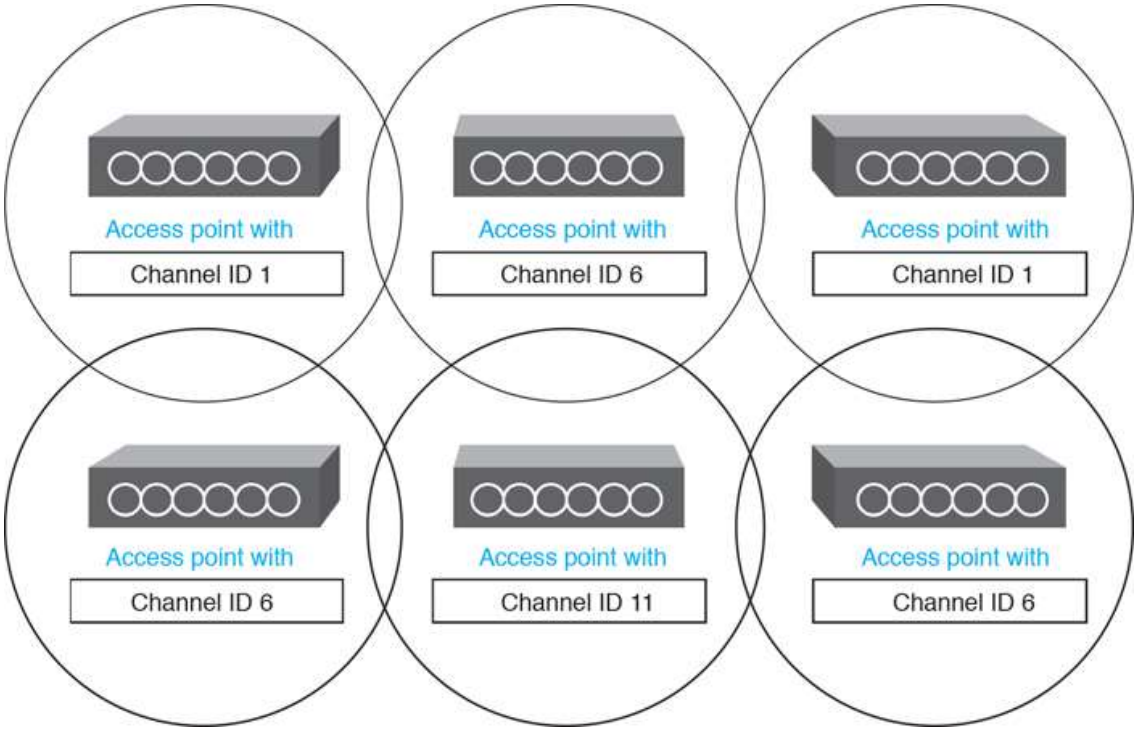


Figure 13.50 802.11b/g/n nonoverlapping channel IDs

With 802.11a, 12 20 MHz channels are available in the 5 GHz range. 802.11n supports 20 and 40 MHz channels. 802.11ac supports 20, 40, 80, and 160 MHz channels. The 5 GHz range has three subranges called Unlicensed National Information Infrastructure (UNII): UNII-1, UNII-2, and UNII-3. All bands can be used for indoor and out
13.51 shows the 5 GHz channels.

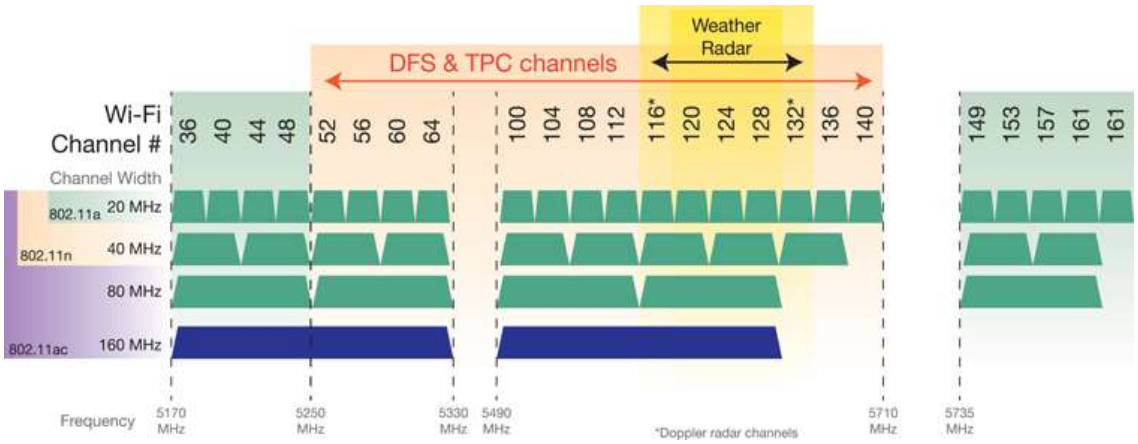


Figure 13.51 802.11 a/n/ac 5 GHz channel IDs

Devices that work in the UNII-2 frequency ranges must support dynamic frequency selection (DFS) and transmit power control (TPC) to avoid interference with military applications. These two terms are most often shortened to simply *DFS channels*. Channels 120, 124, and 128 are used for terminal Doppler weather radar (TDWR) systems. Channels 116 and 132 may optionally be used for Doppler radar. Most wireless routers can automatically configure themselves with the best channel, but if the surrounding area has interfering devices, this may need to be manually planned and configured. Figure 13.52 shows how you can select a specific 2.4 or 5 GHz channel on a TP-Link wireless router (and the transmit power is the option below that).

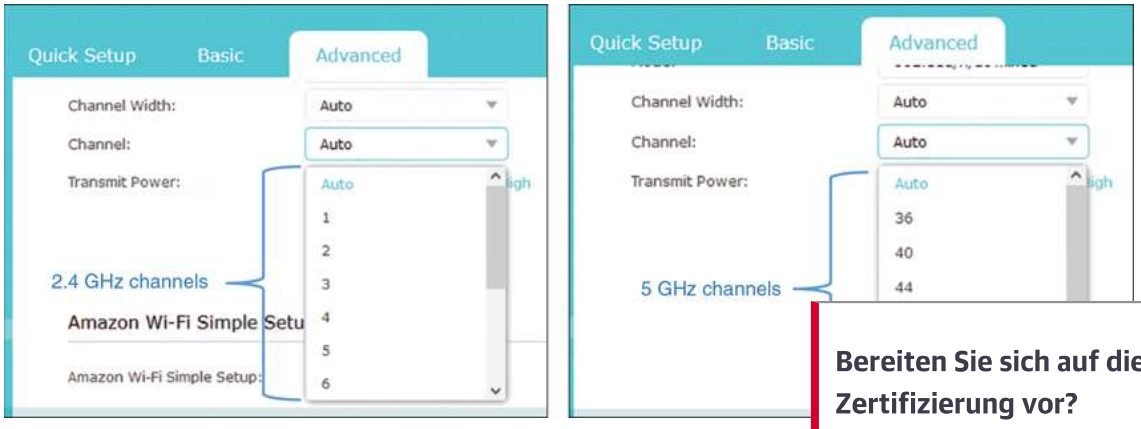


Figure 13.52 2.4 and 5 GHz channel selection

An important point to make is that the frequency ranges, channel ID, number of channels, subchannel range, and so on must adhere to the **wireless regulations**. Most countries also regulate maximum wireless power levels that differ for indoor networks as well as outdoor networks and change often. The good news is there is some consistency in the 2.4 GHz and 5 GHz ranges so that a laptop used in the United States will work on the wireless networks in other countries.

Antenna Basics

Wireless cards and access points can have either external or built-in antennas. Some access points also have integrated antennas. Wireless NICs and access points can also have detachable antennas, depending on the make and model. An antenna radiates or receives radio waves. You can simply move an external antenna to a different angle to obtain a better connection. With some laptops, you must turn the laptop to a different angle to attach to an access point or get a stronger signal (and, therefore, faster transfers). Antenna placement is important in a wireless network.

'ech Tip Where is the wireless antenna on a laptop?

For laptops with integrated wireless NICs, the wireless antenna is usually built in to the laptop display for best connectivity.

There are two major categories of antennas: omnidirectional and directional. An **omnidirectional antenna** radiates energy in all directions. Integrated wireless NICs use omnidirectional antennas. Refer to Figure 10.67 in Chapter 10 to see how the antenna wires attach to two posts on the wireless NIC. These wires connect the antenna to
laptop always has low signal strength, ensure that th
attached.

A **directional antenna** radiates energy in a specific direction. Directional antennas are frequently used to connect two buildings together or to limit wireless connectivity outside a building. Each antenna has a specific radiation pattern (sometimes called a propagation pattern), which is the direction(s) the radio frequency is sent or received. It is the coverage area for the antenna that is normally shown in a graphical representation in the antenna manufacturer's specifications. Figure 13.53 shows the difference in radiation patterns between omnidirectional and directional antennas.

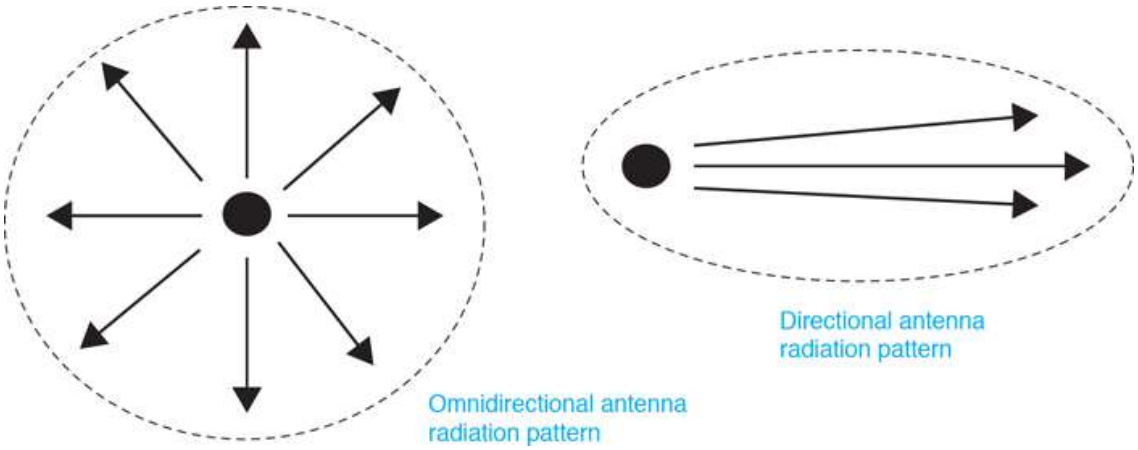


Figure 13.53 Basic antenna radiation patterns

A technician must be familiar with an antenna's radiation pattern so that the appropriate type of antenna can be chosen for the installation. As a signal is radiated from an antenna, some of the signal is lost. Attenuation, which is sometimes called path loss, is the amount of signal loss of a radio wave as it travels (that is, is propagated) through air. Attenuation is measured in decibels (dB), which are a measure of the ratio between two signal levels.

Factors that affect an antenna's attenuation are the distance between the transmitting antenna and the receiving antenna, any obstructions between the two antennas, and how high the antenna is mounted. Another factor that affects wireless transmission is interference, including radio frequencies being transmitted using the same frequency range and external noise. Other wireless devices, wireless networks, cordless phones, and microwave ovens are common sources of interferenc

'ech Tip What is the maximum distance of a wireless networ

The maximum distance of a wireless network depends on the wireless network standard used, the antenna attached to the AP, and the attenuation experienced.

An important concept related to antennas is gain, and to understand gain, isotropic antennas must be discussed. An isotropic antenna is not real; it is an imaginary antenna that is perfect in that it theoretically transmits an equal amount of power in all directions. The omnidirectional radiation pattern previously shown in Figure 13.53 would be the pattern of an isotropic antenna. A lot of ceiling-mounted APs have omnidirectional antennas. Figure 13.54 shows an AP that could be mounted on the ceiling and might have integrated omnidirectional antennas.

Figure 13.54 Ceiling-mounted AP

Antenna power levels are described as antenna ga
in dBi or dBd (dBd equals 2.14 dBi). More gain means
particular direction. A technician must sometimes re
power (that is, lower the signal strength) in order for
access points to function in the same building or area.

'ech Tip You might need to reduce power levels

If an open wireless network is being used by adjacent businesses, reduce the power level of the antenna to reduce the wireless network coverage area.

A **site survey** is an examination of an area to determine the best access point or antenna placement. To conduct such a survey, temporarily mount an access point (or use a telescoping pole to place the AP at different heights). With a laptop that has a wireless NIC and site survey software, walk around the wireless network area to see the coverage range. Some vendors provide site survey software with their wireless NICs.

A site survey can also be conducted by using a laptop and walking around and using the wireless network icon on the taskbar to see the signal strength. Radio waves are affected by obstructions such as walls, trees, rain, snow, fog, and buildings. Radio waves are also affected by **external interference** from other devices and other wireless networks operating in the same frequency range causing **intermittent wireless connectivity**. Figure 13.55 shows a wireless antenna signal strength display on a laptop.

Figure 13.55 Signal strength

'ech Tip The higher the decibel rating, the better the signal

The type of radio antenna and antenna gain affect th
However, no matter how good the antenna, as a wire
farther away from an access point or another wireless device, the more

attenuation occurs. Walls, trees, obstacles, and other radio waves can cause attenuation.

A **Wi-Fi analyzer** or wireless locator can determine whether there are wireless networks or hotspots in the area. It can also locate wireless devices that can be attached to pets, people, keys, remotes, and so on. A phone or mobile device app can also locate a powered mobile device or locate a person who has a mobile device with this enabled.

Multiple input/multiple output (**MIMO**) uses multiple 2.4 GHz and 5 GHz antennas. Figure 13.56 shows an example of MIMO transmissions. Note that although each client that attaches to an AP using MIMO can have multiple data streams, the AP handles one client at a time.

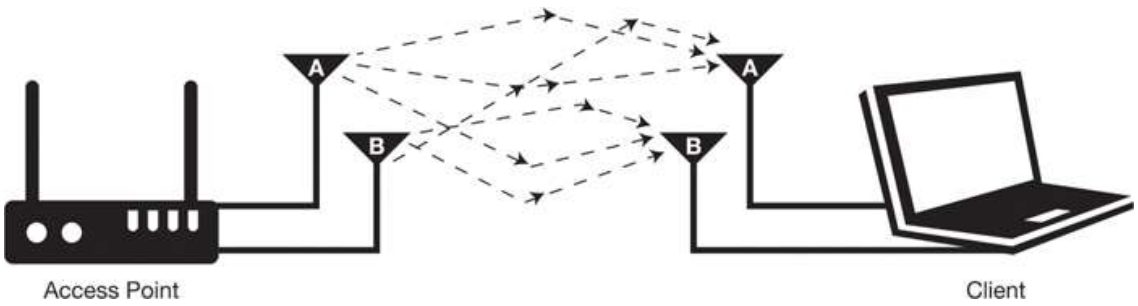


Figure 13.56 MIMO transmissions

MIMO antennas may be external or built in to a wireless device. Greater wireless speeds can be achieved by using multiple antennas. 802.11n, 802.11ac, and 802.11ax radios are defined by how many antennas can transmit and receive as well as the number of data streams supported. The documentation is commonly in a number formatted such as 2x2:1 or 4x4:4. The first number is the maximum number of antennas that can transmit. The second number is the number of antennas that can receive data. The last number is the number of data s
802.11ac and 802.11ax use multi-user MIMO (MU-MI
eight simultaneous streams. MU-MIMO serves multip

ously, whereas with pre-802.11ac implementations, an AP serves only one user at a time.

Wireless Data Transfer Speeds

The data transfer speed between a wireless NIC and an access point or another wireless device is automatically negotiated for the fastest transfer possible. The farther away from an access point a wireless device is located, the lower the speed. A low radio frequency signal (or **low RF signal**) could simply mean the device is too far from the access point and results in **slow network speeds** as well as intermittent wireless connectivity. Move closer or change the angle of the device to get a better signal. Figure 13.57 shows this concept.

External interference can also influence wireless connectivity and wireless transfer speeds. Check the area for devices or other wireless networks using the same frequency. Don't forget that walls, structures, and other objects also affect wireless reception/speeds.

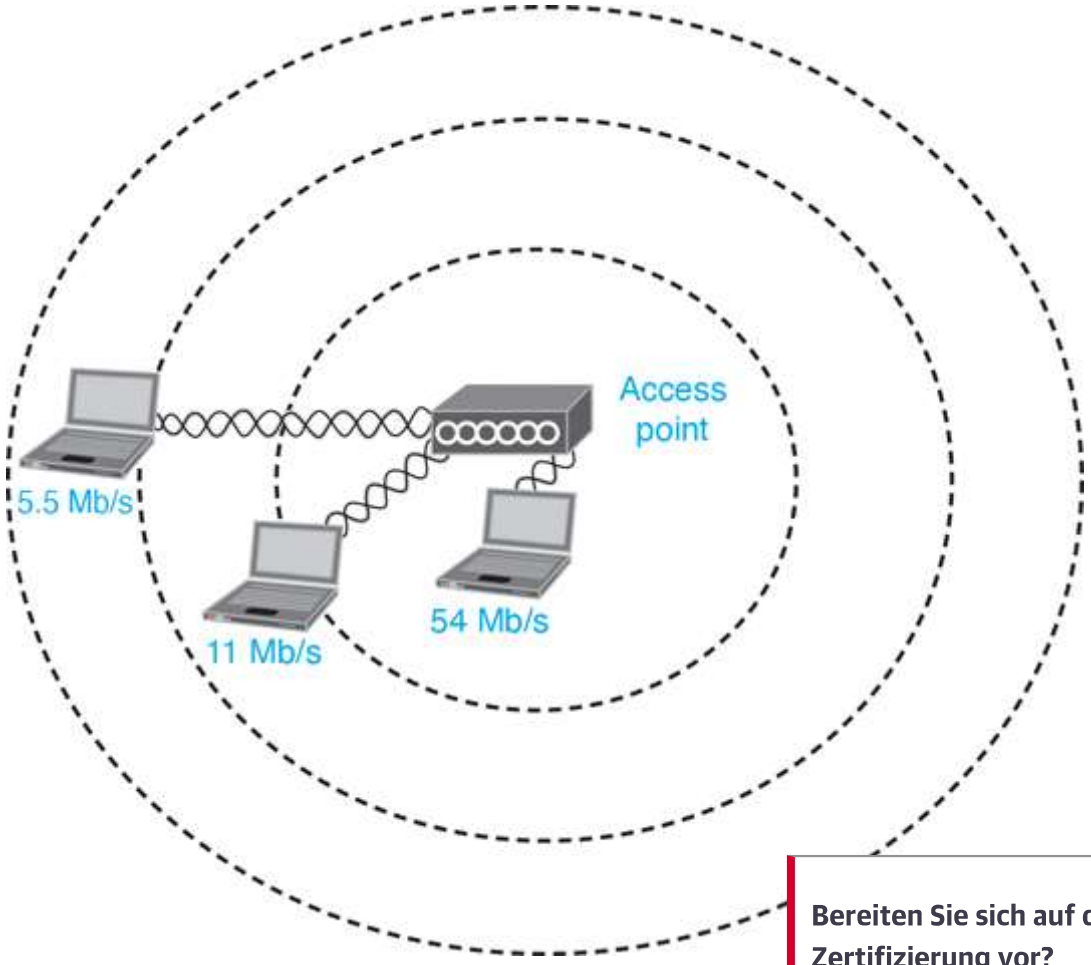


Figure 13.57 Wireless connectivity speed ranges

Wireless and Wired Client Device Configuration Overview

When you are connecting a device to a wired or wireless network, many things might have to be done, such as the following:

- Configure IP addressing.
- If the computer wants to share a printer or folders, file and print sharing might need to be enabled.
- If the device is on a corporate network, the device might have to be put on the domain with a unique name.
- If a wireless device is being configured, the SSID and possibly security parameters need to be entered.

'ech Tip How to name a computer

In Windows, name a computer using the *System* section of the Control Panels or use the *Settings* > *System* option. Each device on the same network must be given a unique name.

Configuring an End Device: IP Addressing

No matter what device connects to a wired or wireless network, the device must have an IP address so that it is uniquely identified on the network. Every device on a wired or wireless network needs three important pieces of information: an IP address, subnet mask, and default gateway. The IP address and subnet mask are what make the network device unique and allow it to be reached by other devices. There are two ways to get IP addressing information: statically define the IP address and subnet mask or dynamically obtain the address/mask by usi
also needs a default gateway IP address in order to c
other networks.

'ech Tip My computer's IP address changes

A computer's IP address can change each time the computer boots because with DHCP, the DHCP server issues an IP address for a specific amount of time.

Statically Configuring an IP Address

When an IP address is statically defined, someone manually enters an IP address and mask into the computer as follows:

- *Windows 7/8/10/11:* Access *Network and Sharing Center* Control Panel > *Change Adapter Settings* link.
- *Windows 10/11:* Access *Settings* > *Network & Internet* > *Change adapter options* link.

Most support staff do not statically define IP addresses except for devices that are network infrastructure devices, such as web servers, database servers, other network servers, routers, or switches. Figure 13.58 shows the window that appears when you right-click a particular adapter and select *Properties* > *Internet Protocol Version 4 (TCP/IPv4)* > *Properties* button.

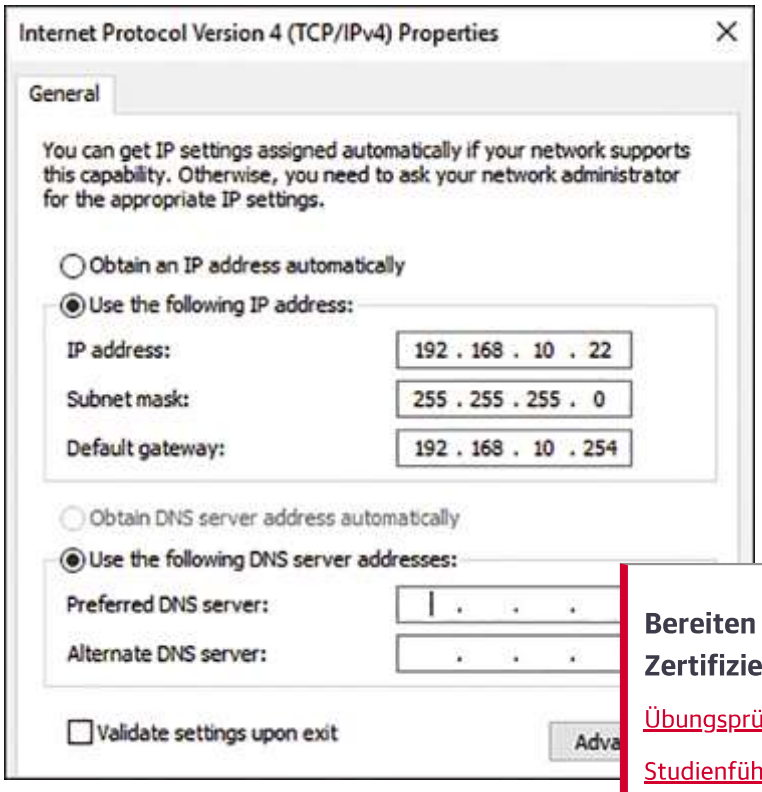


Figure 13.58 IP address configuration using a NIC's Properties

In Windows *Settings* > *Network* & *Internet*, you select either *Ethernet* from the left menu and then select the Ethernet connection shown in the pane on the right. Scroll to the *IP settings* section and select *Edit*. In the *Edit IP settings* dialog box, use the arrow to select *Manual* > and click on the *IPv4* slide option, as shown in Figure 13.59.

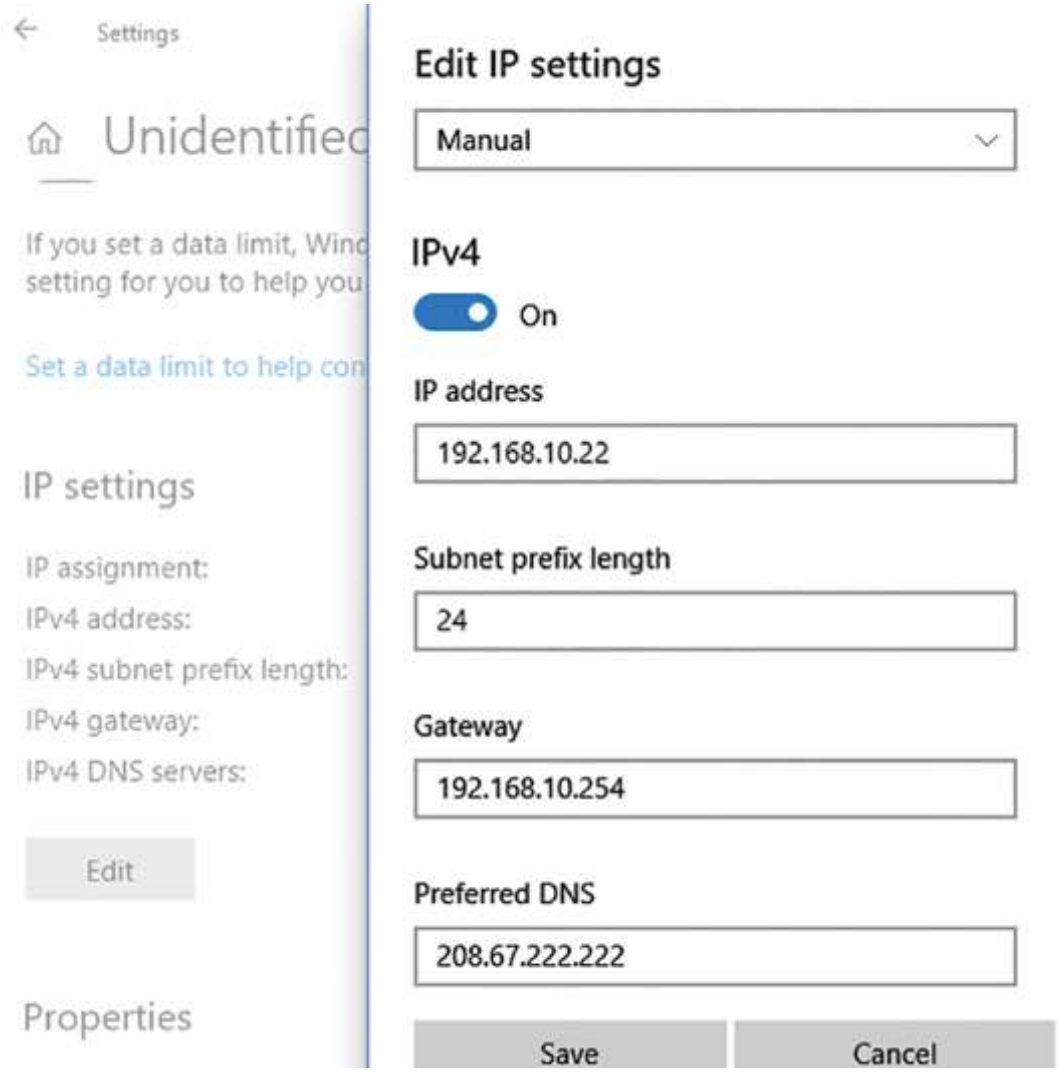


Figure 13.59 IP address configuration using Windows Settings

'ech Tip What happens if you assign the same IP address to two devices?

Entering an IP address that is a duplicate of the address for another network device renders the new network device inoperable on the network and could affect the other device's traffic as well.

Another place that you might need to configure a static IP address is on a wireless router. Most of the time you automatically get an IP address when connecting a router to the internet, but sometimes if a router connects to another router or if you request a static address from the provider, you need to go into the wireless router's configuration and select a static WAN IP address. This is commonly done through the WAN or internet option and selecting *Static IP*, as shown on the TP-Link wireless router configuration screen in Figure 13.60. The *Dynamic IP* option is the default and is used when the address is sent from the internet provider.

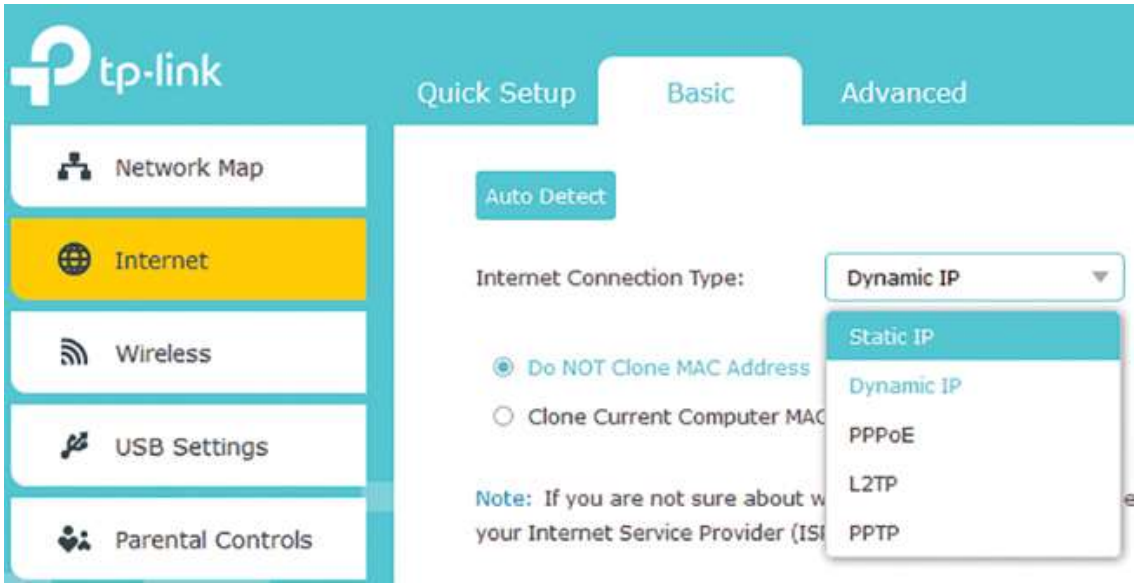


Figure 13.60 Static WAN IP address configuration on a wireless router using DHCP

Dynamic Host Configuration Protocol (**DHCP**) is a
sign IP addresses to network devices. A **DHCP server**
ured on a network server, router, or wireless router)
addresses known as a **DHCP scope** that defines the st

addresses that can be issued to network devices. Commonly on servers or routers, you have to give the DHCP pool/scope a name before entering the range of IP addresses, but on a wireless router used for home or small business, you just enter the IP addresses and ensure that the DHCP server option is enabled, as shown in Figure 13.61.

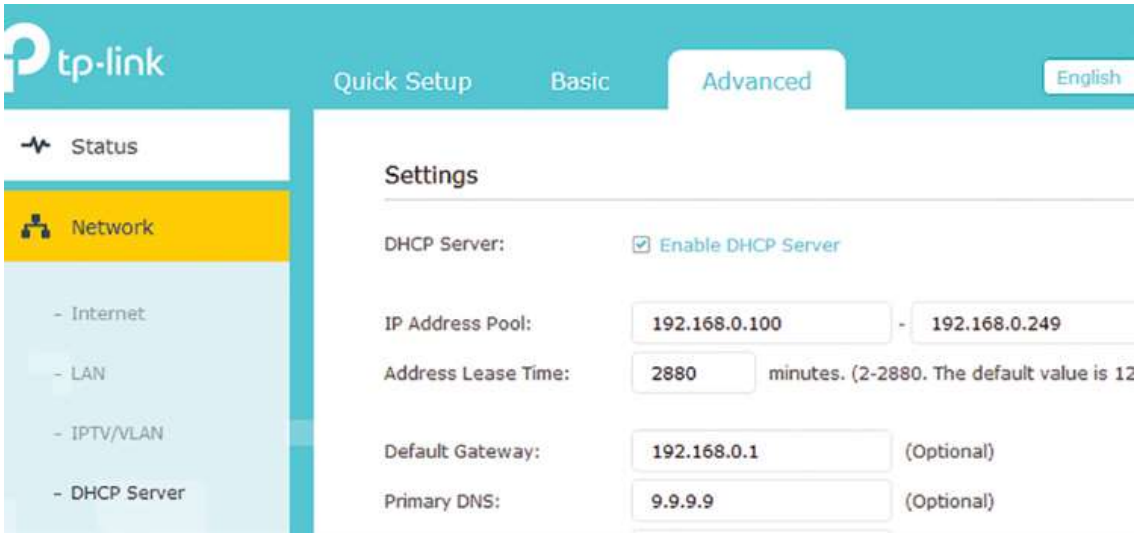


Figure 13.61 DHCP configuration on a wireless router

When a network device has been configured for DHCP and it boots, the device sends out a DHCP request for an IP address. A DHCP server responds to this request and issues an IP address to the network device that may be used for a specific period of time, such as a day or longer, depending on the **DHCP lease time** configured on the DHCP server. The default IP address lease time varies by vendor. For example, TP-Link has the lease time in minutes, with a max of 2880, or 2 days (refer to Figure 13.61). DHCP makes IP addressing easy and prevents network devices from being assigned duplicate IP addresses.

An important configuration on a DHCP server is a **DHCP reservation**, which is an IP address reserved for a particular devi or printer. Instead of statically assigning an IP addre nician enters the physical address (the MAC address) as a network printer, into the DHCP server and the IP

signed to the device. No other device will get that IP address, and the device will always get the reserved IP address. On the DHCP server, each network is configured with a starting IP address and an ending IP address. A technician can also create a range of reserved IP addresses that will not be issued to network devices by the DHCP server but that can be statically configured on the device as an alternative to making an individual reservation on the DHCP server for each device. Figure 13.62 shows this concept.

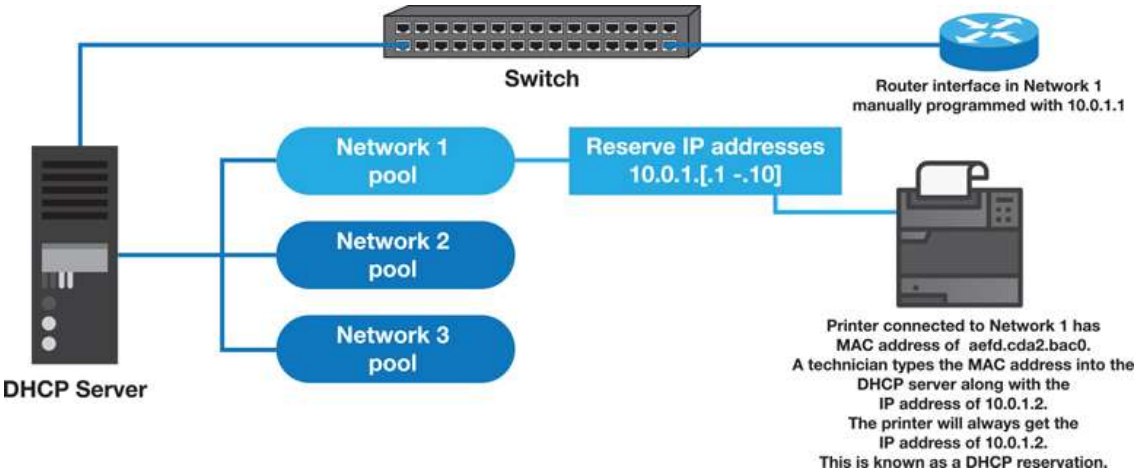


Figure 13.62 DHCP reservations

To configure client-side DHCP in Windows, access the *Network and Sharing Center* Control Panel > access the *Change adapter settings* link > right-click or tap and briefly hold on the wired and wireless NIC and select *Properties* > double-click on the *Internet Protocol Version 4 (TCP/IPv4)* option > ensure the *Obtain an IP address automatically* radio button is enabled (refer to Figure 13.58). In Windows *Settings* > *Network & Internet*, you select either *Ethernet* from the left menu and then select the Ethernet connection shown in the pane on the right. Scroll to the *IP settings* section and select *Edit*. In the *Edit IP Settings* dialog box, use *Automatic (DHCP)*.

'ech Tip Watch out for duplicate IP address messages

If a device displays a message relating to a duplicate IP address, check the device to see if a static IP address has been assigned (and to see if the DHCP server issued the same address to a different device or vice versa). If a computer cannot communicate on a network, use the command to verify that the computer received an IP address. If a computer cannot communicate on a remote network, use the command to verify that the computer received a default gateway. ipconfig `ipconfig`

APIPA

Windows computers support automatic private IP addressing (**APIPA**), which assigns an IP address and mask to the computer when a DHCP server is not available but continues trying to contact the server at five-minute intervals. The IP addresses assigned are 169.254.0.1 to 169.254.255.254. No two computers get the same IP address. If you can connect to other computers on your local network but cannot reach the internet or other networks, it is likely that the DHCP server is down and Windows has automatically used APIPA to assign an address. To determine if APIPA is configured, open a command prompt window and type . If you see the words *Autoconfiguration Enabled Yes,* APIPA is turned on. If the last word is *No,* APIPA is disabled. `ipconfig /all`

Configuring an Alternative IP Address

An alternative configuration is used when a DHCP server cannot assign an IP address, such as when there are network problems or the DHCP server is down. An alternative IP address could also be used on a laptop when DHCP is used at work, but addresses are statically assigned at home, for example. Figure 13.63 shows the *Alternate Configuration* tab settings. Note that this tab appears only if you have the *Obtain an IP address automatically* radio button enabled on the *General* tab of the *Internet Protocol Version 4 (TCP/IPv4) Properties* window.

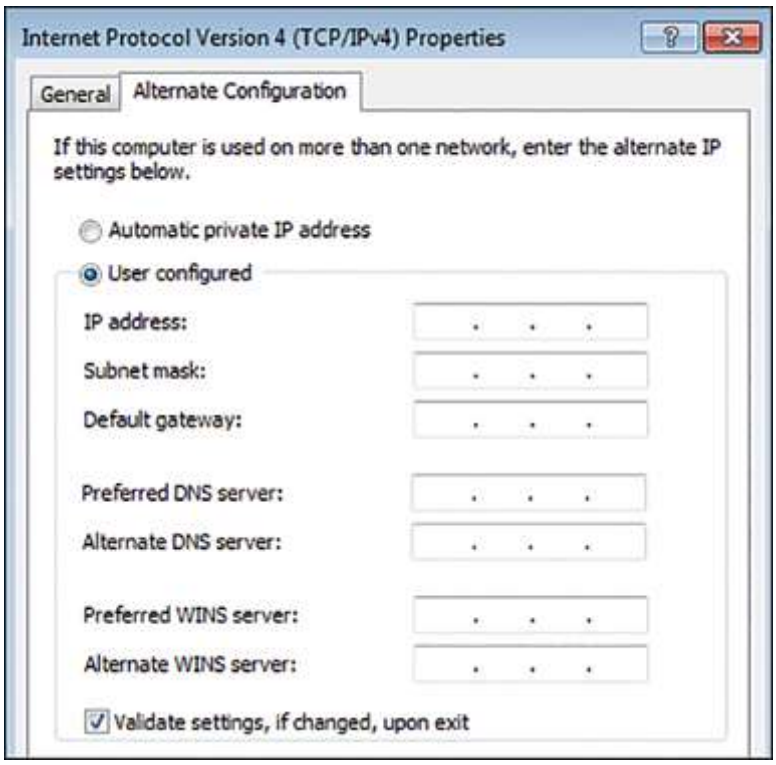


Figure 13.63 Alternate Configuration tab

Default Gateway

Another important concept that relates to IP addressing is a default gateway (sometimes called *gateway of last resort* or simply **gateway**). A **default gateway** is an IP address assigned to a network device that tells the device where to send a packet that is going to a remote network. Default gateway addresses are important for network devices to communicate with network devices on other networks. The default gateway address is the IP address of the router that is directly connected to that immediate network. Keep in mind that the primary job of a router is to find the best path to another network. Routers send traffic from one network to another throughout the internet. Your router at home might be used to get traffic from your wireless network and your wired network out to the internet. Consider Figure 13.64, which shows a router moving traffic from the network on the left to the network on the right (o

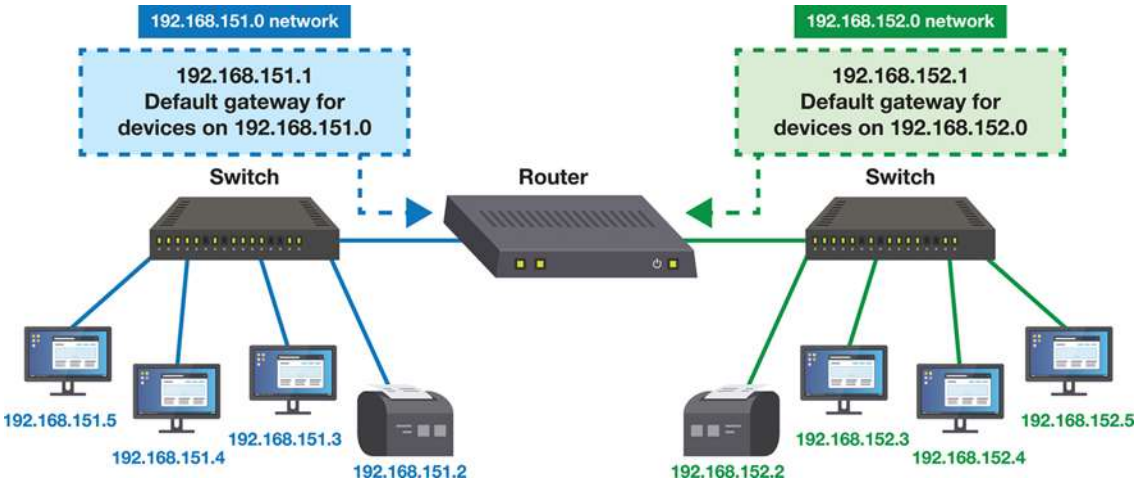


Figure 13.64 Default gateway addresses for two different networks

In the network shown in Figure 13.64, network devices on the 192.168.151.0 network use the router IP address 192.168.151.1 as a default gateway address. When a network device on the 192.168.151.0 network wants to send a packet to the other network, the device sends the packet to the default gateway, the router. The router, in turn, looks up the destination address in its routing table and sends the packet out the other router interface (192.168.152.1) to the device on the 192.168.152.0 network.

The default gateway address for all network devices on the 192.168.152.0 network is 192.168.152.1, the router's IP address on the same network. Any network device on 192.168.152.0 sending information to another network sends the packet to the default gateway address.

'ech Tip How do I assign a default gateway?

If you are statically assigning an IP address, the defau
is configured using the *Network and Sharing Center* C
Network & *Internet* Settings link. Your computer can

ceive a default gateway address through DHCP, just as it receives an IP address and mask.

DNS

One or more DNS server IP addresses may need to be configured or provided through DHCP. Domain Name Service (**DNS**) is an application that runs on a network server (sometimes called a domain name server, or **DNS server**) and translates internet names into IP addresses. DNS is used on the internet so that you do not have to remember the IP address of each site to which you connect. For example, DNS would be used to connect to Pearson Education, Inc. by translating the uniform resource locator (URL) https://www.pearson.com into the IP address 23.197.24.193. Figure 13.65 shows how DNS is organized. An organization can register a second-level domain, but all DNS web address lookups start at the root level.

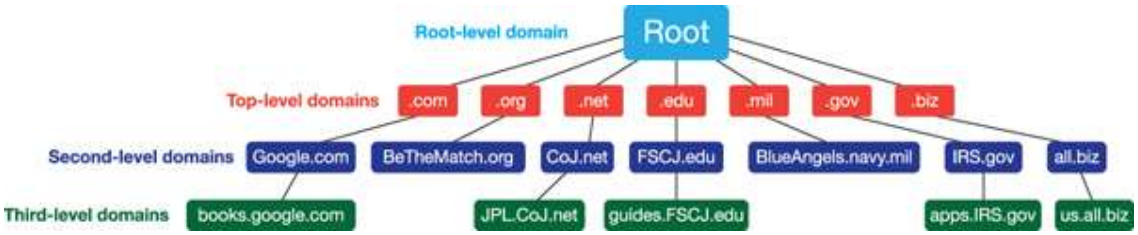


Figure 13.65 DNS address hierarchy

Table 13.18 shows common terms associated with DNS.

Table 13.18 DNS terminology

Term	Explanation

Term	Explanation
A record	An address record that holds the IPv4 address of a particular web address. When the A record contains an at (@) symbol, it means the record is for the root domain.
AAAA record	The DNS record that stores a domain's IPv6 address of a particular website.
MX record	A type of DNS record that forwards email to a mail server in another domain. MX stands for mail exchange.
TXT record	A text record used by administrators for documentation and security (such as email spam prevention and domain verification). Chapter 18, "Computer and Network Security," covers this in more detail.

'ech Tip DNS servers provide name resolution

If a Windows computer is on an Active Directory domain, Active Directory automatically uses DNS to locate other hosts and services using assigned domain names.

If a DNS server does not know a domain name (that is, if it does not have the name in its database), the DNS server can contact another DNS server to get the translation information. Common codes used with DNS (three letters used at the end of a domain name) are (commercial sites), (educational sites), (government sites), (network-related sites), and (miscellaneous sites). `.com .edu .gov .net .org`

Client-side DNS involves configuring a computer to use one or more DNS servers. A computer can be programmed for one
IP addresses by using DHCP. The DHCP server must b
Otherwise, a technician can manually configure the s
more DNS server IP addresses through the *Network a*

Control Panel or *Network* & *Internet* Settings link. Refer to Figures 13.58 and 13.59 to see where to enter the information.

Wired and wireless adapters require IP addresses, default gateways, and DNS configuration, but before any wired or wireless adapters are installed or configured, the basic configuration parameters should be determined.

Adding a Computer to a Windows Domain

In a corporate environment, computers are in a network domain. This means that all the network devices are registered with (joined to) one or more network servers, called *domain controllers*, as shown in Figure 13.66.

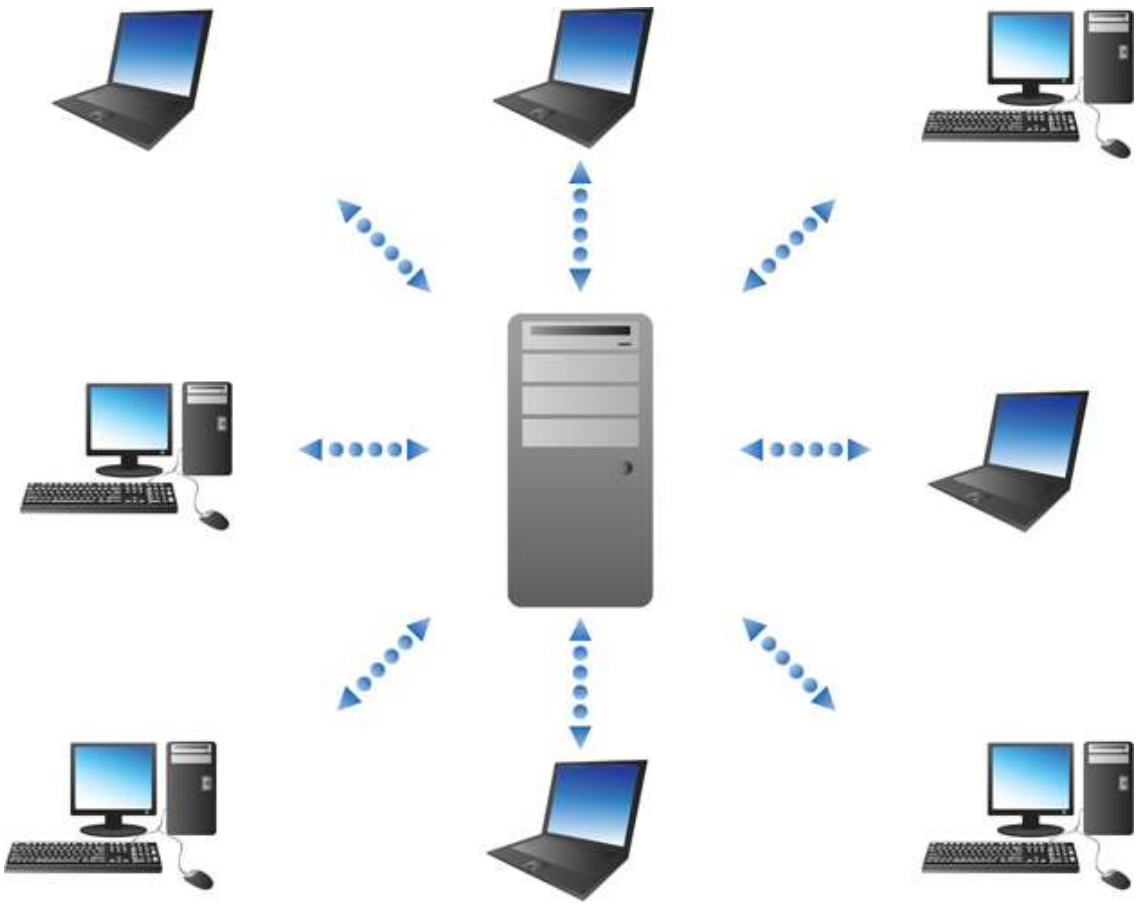


Figure 13.66 Corporate computers joined to a domain controller

A technician who has a domain user account that has the appropriate permission can add devices to the domain. On a Win the *System* Control Panel to access the *Change setting* the *Computer name, domain, and workgroup settings Name* tab > select *Network ID* button > *This computer*

network radio button > *Next* > *My company uses a network with a domain* > *Next* > *Next* > enter a domain user account name that has permission to add a computer to the domain and password > enter a computer name and the domain name > *Next*. Restart the computer. You can also use the *Settings* > *System* link and click the *Join a domain* button.

With macOS, use the *System Preferences* option by clicking the *Apple* icon in the top-left corner > *Accounts* > select *Lock* > *Join* button > *Open Directory Utility* button > select *Lock* > highlight *Active Directory* and select the pencil icon > enter the domain name and a unique computer ID > *Bind* button > enter the domain user account name/password that has permission to add a computer to the domain.

Wireless NIC–Specific Settings

Not all computers in a wireless network need the same type of wireless NIC, but each NIC does require configuration to join a wireless network. After a wireless adapter is installed, SSID and security options can be entered. Specific security options are covered in Chapter 18. Wireless parameters can be configured through a utility provided by the wireless NIC manufacturer or through Windows by selecting the wireless network icon in the notification area, selecting the wireless network shown, and entering the required security information.

If the SSID is not being broadcast (that is, if you see **SSID not found** in the list of available wireless networks), a wireless network can be manually entered using the following procedure for Windows: *Network and Sharing Center* Control Panel > *Set up a new connection or network* link > *Manually connect to a wireless network* option (see Figure 13.67).

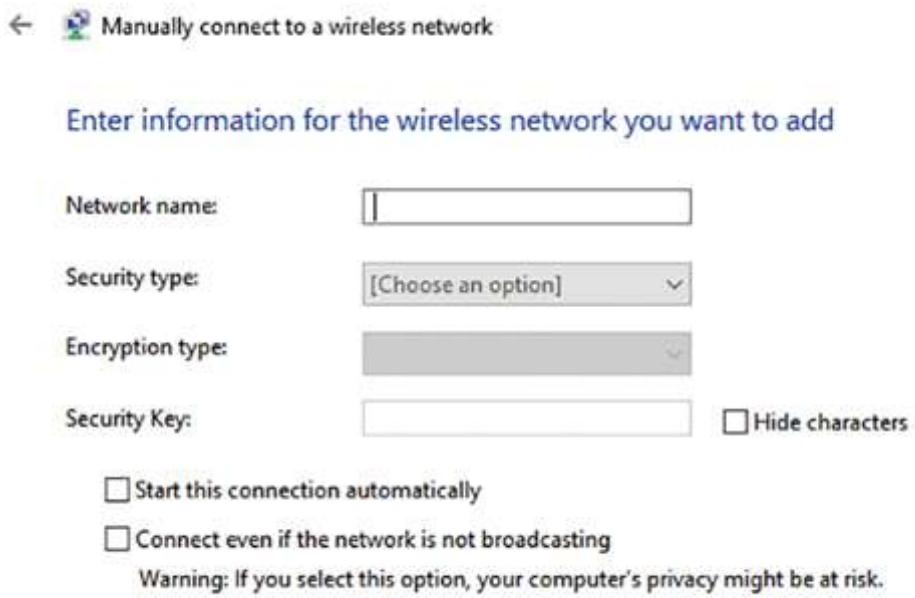


Figure 13.67 Manually entering wireless configuration information in Windows

'ech Tip Ensure that a laptop's wireless NIC is enabled

If a laptop cannot connect to a wireless network, make sure the wireless NIC is enabled. It can be enabled/disabled through the use of a Fn key.

Another common setting for wireless NICs is the type of encryption used. Encryption is covered in Chapter 18, along with other wireless security measures. The following types of encryption can be chosen and must match what is configured on the wireless AP/router (see Figure 13.68):

- *Wireless Encryption Protocol (WEP):* 64- and 128-bit versions
- *Temporal Key Integrity Protocol (TKIP):* May be seen in combination with Wi-Fi Protected Access (WPA) and/or WPA2
- **WPA**: Might be seen with Preshared Keys (PSK), m
  and/or TKIP
- **WPA2**: Uses the Counter Mode Block Chaining Me
  Code Protocol (CCMP) for added security (might b

TKIP)

- *WPA2 with Advanced Encryption Standard (AES):* Uses a block cipher and has key lengths of 28, 192, or 256 bits, with the longer key lengths being the stronger.
- **WPA3**: Uses 128-bit (in Personal mode) or 192-bit (in Enterprise mode) encryption and a four-way handshake called Simultaneous Authentication of Equals (SAE) for authentication

Figure 13.68 Wireless security options

Wireless NICs are easy to install. Be sure to follow the manufacturer's instructions. All the screens and configuration utilities have the same type of information. Understanding what the configuration parameters mean is important. The hardest part about configuring wireless NICs is obtaining the correct parameters before installation begins. Incorrectly inputting any one of the parameters prevents the wireless NIC from joining the wireless network. Planning is critical for configuring wireless NICs.

Advanced NIC Properties

Both wired and wireless NICs have some optional parameters that can be manually configured. These options are shown in Figure 13.69 and discussed in Table 13.19. Access these parameters by right-clicking the NIC from within the *Networking and Sharing Center* Control Panel > *Properties* > *Configure* button > *Advanced* tab.

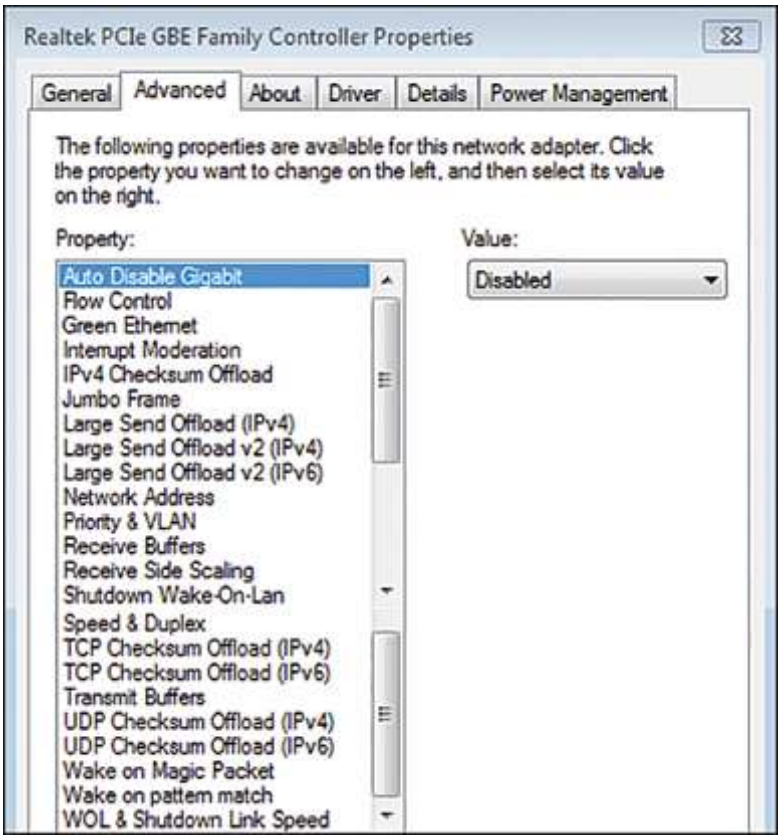


Figure 13.69 NIC advanced properties

Table 13.19 Network card properties

Configuration property	Description
Duplex	Options include half duplex/full duplex/auto. The default is auto or auto negotiation. Duplex might be combined with the Speed configuration option. Speed/duplex should be manually configured on an important device such as a server or checked if the device is experiencing high latency.
On-board NIC (BIOS/UEFI)	If a wired or wireless NIC is integ motherboard or mobile device, yo access BIOS/UEFI to configure sor related to the NIC.

Configuration property	Description
Quality of Service (QoS)	Some NICs have the capability to have QoS features enabled. This allows tagging certain packets for priority transmission. Other similar options might be *Priority and VLAN* or *Tagging*.
Speed (NIC property)	Speed is normally automatically configured, but manual options include 10 Gbps, 1 Gbps, 100 Mbps, and 10 Mbps.
Wake on LAN	This setting allows the computer to be brought out of a low power mode to have configuration changes or updates made. It is usually enabled through the BIOS but can also be set through the NIC properties *Advanced* tab. Other options might include Wake on Magic Packet or WOL.

NIC Configuration When Using Virtualization

Virtualization allows a single computer to host multiple operating systems that share hardware resources. When you configure a computer for virtualization, part of that virtualization is a virtual network interface card, or virtual NIC. One virtual NIC is standard in a virtual machine. More virtual NICs can be assigned. A physical network device has at least one NIC, but if the device is a server, it has more than one NIC.

Each virtual NIC has its own MAC address and can have an IP address assigned. If more than one virtual machine is installed, each can communicate with the other machine based on the NIC settings configured. Furthermore, the virtual NIC can go through the physical NIC and have internet access in the virtual environment. If the virtual machine doesn't have network connectivity, but the host workstation
tual NIC settings. Figure 13.70 illustrates three virtua
Linux, one Windows, and one Microsoft Server, for e
ical machine connecting to the one physical NIC even
machine has its own virtual NIC.

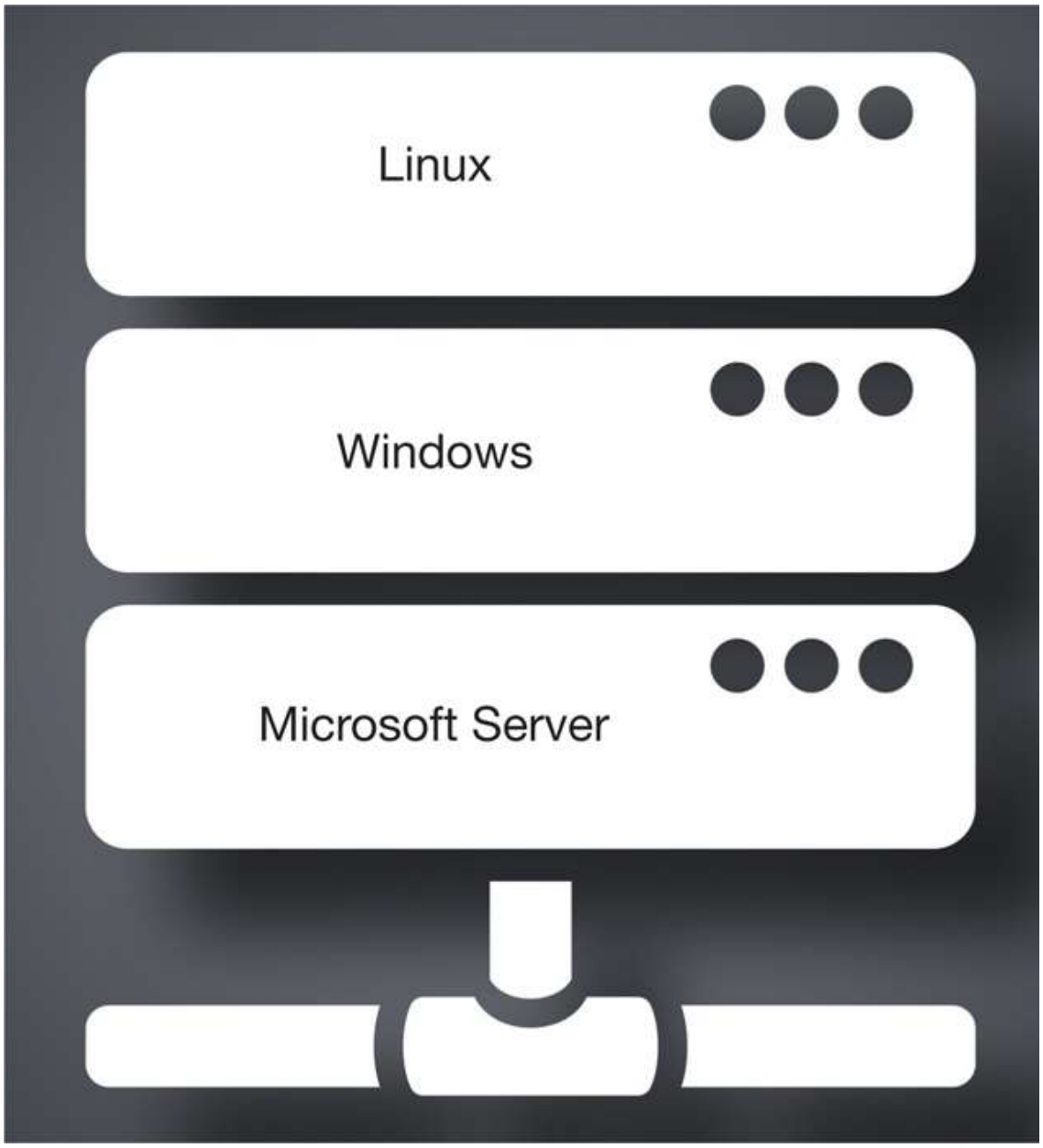


Figure 13.70 VMs connecting to a network

Rather than go into all of the different virtualization vendors' products, let's examine VMware Workstation's NIC settings. Other vendors have similar configurations. In VMware Workstation, a NIC can be configured for bridged, network address translation (NAT), host-only, or custom mode. Table 13.20 describes these modes.

Table 13.20 Virtualized NIC modes of operation

Mode	Description

Mode	Description
Bridged	The NIC is normally manually configured and has access to the host machine's NIC (which normally is connected to the internet and provides internet access to the virtual machine).
Custom	Select the VM network that the NIC is assigned to.
Host-only	Other virtual machines configured with an IP address on the same network can see and communicate with one another. DHCP is supported.
NAT (network address translation)	Cannot be seen by other virtual machines but can use the host machine's NIC for internet access. DHCP is also supported.

Thin or Thick Client Installation Overview

Thin client and *thick client* are terms used in the corporate environment. A business computer that is a tower under someone's desk is likely to be a thick client; thick clients are the most common. A thick client has software applications loaded on the local hard drive. In contrast, a thin client is an all-in-one unit or a small computer that usually mounts to the back of a monitor, as shown in Figure 13.71.

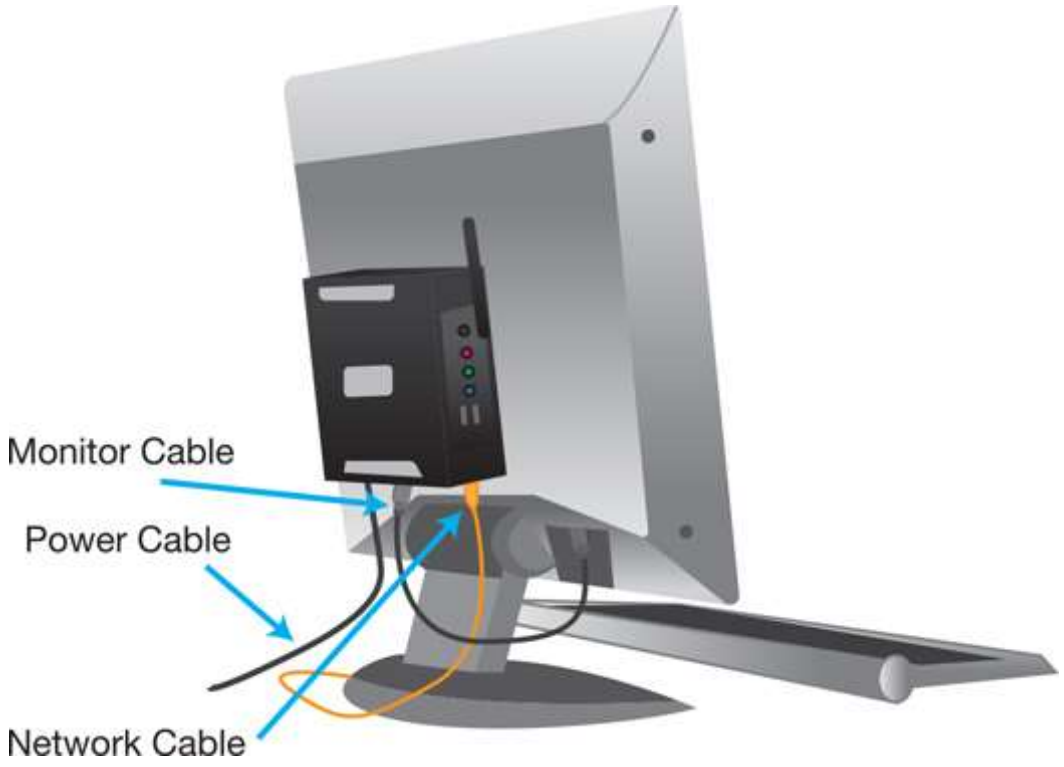


Figure 13.71 Thin client computer

A thin client does not have a hard drive, and it runs all the software from a network server. Thin clients have very few ports. Both thin and thick clients take advantage of and attach to the corporate network.

Thin Client Installation

Before installing a thin client, you need to ensure that the thin client hardware has the minimum hardware to run the server-based applications and a cable to connect to the network. Normally, companies that use thin clients have a system image already configured and stored somewhere. Image management software is used for creating, storing, modifying, and deploying an operating system image to the thin client. Some companies use a server and use Remote Desktop Services (previously called Terminal Services). **Remote Desktop Services** is software on a server that can be accessed by multiple client sessions running simultaneously. This is important when thin clients are used because you can deploy and manage Windows-based applications. Remote Desktop Services can also be used to access and control (manage) remote Windows-based computers and servers.

Settings that relate to thin client installation throu
agement software or Remote Desktop Services includ

- MAC and/or IP address of the thin client
- Schedule settings, including what days and within which time periods the thin client can be used
- Monitor settings, such as resolution, color depth, and refresh rate
- Domain/username, such as the Windows network domain name and the username of the person(s) using the thin client computer
- Hardware drivers

To install a thin client computer, be sure to follow corporate guidelines. Here are the generic steps involved:

Step 1. The thin client may be an all-in-one unit that requires no assembly or a computer and a monitor (which might include a stand to attach both components). If using a computer, monitor, and stand, place the pieces into the stand and secure with screws as needed.

Step 2. Attach power to the thin client.

Step 3. Attach the Ethernet network cable from the wall outlet or cubicle outlet to the Ethernet port on the thin client.

Step 4. Attach the mouse and keyboard to the proper ports.

Step 5. If using a computer and monitor, attach the appropriate video cable from the computer video port to the monitor port.

Step 6. If using an external monitor, attach power to the monitor.

Step 7. Power on the computer and monitor and ensure that the device has network connectivity.

Step 8. If needed, set account settings such as language, time zone, display resolution, and network type.

Step 9. If required, use image management software or Remote Desktop Services to image the computer.

Step 10. Put the computer on the network domain.

Step 11. Ensure that the common applications work.

Step 12. Apply company-required settings or profile.

Thick Client Installation

Before installing a thick client, you need to ensure that the minimum hardware is available to run the applications that will be loaded. As with thin clients, medium to large companies tend to have a system image already configured, stored, and available somewhere on the network, and the same tools are used to get the image onto the computer as for a thin client. Smaller companies might have a technician load each application individually and then configure the account settings manually.

You can also use Remote Desktop Services, just as with a thin client, and push an image to the computer. In small companies, the applications are commonly installed by a technician one by one, or a standard image with the most common applications might be used. Then the technician would have to possibly configure the following settings:

- Network printer
- Local printer
- Application account settings
- Computer settings, such as wireless, display, and desktop icons

Wireless AP/Router Configuration

A wireless AP frequently has the capability to route. This type of device is made for a small office/home office (SOHO) environment. The screens used to configure a SOHO AP varies per vendor, but the process is common. Some of the specific configuration tasks have already been shown, such as DHCP configuration, but the generic steps for configuration follow:

Step 1. Connect an Ethernet cable between the wireless AP and another device that has a web browser.

Step 2. Open a web browser and in the address textbox, ent
dress of the AP, such as . **http://192.168.1.1**

Step 3. Enter the default username (if needed) and default

'ech Tip Change the default username/password

When an access point or wireless router is purchased, sometimes a default username and/or password is assigned. Because default passwords are available on the internet, the password needs to be changed immediately so that unauthorized access is not permitted. Manufacturers recognized this weakness, and as a result, many newer devices enable you to create a password during the initial setup.

Typical AP configuration menu options are shown in Table 13.21.

Table 13.21 Common AP configuration options

Option	Description
Wireless	Used to configure basic wireless settings, such as the SSID. Also includes a link to security options such as MAC filtering, authentication, and encryption (covered in Chapter 18).
Security	Used to enable/disable a firewall and configure firewall features such as a VPN or allow particular network ports to be opened to allow certain types of traffic through.
Storage	Allows monitoring and control of an attached storage device and can even support a File Transfer Protocol (FTP) server.
Maintenance	Allows viewing the current status of the various components as well as access to any logging that is enabled.
Administration	Allows configuration of the devi word, IP address assignment, an Could also include configuratio as VoIP or QoS.

Wireless SOHO access points/routers frequently include network functions such as a demilitarized zone (DMZ), also known as a screened subnet, QoS, a DHCP server (sometimes seen as the DHCP on/off setting), a router, integrated switch ports, and a port to add a hard drive and support network-accessible storage. Chapter 18 provides explanations and configuration details related to wireless security, and Table 13.22 introduces some common configuration features.

Table 13.22 Common wireless network device configuration settings

Option	Description
Basic QoS	Used to enable QoS so that traffic such as gaming traffic or VoIP traffic is prioritized over other data types.
IP filtering	Uses lists to control which users, websites, IP addresses, protocols, and apps can be used on a device. A deny setting blocks, whereas an allow setting specifically permits network traffic.
Content filtering	Blocks access to specific web pages. Might also include a date/time range. Also called URL or web filtering.
Channel ID	Used to specify a particular 2.4 GHz or 5 GHz channel.
Demilitarized zone (**DMZ**)	Allows a PC or server to be accessed from a remote location. Also called DMZ host or **screened subnet**.
DHCP	Used to enable or disable DHCP as well as the specific network number, mask, and range of addresses to use.

Option	Description
Firmware	Used to update the embedded code within a device. Frequently contains security, performance, and software updates.
Network address translation (NAT)/destination NAT (DNAT)	NAT, which is used to translate from private IP addresses to a public address, is enabled by default. DNAT maps a public IP address to a specific private IP address and is used in a home or small business network.
Port forwarding	Also called **port mapping** or port triggering, where specific port numbers, ranges of port numbers, and applications are allowed to be used instead of opening all ports. Port triggering allows data through on a limited basis when a specific/configured situation occurs.
SSID	Used to name a wireless network. An SSID cannot contain spaces. There is commonly an option to enable or disable SSID broadcasting.
Universal Plug and Play (**UPnP**)	Used as an alternative to port forwarding to allow peer-to-peer (P2P) gaming applications to function without further configuration. Could be a security risk for other devices on the network.

WWAN Cellular Configuration

Another type of wireless device that you might configure is a wireless broadband device or a WWAN (cellular) connection. A wireless broadband (WWAN cellular) device is normally a USB device, but this technology is integrated into some mobile devices. Software
either by using a disc or from the device. The device
phone number/account number associated with the

Figure 13.72 shows the type of information provided for a wireless broadband USB device.

Figure 13.72 WWAN cellular properties

IoT and Smart Devices

Internet of Things (**IoT**) is a term that describes the interconnectivity of sensors and devices that connect to a network (usually a wireless one). The IoT has affected all industries, and home devices are particularly common. Smart homes (see Figure 13.73) are becoming popular, and even older existing homes can be made smart.

Figure 13.73 Smart home controls

Smart homes include devices that can monitor water consumption, air and heat, and electricity. In addition, it is possible to control locks, lights, thermostats, garage doors, computers, sound systems, TVs, and refrigerators—and the list just keeps growing. Smart devices are controlled through an app on a phone, tablet, laptop, or other computer. The smart devices can connect to a wired Ethernet network, an 802.11-based wireless network, or using two other standards that are common in smart homes: Zigbee and Z-Wave.

Zigbee is a standard managed by the Zigbee Alliance. Zigbee devices do not have a maximum number of hops (that is, a maximum number of devices the signal can go through to reach the destination). A Zigbee network includes a Zigbee coordinator and Zigbee devic
might include a Zigbee router, also called a Zigbee ga
tends the range of the wireless network. Figure 13.74

topologies used with Zigbee: one without a Zigbee router and one with one.

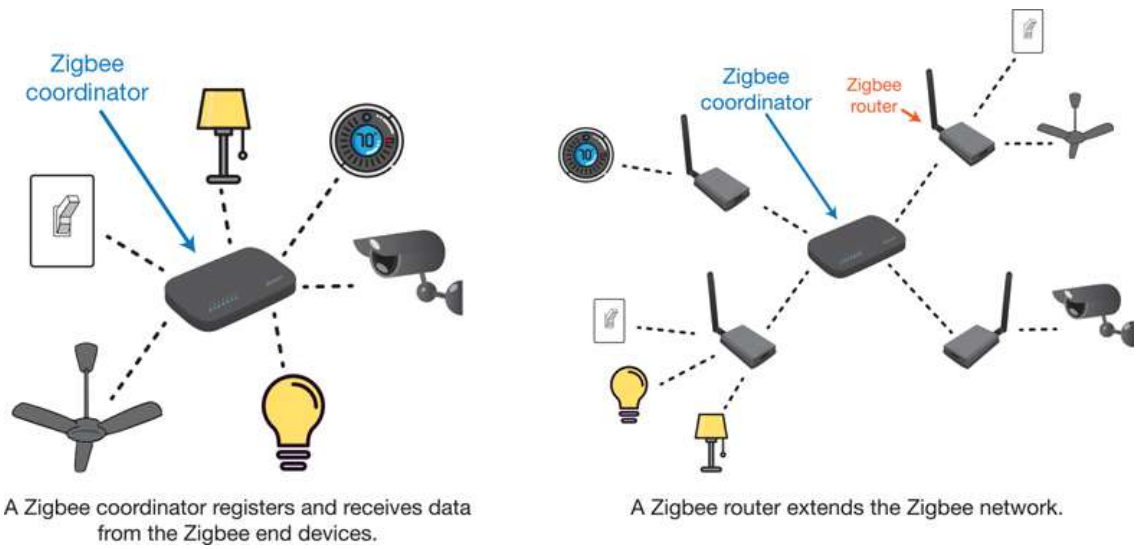


Figure 13.74 Zigbee topologies

Z-Wave is a wireless standard from Silicon Labs. Z-Wave supports only four hops between one particular device and the controller. If DeviceX has to go through Device1, Device2, and Device3 to get to the controller, all is good, but if DeviceX has to go through an additional device to get to the controller, DeviceX cannot be controlled.

Z-Wave has a limit of 232 devices in one network and is used to support thermostats, lights, locks, sensors, switches, and so on. Z-Wave, like Zigbee, requires a controller. The more devices you add to the network, the more repeaters you have because each device then boosts the signal as it transmits the data. Figure 13.75 shows a sample topology. Table 13.23 compares Zigbee and Z-Wave.

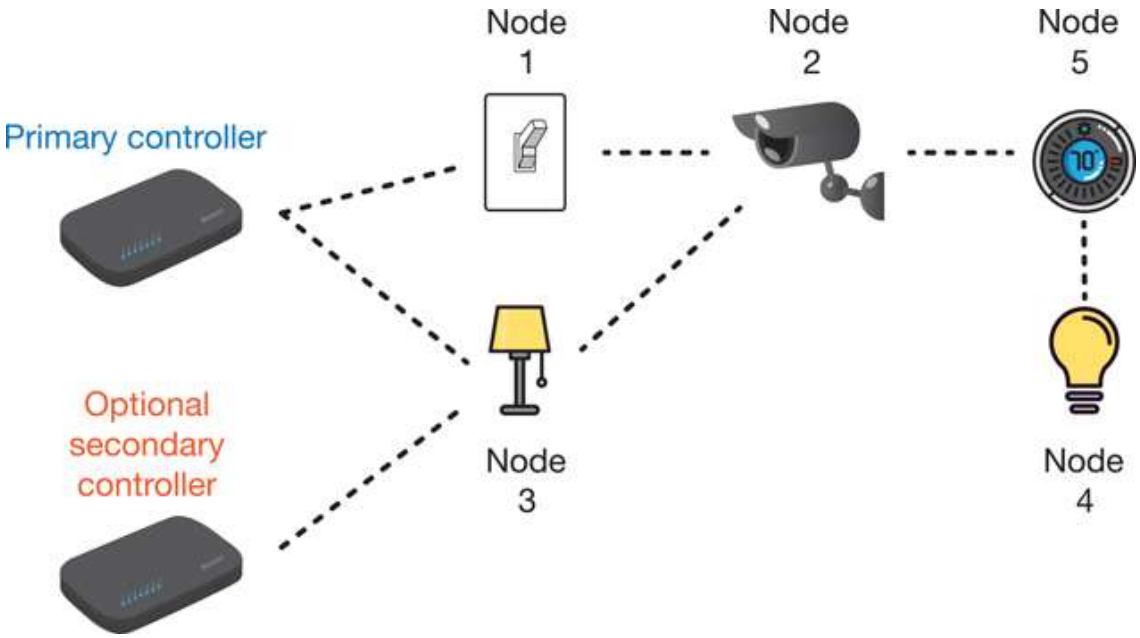


Figure 13.75 Z-Wave sample topology

Table 13.23 Common wireless network device configuration settings

Standard	Frequency	Data rate	Range	Security
Zigbee	915 MHz and 2.4 GHz	Up to 250 kbps	Up to 328 feet (100 meters)	128-bit AES encryption
Z-Wave	908.4, 908.42, and 916 MHz (United States, Canada, and Mexico)	Up to 250 kbps	Up to 328 feet (100 meters)	Proprietary and improved with Security2

Both Zigbee and Z-Wave involve mesh networks. In a mesh network, wireless signals go from device to device, and a central hub/coordinator that commonly connects to the internet. Each device can connect to multiple other devices.

IoT devices are very susceptible to security breaches because of the lack of standardization within the industry; in addition, IoT devices are incapable of supporting security due to lack of hardware. They also provide an easy target if they connect to other networks like 802.11 or Ethernet networks. Here are some security suggestions for implementing IoT devices:

- Research the company and protocol(s) used to connect the devices. Make a selection based on a good security track record.
- Encrypt the IoT data sent between the devices and the systems that receive the data.
- Require user authentication to access the IoT devices.
- Secure the IoT network. Industry security leaders offer IoT solutions.
- Ensure that any communication between an IoT device and an app uses proven security methods.

Network Troubleshooting

One step in troubleshooting a network is to determine how many devices are affected by a problem. For example, if only one computer cannot communicate across a network, the issue will be handled differently than if several (or all) computers on a network cannot communicate. If a computer cannot get on a network at all, it might not have appropriate IP addressing information or may not be joined to a domain. If a network port is suspect, ensure that the interface is enabled, try another cable, or use a loopback plug to test the port. The easiest way to determine how many devices are having trouble is by using a simple test using the command. `ping`

The Command ping

The command can be used to check connectivity fron
vice to another device (if you suspect **no connectivit**
nectivity, or **intermittent connectivity**/**limited con**

13.76 shows the sample network used here to illustrate how is used to check various network points. `ping` `ping`

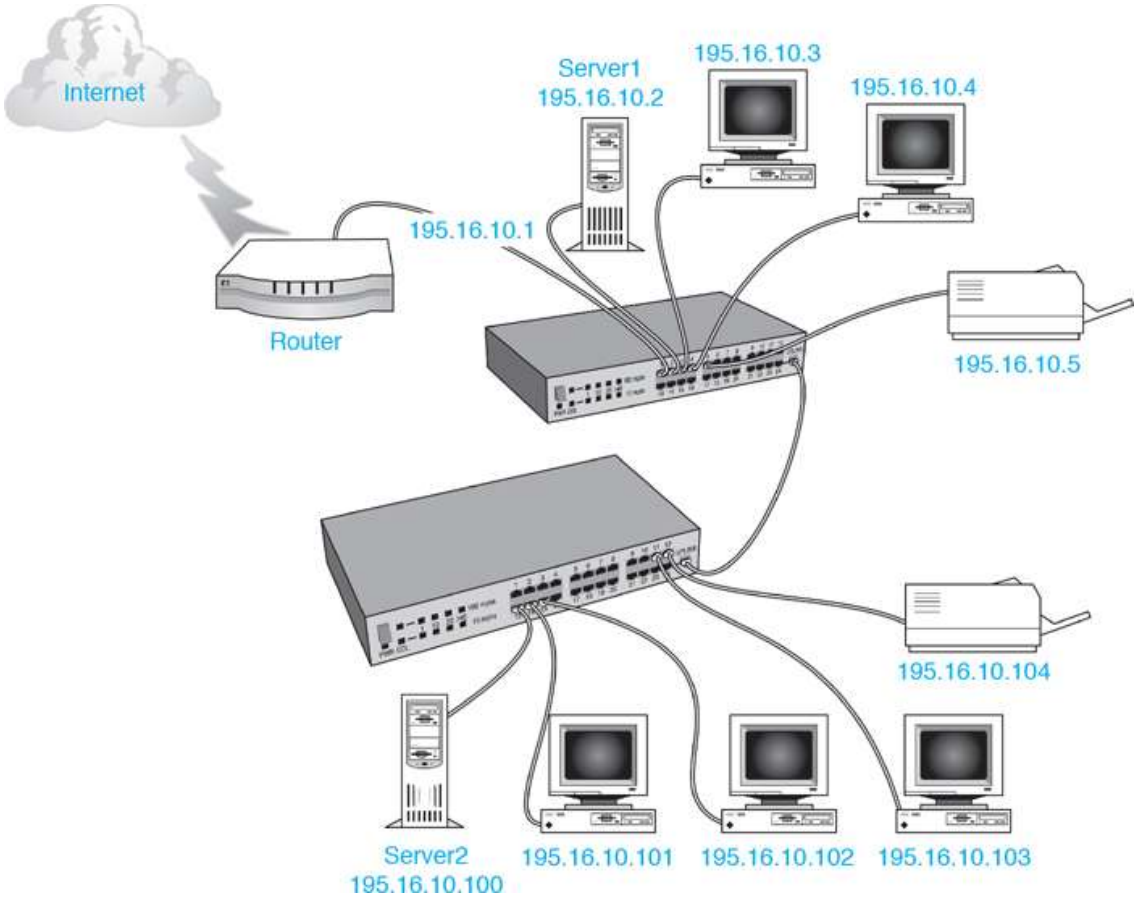


Figure 13.76 Sample network troubleshooting scenario

'ech Tip What does do? `ping`

The command can be used to determine whether a network path is available, whether there are delays along the path, and whether a remote network device is reachable. sends a packet to an IP destination (that you specify), and a reply is sent back from the destination device if everything works fine. `ping` `ping`

The network shown in Figure 13.76 consists of va
vices, including two servers and two laser printers. T
to one of two switches that are connected using the u

Ethernet cable or a fiber cable. A router connects to the top switch, and the router connects to the internet.

If the 195.16.10.3 workstation cannot access a file on Server2 (195.16.10.100), the first step in troubleshooting is to ping Server2 from the workstation. If this ping is successful, you know the problem is with Server2 or the file located on the server.

If the ping is unsuccessful, you know there is a problem somewhere between the workstation and the server or on the server. To test this, ping another device that connects to the same switch; for example, from workstation 195.16.10.3, ping Server1 (195.16.10.2). A successful ping tells you the connection between the 195.16.10.3 workstation and the switch is good, the switch is working, the cable connecting to Server1 is fine, and Server1 is functioning. If the connectivity is intermittent (that is, if you get one or two out of numerous pings), this could be a result of **port flapping** (that is, a port going up and then down) due to faulty cabling or a faulty port.

What Resources Are Unavailable?

One of the first signs of network issues is a user complaining about **unavailable resources**. This might mean the user can't reach the internet or can't reach local resources within the company, such as network shares, printers, or email. The troubleshooting process helps you narrow down where you should ping and verify exactly what network resource(s) cannot be reached.

Pinging devices on the same network is a good check of local connectivity. The term *local connectivity* describes devices on the same network, including the default gateway. If a network device can ping other devices on the same network as well as the default gateway, the network device (and all its components and basic settings) are configured correctly.

'ech Tip Use `ping -t`

Use (where you replace with an IP address or a URL) ous ping to a remote location. When you do, the ping you press Ctrl+C. `ping x.x.x.x -t x.x.x.x`

Now ping workstation 195.16.10.101 (a device other than the server on the remote switch) by typing . If the ping is successful, you know that (1) the uplink cable is operational; (2) the second switch is operational; (3) the cable that connects workstation 195.16.10.101 to the switch is good; and (4) the 195.16.10.101 workstation has been successfully configured for TCP/IP. If the ping is unsuccessful, you know that one of these five items is faulty. The problems could be the (1) Server2 cable, (2) switch port to which the server connects, (3) server NIC, (4) server configuration, or (5) file on Server2. **`ping 195.16.10.101`**

'ech Tip How can I check the TCP/IP protocol stack on my own NIC?

The command can be used to test a network card as well as the TCP/IP protocol running on the NIC, with the command (IPv4), (IPv6), or , where is a hostname that is translated to an IP address known as a private IP address, or loopback address, which means it cannot be used by the outside world. **`ping ping 127.0.0.1 ping ::1 ping localhost`** *`localhost`*

You can use the command followed by the name of the device (or website) being tested (for example,). A DNS server translates the name (pearsoned.com) to an IP address (23.197.24.193). If you can reach the site by pinging the IP address, but not the name, you know there is a problem with the DNS server. `ping` **`ping`** **www.pearson.com**

'ech Tip What the results mean **`ping localhost`**

If a ping is successful (that is, if you get a message indicating that a reply was received from 127.0.0.1 or ::1), you know the TCP/IP protocol stack works correctly on the NIC. If the ping response is nothing (or appears to hang) or a 100% packet loss error, you know that TCP/IP is not properly installed or is not functioning correctly on that partic

The Command `ipconfig`

To see the current IP configuration on a Windows computer, use the command from a Windows command prompt or the command with Linux or macOS. The command can be used to see both wired and wireless NICs if both are installed, as shown in Figure 13.77. The command also allows you to view MAC addresses. `ipconfig` ifconfig `ipconfig /all` `ipconfig /all`

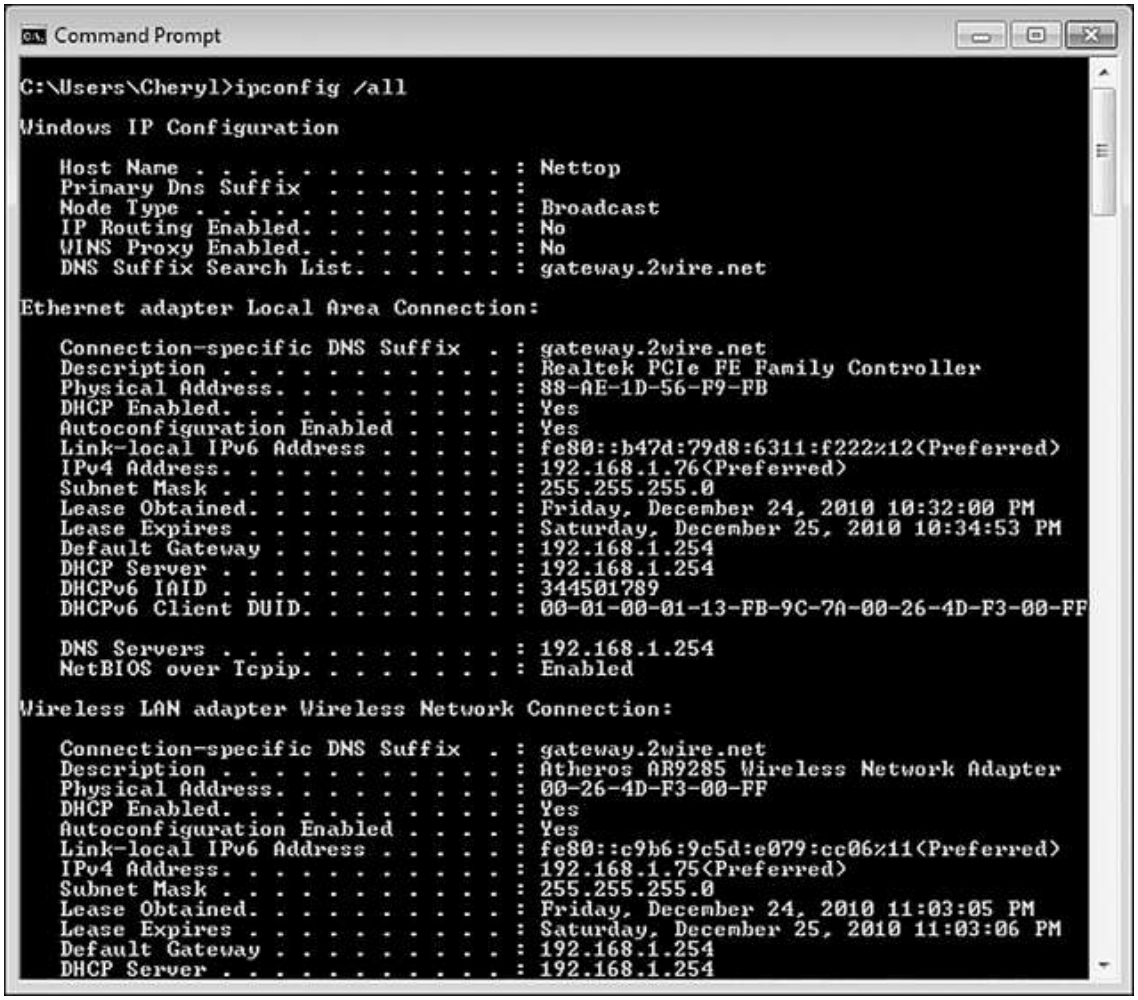


Figure 13.77 command output `ipconfig /all`

A network device may not get an IP address from the DHCP server. A symptom of this problem is a device getting an APIPA (IPv4) or link-local (IPv6) address because a DHCP server is unavailable. When this occurs, use the command and then issue the command. Also ensure that the device is actually configured for DHCP. A message appears on Windows-based devices when two devices have been manually assigned the same IP address. Note that not all operating systems and/or devices do this. Check any device that has a manually configured IP address to locate duplicate IP addresses that are causing an IP address conflict. `/release` `ipconfig /renew`

The and Commands tracert pathping

The command is a tool found in the Microsoft, macOS, and Linux environments. The command is used to display the path a packet takes through the network. The benefit of using the command is that you can see where a fault is occurring. It also allows you to see the network latency. Network latency is the delay measured from source to destination; **high latency** can mean slow network speeds. The command is also useful when you have intermittent connectivity. An example of output from the command is provided in Figure 13.78. `tracert tracert tracert tracert tracert`

```
C:\Users\Cheryl>tracert comptia.org
Tracing route to comptia.org [198.134.5.6] over a maximum of 30 hops:
 1 <1 ms <1 ms <1 ms vankman1 [192.168.1.1]
 2 8 ms 7 ms 8 ms 10.126.208.1
 3 10 ms 8 ms 7 ms 72-31-92-20.net.bhntampa.com [72.31.92.20]
 4 11 ms 14 ms 12 ms ten0-6-0-11.tamp27-car1.bhn.net [71.44.3.186]
 5 17 ms 16 ms 19 ms hun0-4-0-3.tamp20-car1.bhn.net [72.31.117.170]
 6 22 ms 19 ms 18 ms ten0-8-0-0.orld71-CAR1.bhn.net [71.44.1.211]
 7 17 ms 16 ms 19 ms 72-31-217-88.net.bhntampa.com [72.31.217.88]
 8 23 ms 19 ms 14 ms 10.bu-ether15.orldfljo00w-bcr00.tbone.rr.com
[66.109.6.98]
 9 36 ms 31 ms 31 ms bu-ether18.atlngamq47w-bcr01.tbone.rr.com [66.109.1.72]
 10 23 ms 23 ms 24 ms 0.ae2.pr1.atl20.tbone.rr.com [107.14.17.188]
 11 26 ms 29 ms 23 ms 67.106.215.89.ptr.us.xo.net [67.106.215.89]
 12 50 ms 51 ms 50 ms 207.88.13.54.ptr.us.xo.net [207.88.13.54]
 13 52 ms 56 ms 49 ms 207.88.12.174.ptr.us.xo.net [207.88.12.174]
 14 50 ms 51 ms 51 ms 207.88.12.31.ptr.us.xo.net [207.88.12.31]
 15 49 ms 57 ms 55 ms ae0d0.mcr1.chicago-il.us.xo.net [216.156.0.162]
 16 54 ms 52 ms 53 ms 216.55.11.62
 17 52 ms 60 ms 52 ms 198.134.5.6
Trace complete.
```

Figure 13.78 Sample output of `tracert`

A similar command available in the Windows environment is , which is a combination of the and commands. Whereas the command checks for connectivity between one network device and another device and displays the IP addresses of the routers between the source and destination addresses, provides additional information, including the network latency and loss between the source and destination. takes longer to execute than the or commands. Sample output is provided in Figure 13.79. `pathping ping tracert ping tracert pathpi`

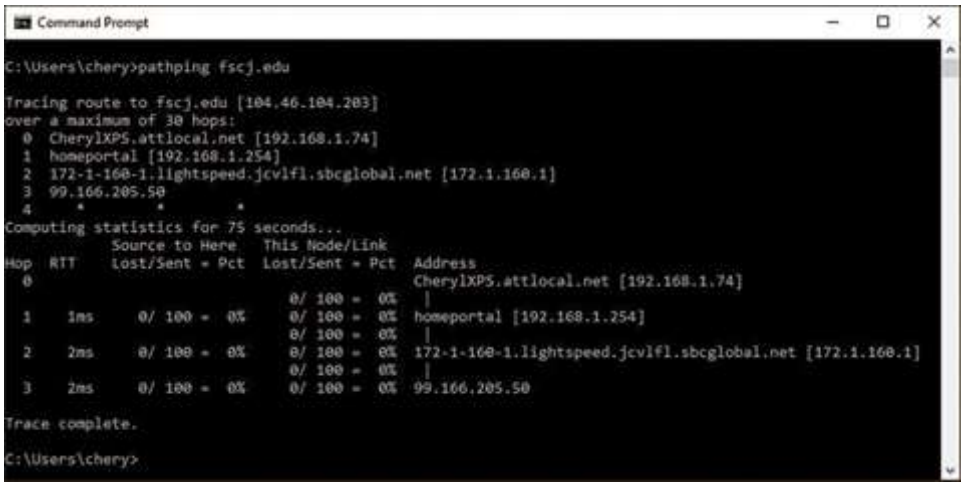


Figure 13.79 Sample output of `pathping`

High latency in wireless networks is caused by interference from devices operating in the same frequency range, obstacles such as walls and concrete, and distance from the access point. High latency in wired networks is typically caused by poor or faulty cabling and/or security issues.

The Command nslookup

The command is a tool that helps with DNS server troubleshooting. enables you to see domain names and their associated IP addresses. When an internet site (server) cannot be contacted by its name but can be contacted using its IP address, there is a DNS problem. The command can make troubleshooting these types of problems easier. To see this tool in action, bring up a command prompt, type , and press ↵Enter. The IP address of the Pearson web server appears. Note that if the command shows a domain name such as a computer, but the domain name cannot be used to contact the device, the command can be used to clear the DNS cache. `nslookup nslookup nslookup nslookup pearson.com nslookup ipconfig /flushdns`

The Command net

The command is used to manage just about everything on a network from a command prompt. The command is followed by other options, and each option has different parameters. Here is the con
syntax: `net net`

Click here to view code image

```
net [ accounts | computer | config | continue | file | group
| help | helpmsg | localgroup | name | pause | print | send |
session | share | start | statistics | stop | time | use |user |
view ]
```

Table 13.24 lists some of the most commonly used command options. `net`

Table 13.24 command options and descriptions `net`

Command	Description
`net help`	Used to get help for the commands. You can also use followed by the command () or or . `net net help net help computer net computer /help net computer /?`
`net computer`	Used to add or remove a computer in a Microsoft domain.
`net config`	Used to display information about a server or workstation service.
`net share`	Used to create, remove, or view network share resources.
`net start`	Used to start a network service.
`net stop`	Used to stop a network service.
net use	Used to map a drive letter to a network resource.
net user	Used to manage user accounts.
`net view`	Used to view network devices.

The Command `netdom`

The command, which is similar to , is used to manage workstations in a domain environment. Use the command to see all the options. Table 13.25 shows some of the most popular command options. `netdom net netdom /? netdom`

Table 13.25 command options and descriptions `netdom`

Command	Description
`netdom add`	Used to add a workstation account to a domain
`netdom join`	Used to join a workstation to a domain
`netdom remove`	Used to remove a workstation from a domain
`netdom renamecomputer`	Used to rename a computer and its domain account
`netdom reset`	Used to reset the connection between a workstation and a network domain controller
`netdom resetpwd`	Used to reset the computer account password
`netdom verify`	Used to verify the connection between a workstation and a Microsoft domain controller

NIC Troubleshooting

The following methods can help with NIC troubleshooting:

- In a command prompt window, use to test the NIC
- Ping another device on the same network. If the p
  know the NICs, device, cable, switch or hub are al
- Ping the default gateway. If the ping is successful,
  ity and configuration of the device for communica

work work, and the device has the potential to communicate with other networks.

- Ping a device on a remote network. If the ping is successful, you know the Layer 3 device serving as the default gateway is working.
- Use the command to determine the location of the fault (such as whether the problem is inside or outside the company). `tracert`
- Check the status light(s) on the NIC (see Figure 13.80) to see if the physical connection is good. Different NICs have lights of different colors, but the two most common colors used with status lights to indicate a good connection are green and orange. Some status lights indicate the speed at which the NIC is operating (10 Mbps, 100 Mbps, or 1 Gbps).

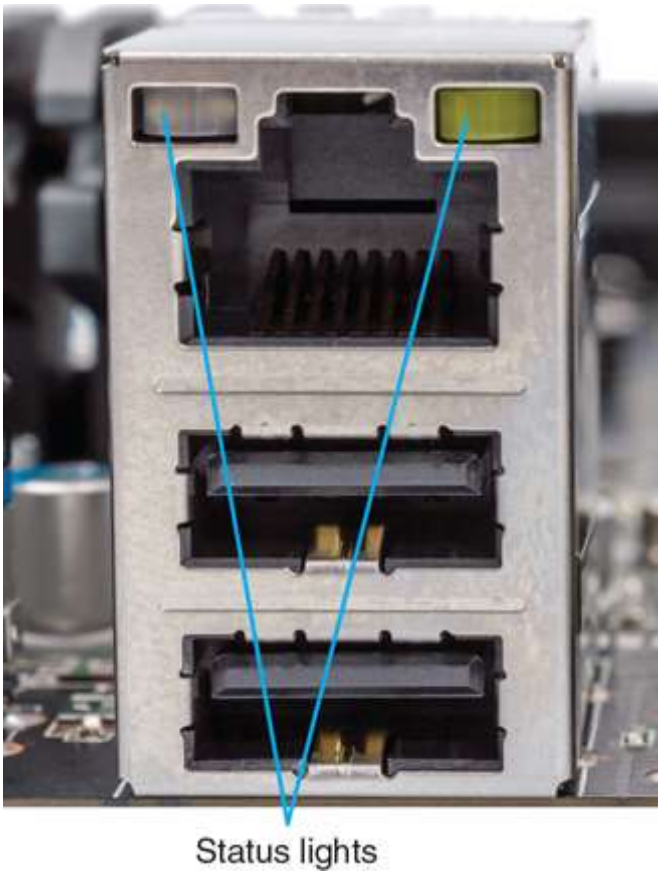


Figure 13.80 NIC status lights

- Check the status light on the hub or switch (see Figure 13.81) that is used to connect the workstation NIC to the network. Green is a common color for a good connection on these devices.
- Check cabling. Even if the status lights indicate that the connection is good, the cabling may still be faulty.
- Update the device driver by obtaining a newer on manufacturer's website.
- Check the IP addressing used. Use the command f sure that the NIC has an IP address assigned. If you get a duplicate IP

address error message, change the IP addressing to DHCP or another statically assigned address (that has not already been used). `ipconfig`

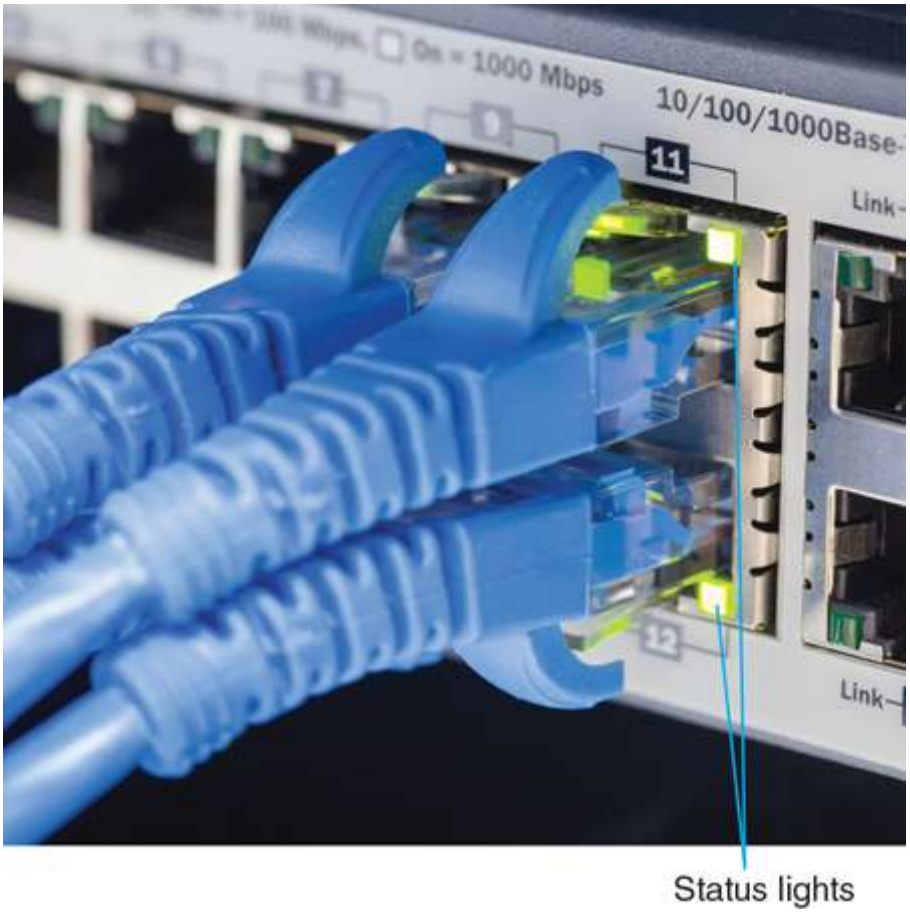


Figure 13.81 Switch or hub status lights

- On a mobile device, ensure that wireless is enabled and that the wireless NIC is enabled. Look for a button or a keystroke combination that re-enables the wireless antenna and ensure that the NIC is not disabled in the *Network and Sharing Center* Control Panel.
- If your network connection on the desktop or from within the *Network and Sharing* section of the Control Panel shows limited connectivity (see Figure 13.82) or if you cannot reach the internet at all, try rebooting the PC (because of a 169.254.*x.x* address) or the router (if in a home or small business network). With a wireless connection, check security settings, the wireless button that controls the wireless antenna, or a wireless key that toggles the wireless NIC. If on a wired network, the cable could be an issue.
- If the network connection is intermittent or slow
tion, move closer to the AP, change the position of
or add another AP in the area to extend the wirele
wired connection, check cabling and duplex settin
with a switch.

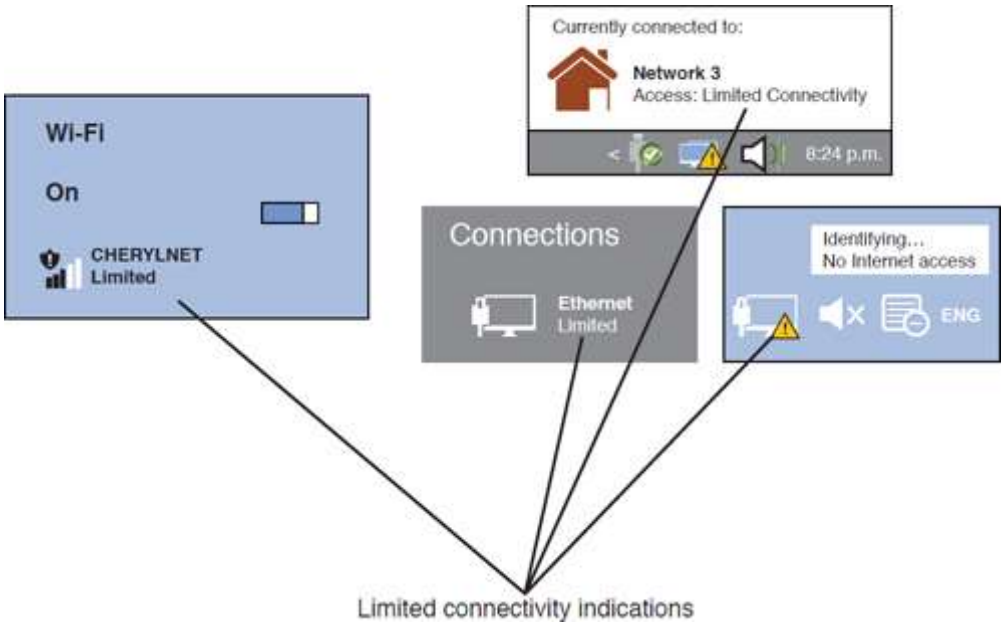


Figure 13.82 Windows limited connectivity network indications

Troubleshooting Cable and DSL Modems

Because most cable and DSL modems are external, the best tools for troubleshooting connectivity problems are the lights on the front of the modem (see Figure 13.83). The lights vary from vendor to vendor, but common ones are listed in Table 13.26.

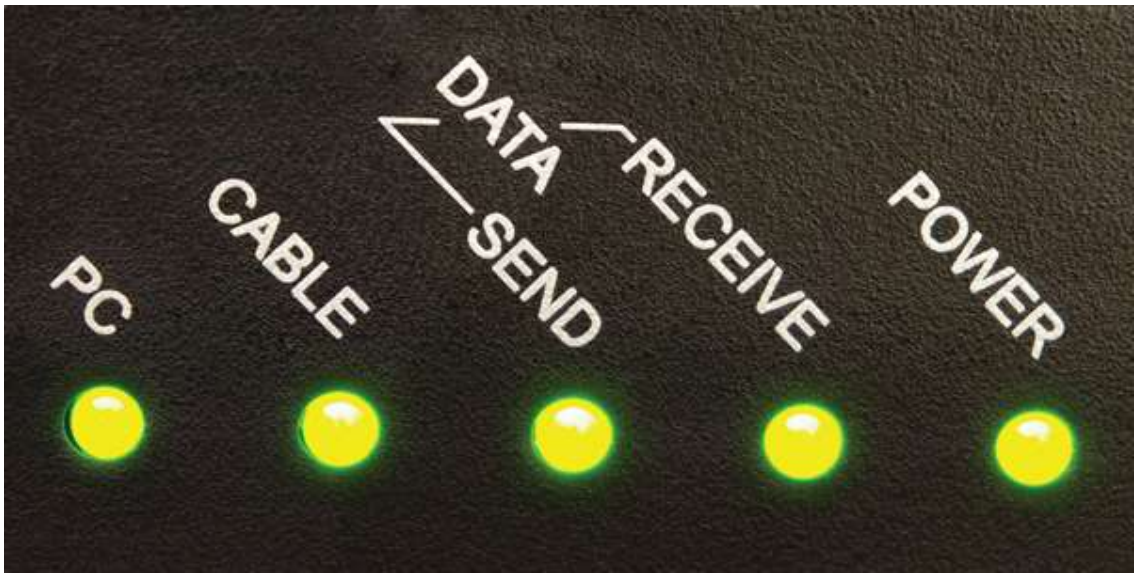


Figure 13.83 Cable/DSL modem lights for troubleshooting

Table 13.26 Cable/DSL modem lights and troubleshooting*

Light	Explanation

Light	Explanation
Cable, Data, or D/S	Usually blinks to indicate connectivity with internet provider
ENET, E, or Ethernet	Usually indicates connectivity between the PC and the modem; if unlit, ensure that you are using Ethernet (though if using USB, this will be unlit), check cabling, and check PC network card settings
Internet, Ready, or Rdy	Stays lit when the modem has established an internet connection
Link Status	Usually flashes when acquiring a connection with a provider and is steadily on when a link is established
PC	Used instead of Ethernet or USB lights to show the status of the connection between the modem and the PC
Power	Indicates power to the modem
USB or U	Usually indicates connectivity between the PC and the modem; if unlit, ensure that you are using USB (though if using a NIC, this light will be unlit), check cabling, and check *Device Manager* to see if the modem is recognized

* Refer to the modem documentation for the exact status of the lights.

After you have checked lights and possibly checked cables, if you still have a problem, power off the modem, wait two minutes, power the modem back on, and reboot the computer. Give the modem a couple minutes to initialize. Most modems have a reset button that ca
powering off and powering back on works without h
configuration information. If a modem is still not wo
these steps, contact the service provider.

Networking Multifunction Devices

Chapter 9, "Printers and Multifunction Devices," outlines how to share a printer or multifunction devices across a network as well as how to access a wired or wireless network printer. Now that you know a bit more about networking, the processes outlined in Chapter 9 might be easier to understand. **Printer sharing** is commonly done in a home or small business environment. In a corporate environment, a print server is used, and printers are published or visible to users and devices on the network. A network printer will definitely have an IP address assigned. Users can perform network printer mapping, which enables network users to add a printer to their computer by using the domain printer name or printer IP address. To find printers by name in a corporate network domain, do the following:

- *Windows 7:* Use *Windows Explorer* to explore the network for printers.
- *Windows 8/10/11:* Use *File Explorer* to explore the network for printers.

You can also use a Control Panel or Windows Settings link to add a network printer:

- Access the *Add a device* Control Panel link > select *The printer that I want isn't listed* > enable the *Select a shared printer by name* radio button and enter the domain name (an example might be the domain name SchmidtCo, in this format: \\SchmidtCo\) and select from the printers that are listed.
- Add the printer by using the printer's IP address. A network printer commonly has a front panel that is used to access network configuration settings. A printer that connects directly to the network through a wired or wireless connection has a statically configured IP address, mask, and default gateway. Many times technical support staff attach a label to the printer that shows the IP address. You could access the network settings from the *Devices and Printers* > *Printers* section of the Control Panel to view the assigned IP address. Refer to Chapter 9 for how to connect using a printer's IP address.
- Use the *Printers & scanners* Settings link > *Add a p* *Add device* box. If you don't see the printer listed, *printer by name* and enter the network share nam

Network Printer/Scanner Services Configuration

Networked printers, copiers, scanners, and multifunction devices might include network services that provide the ability to copy/scan a document and email it to someone or to put a copied/scanned document in a network folder. Typically when configuring a device to be able to email a document, you must provide the following information:

- IP address of the email server (which might be listed as the Simple Mail Transfer Protocol [SMTP] gateway)
- The port number used for the server, obtained from the network administrator who manages the email server
- The email account created by the administrator for the printer
- On some devices, define a standard subject line for any documents emailed from the device

Devices might also be able to store a copied or stored document in a network folder. Make sure you know the network path to the shared folder and ensure that the folder permissions are set to allow new files to be placed into the folder. (Directions on how to share a folder are given later in this chapter.) An example of a network path is \\CherylXPS\ScannedDocs, where the first part is the network device name and the second part is the name of the shared folder. Configuration on the network device used to scan/copy the document typically requires the following:

- A name that appears in the device's address book. This name should be descriptive so that anyone wanting to store a document in the network folder will recognize it. An example is Shared Scanned Documents.
- The protocol used by the device to send the document to the folder. The most common one used is Server Message Block (**SMB**), though you might also see Common Internet File System (**CIFS**).
- The IP address of the SMB server or the device that holds the shared folder.
- The network path to the shared folder.
- The username/password used to put files in the sh
  may have to be obtained from the network admin
  server.

Network Printer/Scanner Troubleshooting

To begin troubleshooting a network printer, do all the things that are normally done when troubleshooting a local printer (refer to Chapter 9) and check the obvious things first. Does the printer have power? Is the printer online? Does the printer have paper? Are the printer's connectors secured tightly? Is the correct printer driver loaded? If all these normal troubleshooting steps check out correctly, try the following steps:

- Print a test page and see if the printer's IP address outputs or see if the printer is labeled with its IP address. If so, ping the printer's IP address to see if there is network connectivity between the computer and the printer. Use the command to see if there is a complete network path to the printer. `tracert`
- Check the printer's *Properties* page to see if the printer has been paused.
- Cancel any print jobs that are in the print queue and resubmit the print job.
- Reset the printer by powering it off and back on. If it connects to a print server device, reset that, too.
- Be sure the print job has been sent to the correct printer. Companies commonly have several network printers to use.
- If a network printer fails and a user has a USB-attached printer, share the USB printer. (Chapter 9 shows how to share a printer across a network.)
- If the printer has never worked, try a different version of the print driver.

Network Servers

Servers are an important part of networking and provide different functionality. One server could provide more than one function. For example, a corporate server might act as a web server as well as a DHCP server. Figure 13.84 shows several network servers mounted in a rack. Each physical box could contain several virtualized server

Figure 13.84 Network servers

Table 13.27 summarizes the most common servers on a network.

Table 13.27 Server types and descriptions

Server type	Description
Authentication server	Used to verify credentials (usually username and password), such as when someone logs in to a domain workstation. Sometimes called an authentication, authorization, and accounting server (**AAA server**).
DHCP server	Used to issue IP-related information, including IP address, subnet mask, default gateway, DNS server, and domain name. Commonly has a block of addresses that are in a pool to be assigned to common devices such as PCs and IP phones. A few addresses are reserved for statically assigned devices such as routers, switches, APs, and print
DNS server	Used to translate domain names

Server type	Description
Endpoint management server	Used as a centralized solution for discovering devices, distributing software, provisioning, updating, configuring, managing security, managing profile, imaging/re-imaging computers, and managing inventory.
File server	Used to store files that can be accessed and managed from a remote location. Sometimes called a **fileshare server**.
Mail server	Used to maintain a database of email accounts, store (email) messages sent and received, communicate with other mail servers, and use the DNS protocol to locate other servers. Also known as an email server.
Print server	Used to manage one or more network printers. See Chapter 9 for more information.
Proxy server	Used as a go-between between an application such as a web browser and a physical server. Details on how to configure a network device for a proxy server are provided in Chapter 18.
Syslog server	Used to receive information from multiple network devices and used as a historical record of events such as devices losing power, a particular interface going down, and logins or logouts on a particular device. Also called a logging server.
Web server	Used to provide web-based content that is accessed through a web browser that com the information through TCP po 443.

Embedded, SCADA, and Legacy Systems

An **embedded system** is a computer that has a specific function within a larger system. Embedded systems have many of the same components as desktop or mobile computers: processor, RAM, flash memory, and ports. Embedded systems can be found in many places, including airports, manufacturing plants, medical equipment, electrical systems, mechanical systems, and telecommunication systems. Embedded systems tend to be self-contained, but they commonly attach to a wired or wireless network and may be part of an IT person's responsibility.

Closely related to an embedded system is a supervisory control and data acquisition (SCADA) system that is used in just about every industry you can think of, including power, water, manufacturing, oil/gas, mass transit, and food/beverage production. **SCADA** uses a wide variety of networks, servers, and software to handle industrial processes, provide 24/7 monitoring, and supply data in real time (see Figure 13.85). Frequently a SCADA system automates tasks in an attempt to eliminate human error, increase productivity, reduce risks, and improve management by providing real-time data and alerts. One concern about these types of systems is the security risk because of the complexity of hardware, software, protocols, and systems used.

Figure 13.85 SCADA example

A **legacy system** is an outdated computer system equipment that in an ideal world would be replaced something new but is commonly kept because it mig

replace it, it is used with a particular system that can't be replaced, or it provides a functionality that will not be needed much longer. A legacy system might contain ports that require converters to be attached to the newer equipment, outdated methods used for access, or proprietary cables that might not be easy to obtain or find. Legacy systems are challenging for technicians because of the lack of support and documentation, but they may still be part of the job requirements.

Software-Defined Networking

Traditional networking involves hardware and software to move information from one place to another. Software-defined networking (SDN) is like ramped-up virtualization. With SDN, network hardware can be virtualized and centrally controlled. Advantages of SDN include the following:

- Provides centralized management and control
- Makes applying security policies across the entire network easier
- Makes it possible to expand and contract the network by quickly and effortlessly adding or removing devices as needed
- Enables fine-tuning of the network for a specific application, time, or purpose

Two basic concepts associated with SDN are the control plane and data plane. The **control plane** is the part of SDN that is involved with getting the data ready to move, whether that means building a routing table for the routing function or a MAC address table for a switch. The **data plane** is where all the work is done to move or forward traffic from the source to the destination, such as sending the data out a specific router or switch port. By splitting up these areas, it is easy to virtualize network equipment.

Let's look at switches as an example. You may remember that switches build a MAC address table, and the network is therefore able to efficiently send data based on the destination MAC address out a specific port. The process of learning the MAC addresses, storing them, port to send the data to could be handled by the cont the transmission of data could be handled by the dat SDN switches to be used (see Figure 13.86).

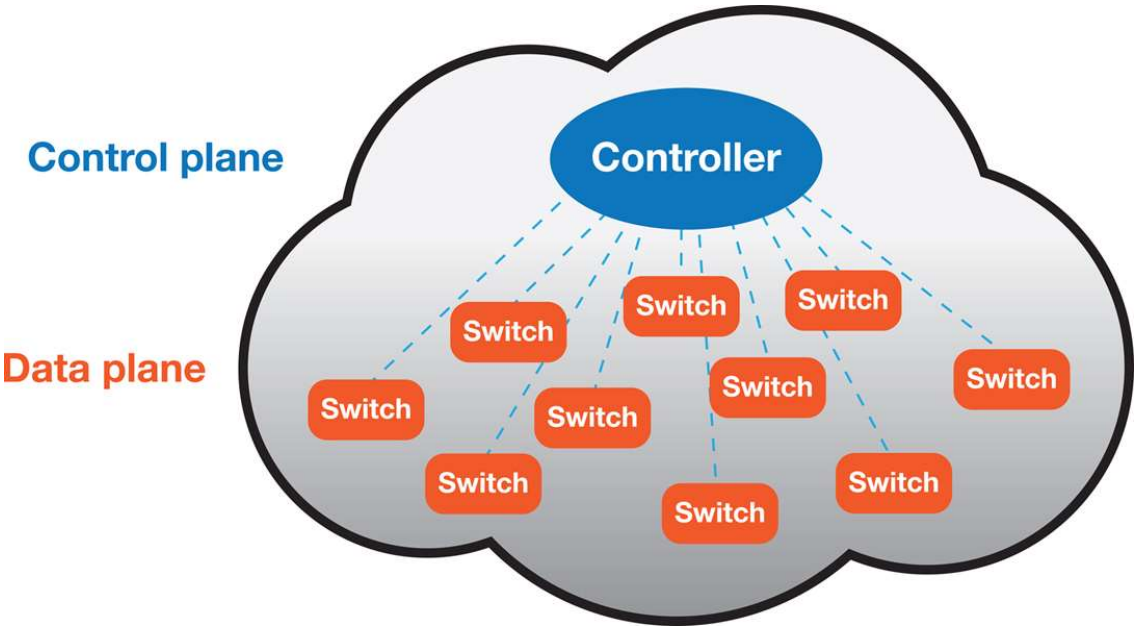


Figure 13.86 SDN network switching example

SDN started in the data center but has moved into other areas, including WANs and cloud connections, and it affects every part of network functionality today.

Network Terminology

In the networking field, you must be familiar with a great many acronyms and terms. Table 13.28 shows a few of the most common terms.

Table 13.28 Common network terms

Term	Description
Address Resolution Protocol (ARP)	A protocol used to discover MAC addresses. To send a message, a computer needs four key addresses: source IP, source MAC, destination IP, and destination MAC addresses. The computer sending the message knows its own source IP and MAC addresses. When the computer does not know the destination MAC address (but knows the destination IP address), ARP is used to [illegible] nation MAC address.

Term	Description
Bandwidth	The width of a communications channel, which defines its capacity for data. Examples include up to 56 kbps for analog modems and up to 100 Gbps for an Ethernet network.
Broadband	Cable bandwidth that is divided into multiple channels, on which simultaneous voice, video, and data can be sent.
Internet Control Message Protocol (ICMP)	A Layer 3 protocol used when troubleshooting or evaluating networks. The , , and commands use ICMP. `ping` `pathping` `tracert`
Network address translation/port address translation (NAT/PAT)	A method of conserving IP addresses. NAT uses private IP addresses that are translated to public IP addresses. PAT does the same thing, except it uses fewer public IP addresses by “overloading” one or more public IP addresses and tracking port numbers.
Secure Sockets Layer (SSL)	A protocol used to transmit internet messages securely. This protocol is used with HTTPS and online shopping websites to secure credit card information. Transport Layer Security (TLS) is the successor of SSL, which is now considered deprecated.
Transmission Control Protocol (TCP)	A connection-oriented protocol that ensures reliable communication between two devices. TCP and UDP are the two most common transport layer protocols. TCP is used whe needs to be made, and if the dat the data is re-sent. Website con file transfer protocols use TCP.

Term	Description
User Datagram Protocol (**UDP**)	A Layer 4 connectionless protocol that applications use to communicate with a remote device. TCP and UDP are the two most common transport layer protocols. UDP is used when a connection is not very important, when low overhead is needed (that is, when the UDP header is a lot smaller than a TCP header), or when speed is of the essence. VoIP and DHCP use UDP.

The TCP/IP Model in Action

To see the TCP/IP model in action, imagine opening a web browser with two separate windows: and . Two separate packages of data would be formed. For example, because HTTPS data is sent, HTTPS specifies how the data is to be formatted at the application layer. So, web page 1 gets HTTPS data at the application layer and moves down to the transport layer (inside the computer). At the transport layer, TCP is used for HTTPS traffic, and TCP adds a source port number 51116 and a destination port number 443 as part of building the transport layer header. All this HTTPS and TCP information moves down to the internet layer, where IP adds source and destination IP addresses. Because Pearson Education's web server has the IP address 23.197.24.193, that is the destination IP address. The packet continues moving down the model to the network access layer, and because the LAN is an Ethernet LAN, a source MAC address and destination MAC address are added. The data and all the headers are placed onto the Ethernet cable and sent on their way. The same thing happens with the second web page, except that at the transport layer, TCP adds port number 51117 and destination port number 443. https://www.pearsoned.com https://www.google.com

'ech Tip Use to view current connections netstat

To see current connections and associated port numb
mand prompt and type . `netstat`

When the Pearson Education web server delivers the web page to the computer, the data is, of course, from the web server, but the TCP port numbers are reversed. The web server places port number 443 as the source port number and port number 51116 as the destination port number. The source and destination IP addresses and MAC addresses are reversed as well. When the original computer gets the message, it knows which browser window generated port number 51116, and it places the Pearson Education information from the web server into the correct browser window. The same is true when the Google request comes back from the Google web server. TCP/IP-based protocols are required to send and receive data through the internet. Table 13.29 describes some of the most popular protocols and lists the TCP/IP port numbers that are commonly used for the various protocols. Table 13.30 lists some of the common protocols or network standards and the TCP/IP model layers at which they operate.

Table 13.29 TCP/IP protocols and port numbers

Protocol	Common port number(s)	Description
Dynamic Host Configuration Protocol (DHCP)	67/68	Issues IP addressing information, such as IP address, subnet mask, default gateway, and DNS server address to network devices.
Domain Name System (DNS)	53	Translates internet names and URLs into IP addresses.
File Transfer Protocol (FTP)	20/21	Sends/receives files from one computer to another network device; actually requires two port numbers: one to issue commands and the other one for sometimes but n data. FTP sends c and is not consid

Protocol	Common port number(s)	Description
Hypertext Transfer Protocol (**HTTP**)	80	Provides browser-based internet communication. Not considered secure.
HTTP over SSL/TLS (Secure Sockets Layer/Transport Layer Security) Protocol (**HTTPS**)	443	Provides encrypted HTTP communication through an SSL/TLS session.
Internet Message Access Protocol (**IMAP**)	143	Supports email retrieval. Allows synchronization from multiple devices. The latest version is IMAP4.
Lightweight Directory Access Protocol (**LDAP**)	389	Provides records related to directory services (any type of network resource, such as users, printers, phone numbers, files, access points, and so on).
NetBIOS over TCP/IP (**NetBT**)	137–139	Supports outdated applications that rely on the NetBIOS API to use a TCP/IP-based network. Also known as NBT.
Network Time Protocol (NTP)	123	Synchronizes time between network devices.
Post Office Protocol version 3 (**POP3**)	110	Supports email r email on a single (Contrast with IM

Protocol	Common port number(s)	Description
Remote Desktop Protocol (RDP)	3389	Connects one Windows computer to a remote Windows computer.
Secure File Transfer Protocol (SFTP)	22	Supports file transfer using the SSH protocol suite.
Secure Shell (SSH)	22	Supports secure connectivity to a remote device and allows secure file transfer.
Server Message Block (SMB)/Common Internet File System (CIFS)	445	Provides access to shared network devices, files, and printers, especially in a mixed environment, such as a network consisting of Mac and Windows computers. CIFS is a version of SMB. SMB/CIFS can use TCP port 445, but when used with the NetBIOS API, UDP ports 137 and 138 as well as TCP ports 137 and 139 are used. (See NBT.)
Service Location Protocol (SLP)	427	Announces and discovers services in a LAN.
Simple Mail Transfer Protocol (SMTP)	25	Transmits email and is commonly used with MIME (Multipurpose Internet Mail Extensions) to include non-ASCII charac rich media conte

Protocol	Common port number(s)	Description
Simple Network Management Protocol (SNMP)	161/162	Used to monitor, communicate with, and manage network devices.
Telnet	23	Supports connecting to a remote network device; is not secure.

Table 13.30 TCP/IP layers and associated protocols/standards

Layer	Protocols
Application	HTTP, HTTPS, Telnet, SSH, FTP, SFTP, DNS
Transport	TCP, UDP
Internet (internetwork)	IP, DHCP, ICMP
Network access	ARP, 802.3 (Ethernet), 802.11a, b, g, n, ac, and ax (wireless)

Networking protocols can seem a bit overwhelming at times, but remember that each one is just a set of rules for a specific purpose.

One more aspect of protocols that you need to understand is how TCP and UDP differ. What they have in common is that they both operate at the transport layer of the TCP/IP model, and they both work on port numbers. What is different is that TCP has a bigger heade
tures that let it do a lot more things, like make sure th
nection is available and stay in constant contact with
ing the data transfer. This is called being **connection**
the TCP/IP protocols are connection-oriented, includi

SSH. Another feature of TCP is that if any data is lost along the way, it is re-sent.

In contrast, UDP is considered to be a **connectionless** protocol. I think of this as throwing a baseball (the data) and just hoping it gets to the destination. There are no "do overs," and data is not re-sent. UDP transfers are faster than TCP transfers. Some application layer protocols that use UDP are DHCP and TFTP. The voice data in VoIP calls is sent using UDP because VoIP cannot tolerate delay. DNS servers can actually use both TCP and UDP.

More Windows Network Settings

When you first configure a computer, you have to specify whether the computer is on a private network, such as your home or corporate network, or on a public network. This can be changed using the Windows *Network & Internet* Settings link, as shown in Figure 13.87. Once you select the *Properties* button from whatever type of network connection you are using, you can select whether the computer has a public or private network profile, as shown in Figure 13.88.

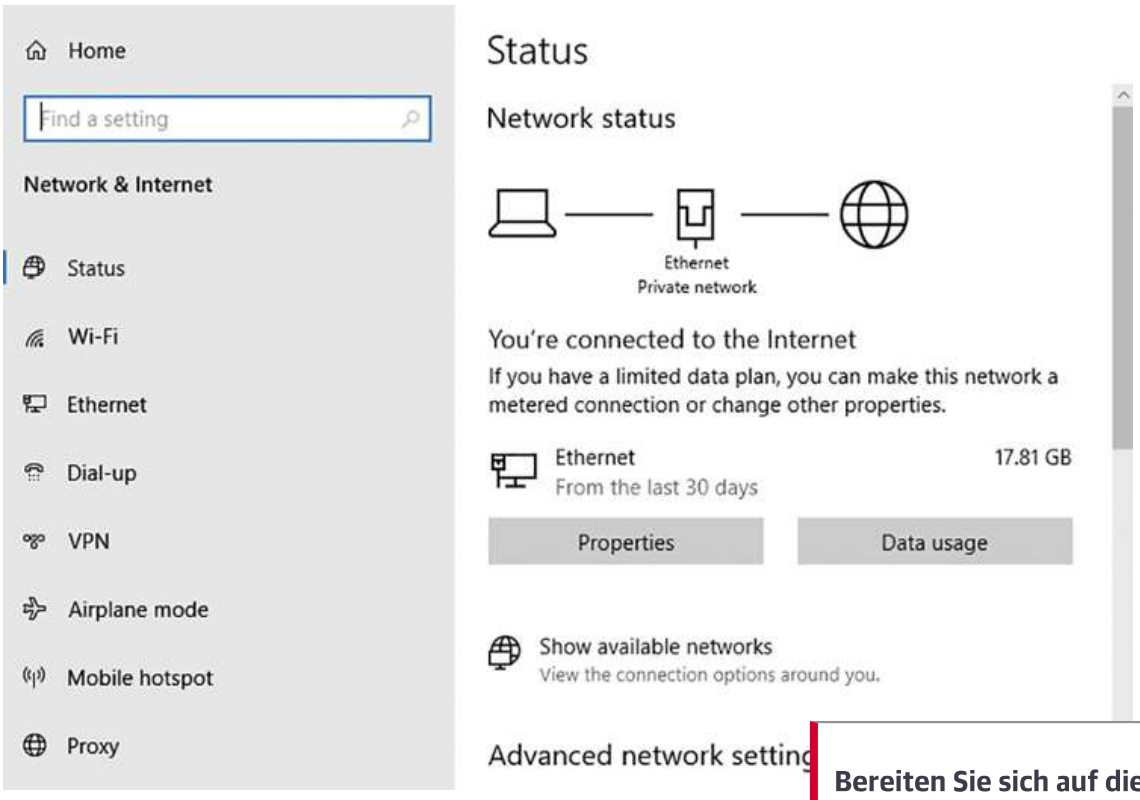


Figure 13.87 Windows Network & Internet options

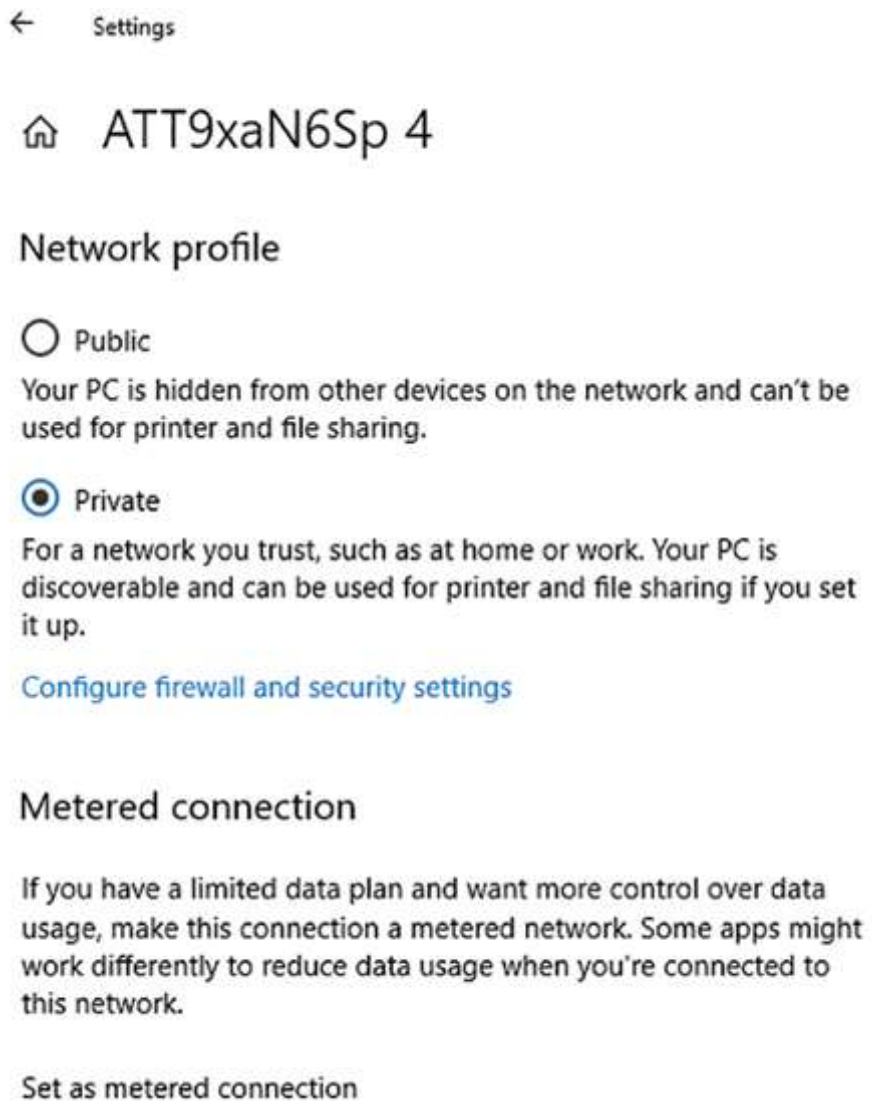


Figure 13.88 Windows public or private network profile

Notice at the bottom of Figure 13.88 the section for a metered connection. A **metered connection** is an internet connection that has a data limit imposed by the internet provider. You may be f
cause of your cell phone and cellular plan. Wi-Fi and
connections can also be configured to be metered.

Even though you can control many things from the notification area or from some of the Settings options on Windows 8, 10, and 11, many network configuration settings are still done through the *Network and Sharing Center* Control Panel. The *Network and Sharing Center* Control Panel has been used both in this chapter and in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies," but knowing the details and purpose of the options is important to IT personnel. Figure 13.89 shows the *Network and Sharing Center* window.

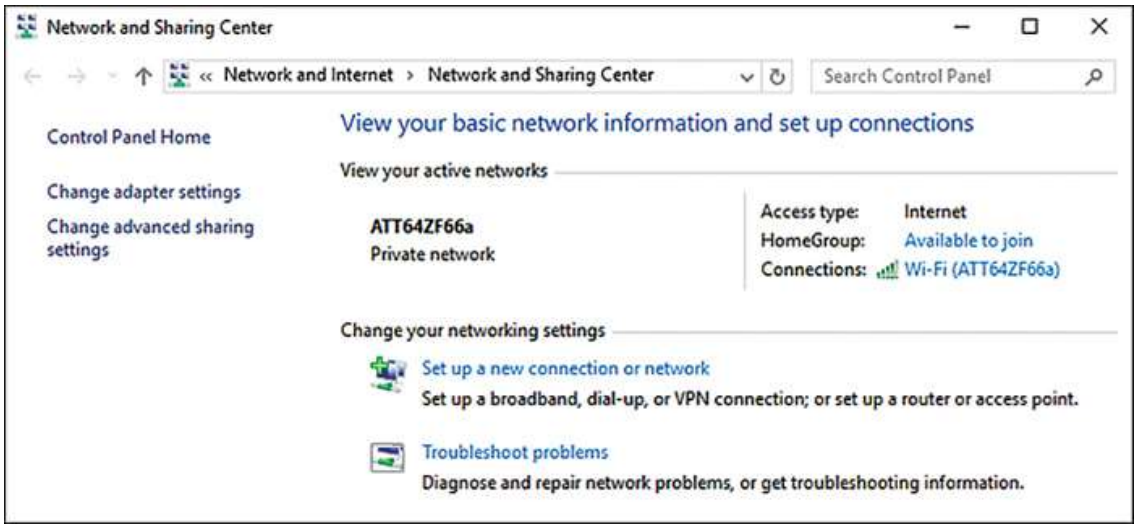


Figure 13.89 Windows Network and Sharing Center window

Notice in the main portion of the screen that you can see what network is currently being used. You can see whether the connection is wired or wireless and the name of the network. You can also tell in home or small business networks if the computer can share files with other devices (which is covered in the next section).

There are two important links in the left pane: *Change adapter settings* and *Change advanced sharing settings*. The *Change adapter settings* link enables you to access the network adapters that are i
Figure 13.90. If a network adapter that is installed in
listed, use *Device Manager* to troubleshoot and ensur
enabled through UEFI/system BIOS.

Figure 13.90 Windows 10 Network Connections window

The *Network Connections* window is important when configuring an adapter. In it you can perform some of the following tasks:

- Double-click the adapter icon to view device information. A wireless NIC shows wireless connectivity (see Figure 13.91), a wired NIC shows the wired network information (see Figure 13.92), and a Bluetooth adapter shows any Bluetooth pairs. At the bottom of each of the wired and wireless NIC windows, you can see the number of sent and received bytes.
- Select the *Details* button in the wireless or wired NIC windows (*Wi-Fi Status or Local Area Connection Status*) to see information similar to that provided with the command (see Figure 13.93). `ipconfig /all`

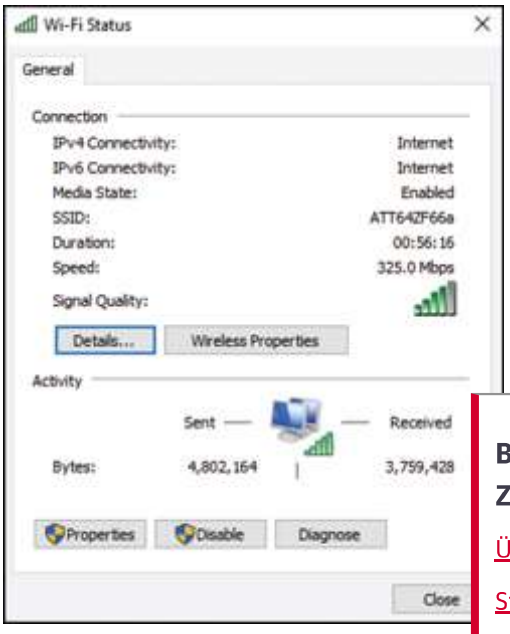


Figure 13.91 Wireless NIC window

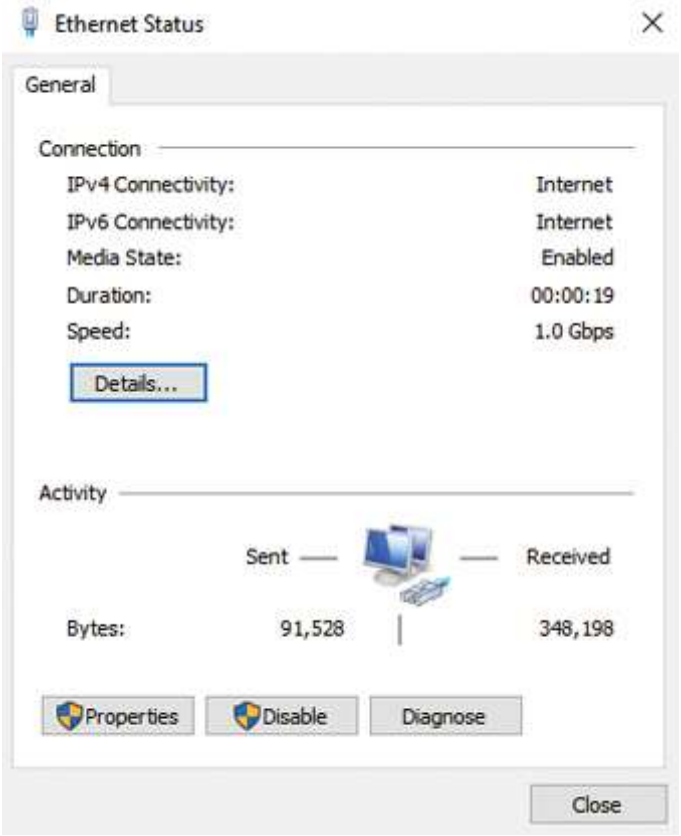


Figure 13.92 Wired NIC window

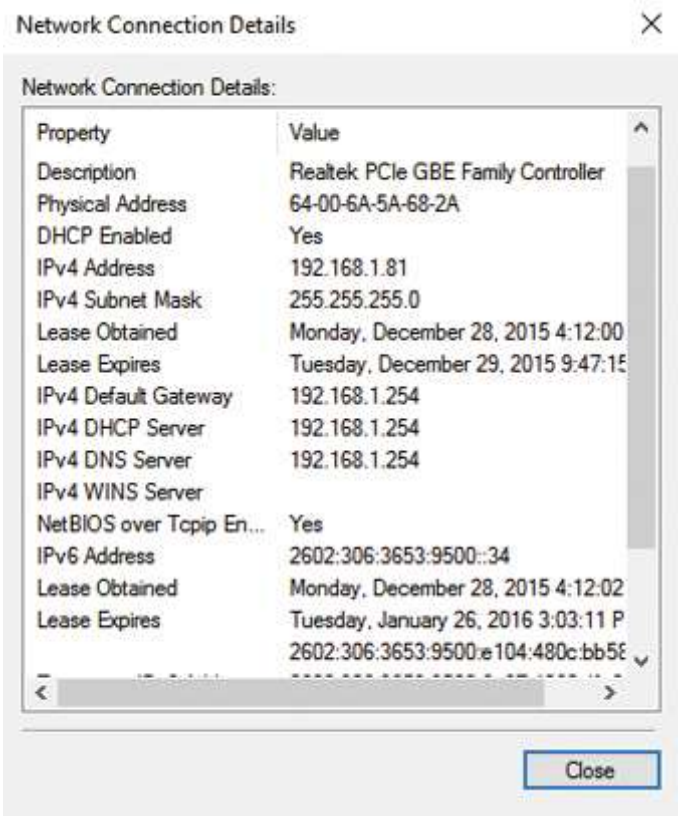


Figure 13.93 Wired or wireless NIC details

- Click the *Wireless Properties* button in the wireless NIC window (*Wi-Fi Status* window) to view information about the specific type of wireless network. Use the *Security* tab to view the type of security applied.
- In both the wireless and wired NIC windows, click the *Properties* button to manually configure the NIC properties or modify a connection, such as the TCP/IPv4 or TCP/IPv6 parameters (see Figure 13.94).
- Double-click the *Internet Protocol Version 4 (TCP/IPv4)* (or *TCP/IPv6*) link to configure the adapter for DHCP, statically assign an IP address (refer to Figure 13.58).
- Click or tap the *Configure* button to set wired or wireless NIC-related settings, such as speed and duplex.

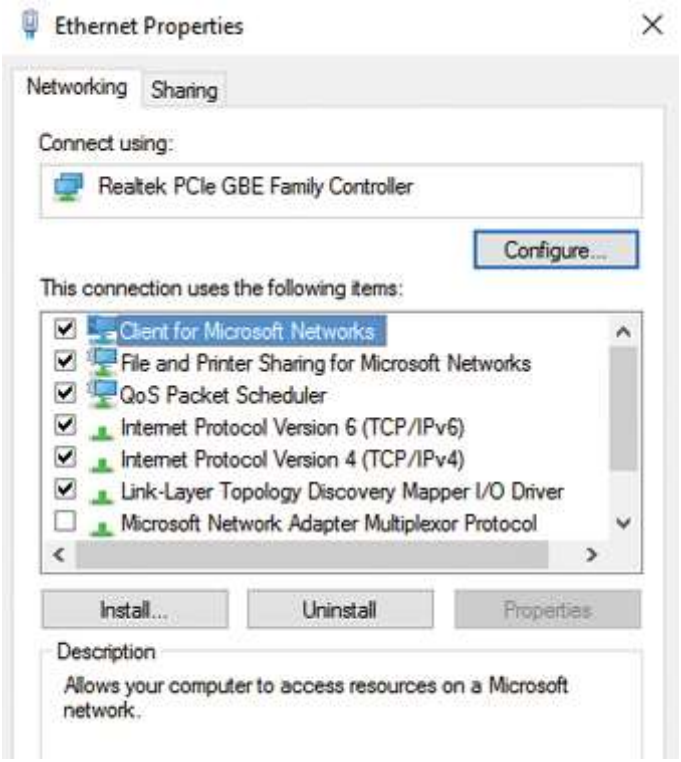


Figure 13.94 Wired or wireless networking properties window

- Manually configure the wireless NIC for a specific nonbroadcasting wireless network (refer to Figure 13.67).
- Set up a new Bluetooth connection. In Windows, access the *View Devices and Printers* Control Panel > *Add a Device* link. Ensure that the Bluetooth device is turned on and visible in the *Add a Device* window (see Figure 13.95). Select the device and click *Next*. Sometimes, a PIN or passcode must be verified in Windows and on the device.

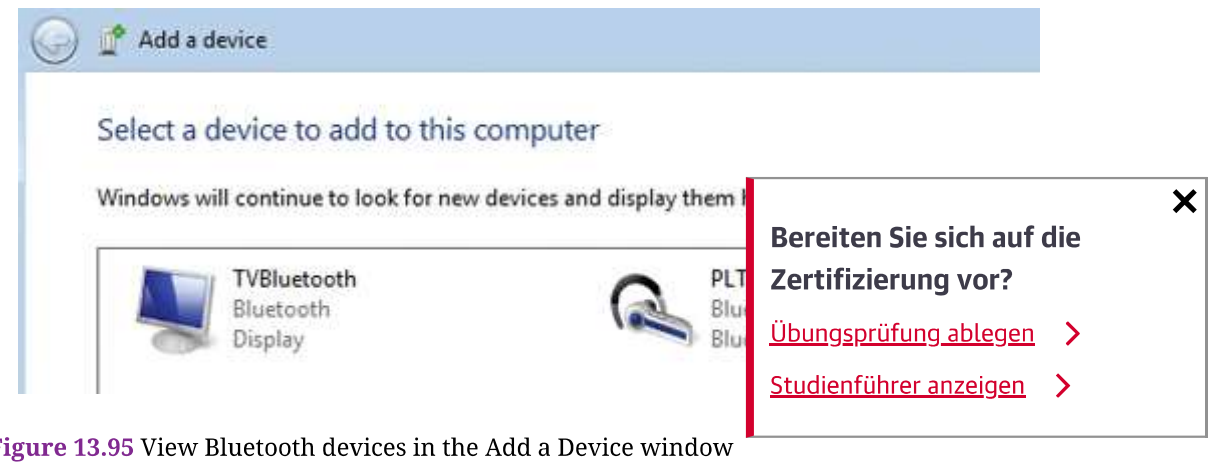


Figure 13.95 View Bluetooth devices in the Add a Device window

- Finally, from the *Network and Sharing Center* Control Panel, select *Change advanced sharing settings*. These settings relate to what the next section covers: sharing information across the networks you are now familiar with. Figure 13.96 shows the *Advanced sharing settings* window. Notice in the figure that there are three distinct and expandable sections: Private, Guest or Public, and All Networks. The Private section has been expanded so you can see the available options.

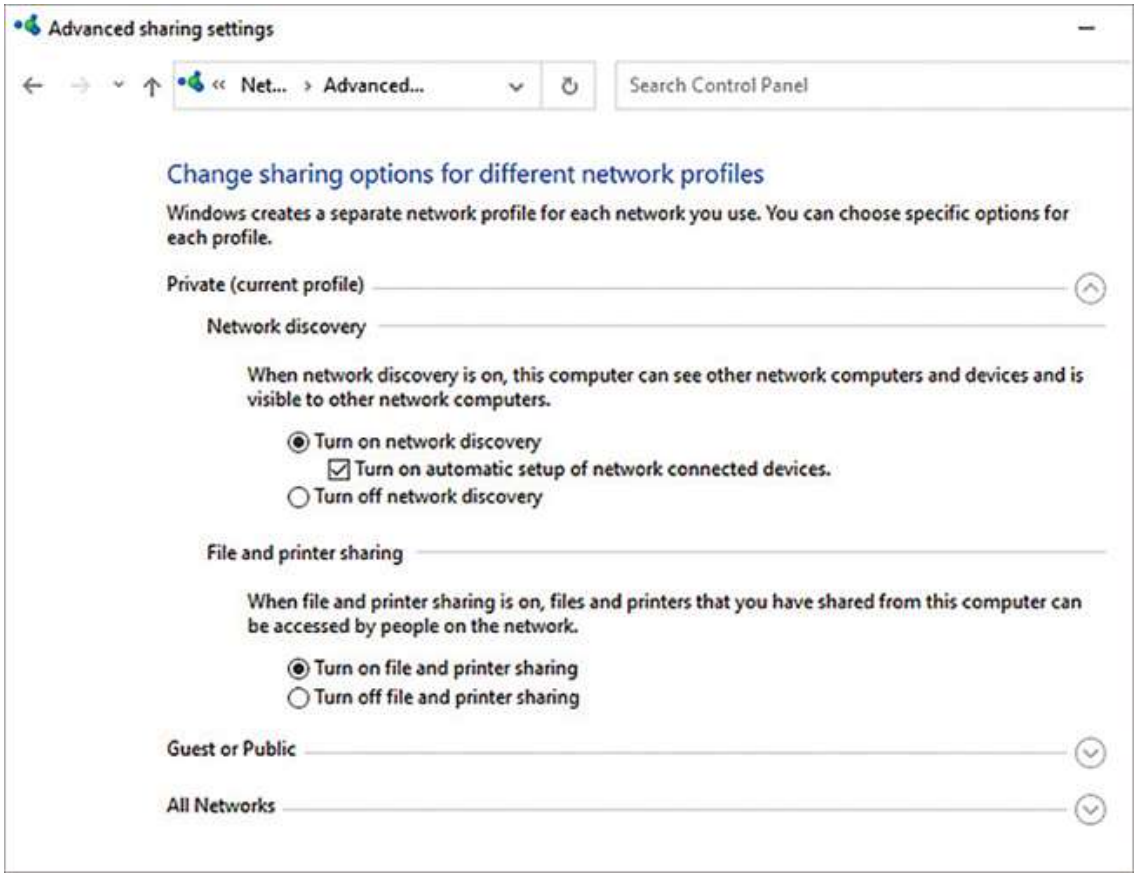


Figure 13.96 Advanced Sharing Settings window

Introduction to Shared Folders

When you double-click the *Network* option in Windo
(Windows 7) or File Explorer (Windows 8/10/11), you

work devices by their assigned names. You can also view network device names by typing at a command prompt. Knowing a network device name is important when accessing a network share across the network. A **network share** is a folder or device that has been shared and is accessible from a remote network device. `nbtstat -n`

Using the Sharing Tab > Share Button

You can set up any Windows computer as a file server and share files with other network devices. If you right-click on any folder and select *Properties* > *Sharing* tab, you can share documents within a folder two different ways. The most common way is with the *Share* button (See Figure 13.97).

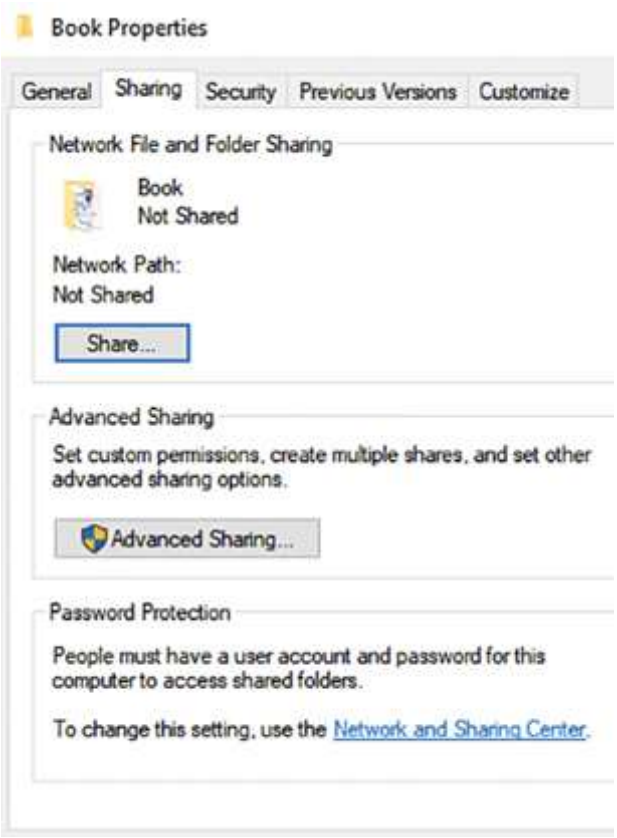


Figure 13.97 Sharing tab > Share button

Once you click on the Share button, you must cho
share the document with by clicking the down arrow

creating a new user, clicking the *Add* button > *Share* button (see Figure 13.98).

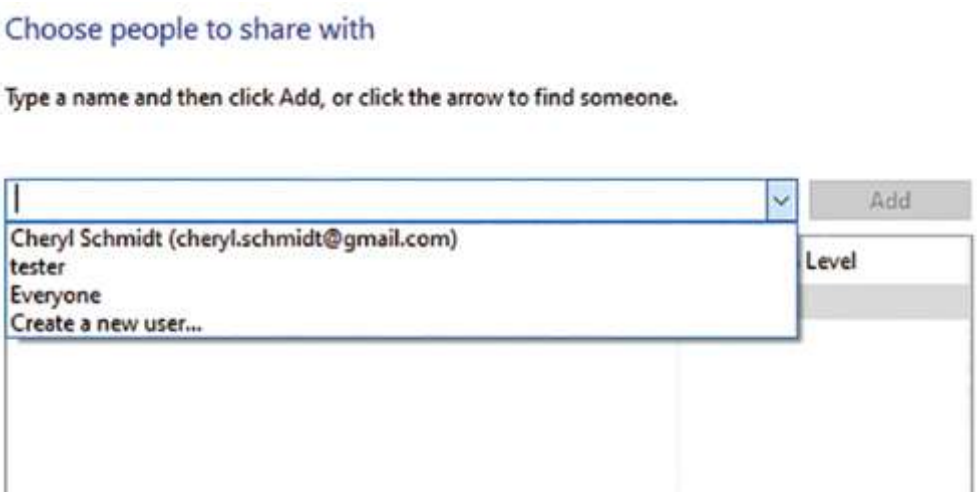


Figure 13.98 Adding a username to share the folder with

Once you click the *Share* button, the network path appears in the properties window, as shown in Figure 13.99.

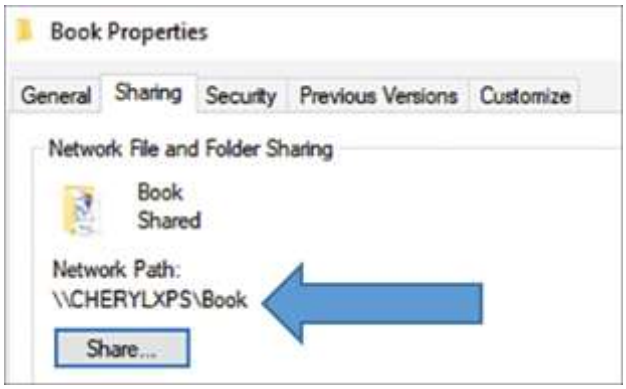


Figure 13.99 Network path

The network path is important to know when creating network shares. The **network path** is similar to driving locations to a restaurant except that it is how to get to something shared on the network from a remote device. The network path can be used from the command prompt or File Explorer to access the folder quickly. The networ full path to get to the document or shown using the U Convention (UNC). For example, say that a computer a network share called *TESTS*. By typing at the comm

access the network share. Or you can type the IP address of the computer instead of the computer UNC. For example, if the CSchmidt computer had IP address 192.168.10.5, you could use from the command prompt instead. The problem with this method is that computer IP addresses are commonly provided by DHCP and could change. Next week, the CSchmidt computer could have the IP address 192.168.10.77, and the command would have to be adjusted. The *Advanced Sharing* button can also be used to create a network share (see Chapter 18). `\\CSchmidt\TESTS \\192.168.10.5\TESTS`

Mapping to a Share

In a network, it is common to map a drive letter to a frequently used network share. To map a drive letter to a network share in Windows 7, click the *Start* button > *Computer* > *Map Network Drive* > select a drive letter in the *Drive* box > in the *Folder* textbox type the UNC for the network share or click the *Browse* button to select the network share. The *Reconnect at logon* checkbox allows you to connect to the mapped drive every time you log on.

In Windows 8/10/11, use File Explorer to locate and right-click *This PC* > *Map Network Drive* (though note that in Windows 11 you might have to select *Show more options* to see) > select a drive letter in the *Drive* box > in the *Folder* textbox type the UNC for the network share or click the *Browse* button to select the network share. The *Reconnect at sign-in* checkbox allows you to connect to the mapped drive every time you log on. Figure 13.100 shows the windows to map drive letter to the shared folder on the computer called CHERYL-PC. Expand the CHERYL-PC option to see the shared folders on this computer. `Z:`

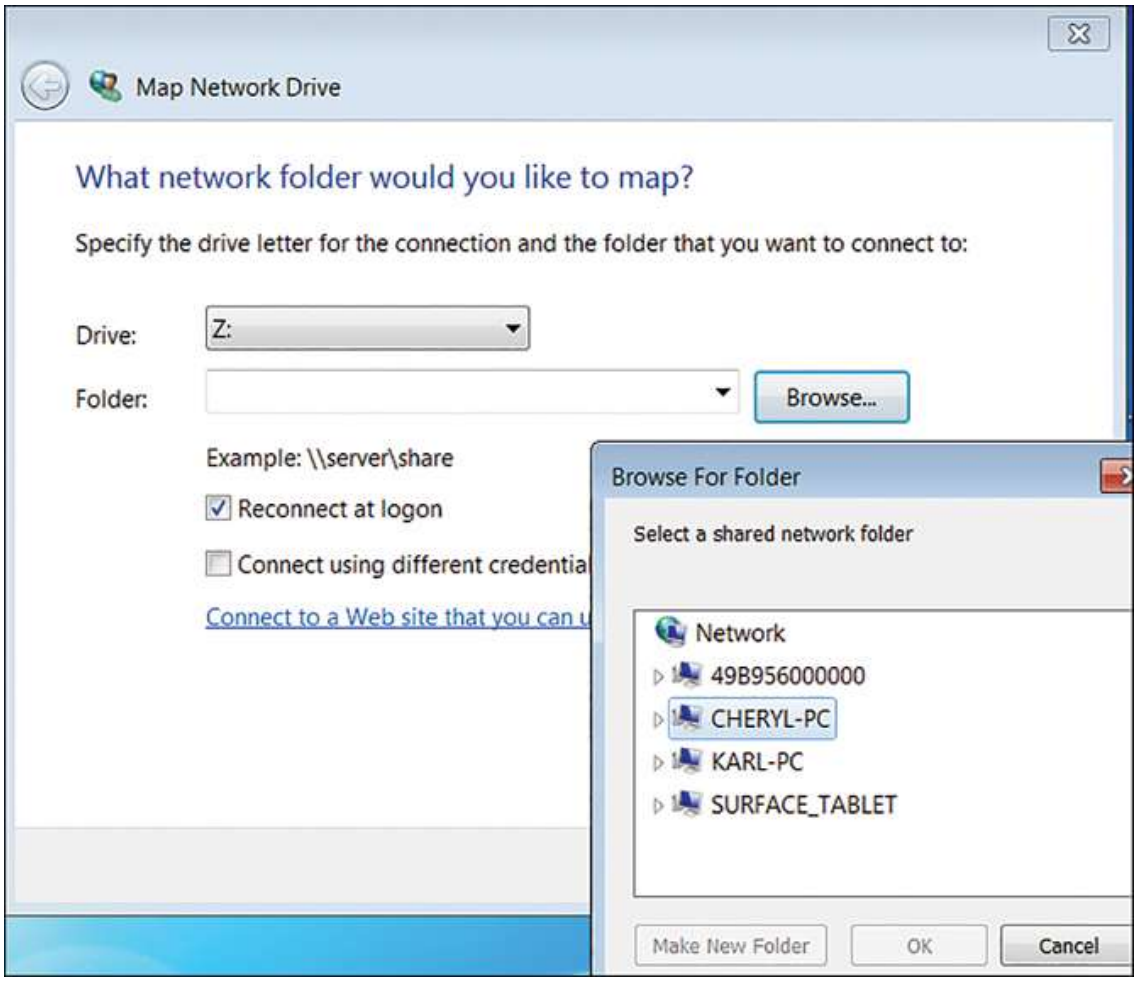


Figure 13.100 Windows Map Network Drive window

'ech Tip Seeing a mapped drive path in File Explorer

Select *This PC* and expand *Network locations*. Double-click the mapped drive to see the network path.

'ech Tip Mapping from a prompt

A drive can be mapped from a command prompt. Use more help. For example, say that a computer with the share called *Cheryl*. The following command can be u ing the drive letter `net /? M: net use m: /persist \\TECH01\Cheryl`

Computer users commonly have frequently used network shares mapped to drive letters. It is faster to access a network share by drive letter than by searching around for the share through the *File Explorer Network* option.

Soft Skills: Being Proactive

A good technician is **proactive**, which means the technician thinks of ways to improve a situation, anticipates problems, and fixes problems before being told to. A proactive technician follows up after a service call to ensure that a repair fixed the problem rather than waiting for another help desk ticket that states that the problem is unresolved. When something happens or a problem with a customer occurs, a proactive technician provides a list of recommended solutions or procedural changes to the supervisor rather than waiting for the supervisor to delineate what changes must occur.

For example, consider a technician at a college. The technician is responsible for any problems logged by computer users through the help desk. The technician is also responsible for maintaining the computer classrooms used by various departments. Each term, the technician reloads the computers with software updates and changes requested by the teachers. A proactive technician checks each machine and ensures that the computers boot properly and that the load is successful.

Another example involves checking new software. When the computers are reloaded each term, a faculty member is asked to check the load. A proactive technician has a list of "standard" software loaded on the computer, such as the operating system, service pack level, and any applications that are standard throughout the college. A separate list would include the changes that have been applied to the computer. Then the faculty member can simply look at the list and verify the load. Being proactive actually saves time for both the technician and th

The opposite of proactive is *reactive*. A reactive te situations only when there is a problem reported. A r does not look for ways to avoid problems. For examp

nician ensures that a computer is configured with automatic updates of virus scanning software. A reactive technician waits until a help desk ticket is created for a computer that exhibits unusual behavior (for example, it has a virus) even though the technician notices the unusual behavior when installing a second monitor.

As a student, practice being proactive. Start an assignment a day before you would normally start it. Talk to your teacher about your grade in advance (before the day preceding the final). Bring to school something to write with and paper. Finally, take this practice into your IT career: Be proactive as an IT professional and increase the level of service and professionalism in the field.

Chapter Summary

- Networks are created to share data and devices and connect to the internet. Types of networks include PANs, LANs, MANs, SANs, WANs, and WMNs.
- Networks can be wired or wireless.
- A workgroup network is composed of a small number of computers, whereas larger companies use a domain environment. A domain environment has a server that provides authentication to resources with a centralized user ID and password. A workgroup network manages the usernames on a computer-by-computer basis, which grows less secure and more difficult to manage as the network grows.
- An Ethernet LAN, which is the most common type of LAN, is wired in a star or extended star topology. A switch is used to connect the devices. Each network connects to a router for communication with other networks. The router's IP address is the default gateway for all network devices on a particular LAN.
- Computers must have IP addresses to participate in a TCP/IP-based network (and gain access to the internet). IPv4 is the most common addressing used on computers today, but IPv6 addresses are slowly being assigned and used by corporate devices and internet providers.
- IP addresses are grouped by classes, with a particu
  each class. Each default mask can be changed to f
  network for more efficient and manageable addre
  provide addresses to network devices, or a static a

signed. Public addresses are routable on the internet. Private addresses are used within homes and companies.

- TCP/IP is a suite that includes the following important protocols: FTP, Telnet, SMTP, DNS, DHCP, HTTP, HTTPS, POP3, IMAP, RDP, LDAP, SNMP, SSH, SFTP, SMB/CIFS, TCP, UDP, IP, and ICMP.
- The OSI model is a networking model that has seven layers: application, presentation, session, transport, network, data link, and physical. The TCP/IP model is a working model that contains four layers: application, transport, internet (internetwork), and network access. The devices and applications that work at Layer 3 (network or internet layers) include routers, IP, and ICMP. The devices and applications that work at Layer 2 (data link or network access) include switches, access points, and ARP. Keep in mind that Ethernet has Layer 2 specifications. This is why a MAC address is a Layer 2 address. The devices that work at Layer 1 (physical layer or network access layer) are cables, connectors, hubs, and wireless antennas.
- 802.11 and Bluetooth are wireless network technologies. Bluetooth is used in PANs, and 802.11 is used in wireless LANs. 802.11 wireless NICs include 802.11a, b, g, n, ac, and ax. 802.11a, n, ac, and ax work in the 5 GHz range; 802.11b, g, n, and ax work in the 2.4 GHz range. 802.11ax also functions in the 6 GHz range using Wi-Fi 6E. 802.11 antennas are either directional or omnidirectional.
- The key tools for troubleshooting a networked computer are the , , , and commands and a cable tester. `ipconfig ping pathping, nslookup tracert`
- A technician should be proactive as opposed to reactive and should prevent problems and situations whenever possible.

A+ CERTIFICATION EXAM TIPS

- ✓ This chapter provides information related to both the 220-1101 and 220-1102 exams. The information related to the 1102 exam includes the *Network and Sharing Center* Control Panel, *Network & Internet* settings, and network client configuration (including IP addressing scheme, DNS settings, subnet mask, gateway, static and dynamic ad work connection, wireless, wireless WWAN [cellular] commands—, , , , , , , and —NIC properties, network mapping). `ipconfig ifconfig nslookup tracert ne user pathping ping`

- ✓ Know the difference between a LAN, WAN, PAN, MAN, SAN, and WLAN.

- ✓ Know the purposes of these network devices: hubs, routers, access points, firewalls, patch panels, cable/DSL modems (see Chapter 12), repeaters, PoE devices (injectors and switches), and switches (both managed and unmanaged). Also be able to describe how software-defined networking (SDN) takes functions normally provided in hardware by dividing functions into the control and data planes.

- ✓ Know the purposes of key networking protocols, port numbers used by the protocols, and the differences between TCP and UDP.

- ✓ Know when to use a particular type of networking tool, whether it is a physical tool or a command. Physical tools include crimpers, cable strippers, Wi-Fi analyzers, toner probes, punchdown tools, cable testers, loopback plugs, and network taps.

- ✓ Describe how a hub and switch operate and the differences between the two. Know what a VLAN is and how it is configured on a switch.

- ✓ Know what to do when one or more computers cannot connect to the internet or when they have an IP address conflict. Be able to tell whether the problem is an internet connection problem or what specific network resources the device can't reach, such as network shares, printers, or email.

- ✓ Know how to manually configure an IP address on a network device such as a computer, an AP, or a printer.

- ✓ Know the different types of wireless networks and their compatibility with each other.

- ✓ Be able to configure a wireless network and 2.4 GHz and 5 GHz channels so multiple wireless APs can coexist as well as other parameters, such as an administrator password and DHCP.

- ✓ Know the purpose of an IP address, a default gateway

- ✓ Know the difference between an IPv4 address and an

- ✓ Recognize when an address is a private IP address and understand the difference between a public IP address and a private IP address.
- ✓ Be familiar with DHCP terminology such as leases, reservations, and scope.
- ✓ Know the different types of network cabling and connectors.
- ✓ Recognize when a computer gets assigned an IP address from APIPA.
- ✓ Know the port numbers and purposes of the following protocols as well as the differences between TCP and UDP: 20/21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 67/68 (DHCP), 80 (HTTP), 110 (POP3), 143 (IMAP), 443 (HTTPS), 3389 (RDP), 137–139 (NetBIOS/NetBT), 161–162 (SNMP), 389 (LDAP), 445 (SMB/CIFS).
- ✓ Know the purposes of different servers: web, fileshare, print, DHCP, DNS, mail, syslog, and authentication (AAA).
- ✓ Review the section on troubleshooting network printer problems.
- ✓ If a wireless laptop cannot get on a wireless network, you might have to forget the network, reconnect, and provide credentials. You can also check to see if wireless has been disabled.
- ✓ Be able to recognize and troubleshoot problems with IP addressing information that comes from a DHCP server (including IP address, default gateway, subnet mask, and DNS server address).
- ✓ Be able to troubleshoot wireless problems. Move the device to a different location. Make sure that the wireless NIC is turned on.
- ✓ Be able to use the command and review the options available (to see). `ipconfig ipconfig /?`
- ✓ Know the difference between how a hub operates an operates.
- ✓ Review the different DNS message types: A, AAAA, M

✓ Be able to describe the services provided by IoT devices and legacy/embedded systems like SCADA.

Key Terms

2.4 GHz

5 GHz

6 GHz

802.11a

802.11ac (Wi-Fi 5)

802.11ad

802.11ax (Wi-Fi 6)

802.11b

802.11e

802.11g

802.11i

802.11n

A record

AAA server

AAAA record

access point

AES

APIPA

Bluetooth

broadcast address

cable management system

cable stripper

cable tester

Cat 5

Cat 5e

Cat 6

Cat 6a

channel

CIDR

CIFS

client-side DNS

connection-oriented

connectionless

content filtering

control plane

crimper

crossover cable

data plane

default gateway

DHCP

DHCP lease time

DHCP reservation

DHCP scope

DHCP server

direct burial cable

directional antenna

DMZ

DNS

DNS server

domain

duplex

embedded system

Ethernet

Ethernet over Power

external interference

FC

fileshare server

firewall

firmware

FTP

gateway

high latency

host address

HTTP

HTTPS

hub

`ifconfig`

IMAP

intermittent connectivity

intermittent wireless connectivity

IoT

IP address

IP addressing scheme

IP filtering

`ipconfig`

IPv4

IPv6

iSCSI

LAN

LDAP

legacy system

limited connectivity

link-local address

loopback plug

low RF signal

MAC address

mail server

MAN

managed switch

metered connection

MIMO

MU-MIMO

MX record

`net`

`net use`

`net user`

NetBT

`netstat`

network number

network path

network protocol

network share

no connectivity

no internet connectivity

`nslookup`

omnidirectional antenna

OSI model

PAN

patch panel

`pathping`

`ping`

plenum cable

PoE

PoE injector

PoE switch

POP3

port flapping

port forwarding

port mapping

print server

printer sharing

private IP address

private network

proactive

proxy server

public IP address

public network

punchdown tool

PVC

QoS

RDP

Remote Desktop Services

RJ11

RJ45

router

SAN

SCADA

screened subnet

site survey

slow network speed

SMB

SMTP

SNMP

speed (NIC property)

SSH

SSID

SSID not found

STP

straight-through cable

subnet mask

switch

syslog server

T568A

T568B

TCP

TCP/IP

Telnet

TKIP

tone generator

toner probe

`tracert`

twisted pair cable

UDP

unavailable resources

unmanaged switch

UPnP

UTP

virtual NIC

VLAN

Wake on LAN

WAN

web server

WEP

Wi-Fi analyzer

wireless extender

wireless regulations

WLAN

WMN

workgroup

WPA

WPA2

WPA3

WWAN

Zigbee

Z-Wave

Review Questions

1. Match the network type on the left with the scenario on the right.

____ MAN	**a.**	Home network of four PCs
____ SAN	**b.**	City of Schmidtville networks
____ PAN	**c.**	Hewlett-Packard corporate networks
____ WAN	**d.**	Bluetooth network of two devices
____ LAN	**e.**	Data storage for a company

2. Match the following. Note that even though an answer may be valid for more than one answer, only one answer will allow all answers to be used. No term is used twice.

a. Cat 8	____ Common type of LAN cable
b. Cat 6a UTP	____ 1 Gbps over UTP
c. 1000BaseT	____ Can only use STP
d. 1000BaseSX	____ 1 Gbps over fiber

3. Which network device would be best to use to connect wired devices, is common for this purpose, and can send data directly to the destination device without sending the data as a broadcast to every connected device?

[Access point | Hub | Router | Switch]

4. Match each TCP/IP model layer to a description. Note that a layer can be used more than once.

a. Application	____ HTTP	____ a straight-through cable

b. Transport	____ a router	____ UDP	____ DNS
c. Internet	____ a switch	____ IP	____ TCP
d. Network access	____ ICMP	____ MAC address	____ a wireless antenna

5. Some computers (both wired and wireless) in a specific area of the building are having problems connecting to printers, servers, and the internet. What should the technician do?

a. Use a tone generator.

b. Check the access point.

c. Check the router that connects to the internet.

d. Check problem computers for a DNS server address.

6. Software-defined networking splits tasks into which two major areas?

a. Data plane and control plane

b. 2.4 GHz and 5 GHz

c. UTP and STP

d. Network and transport

7. Which network device works at Layer 1 and sends received data out all its ports (except the port that received the data)?

[Switch | Antenna | Router | Hub]

8. What is the most common network protocol suite and required to communicate on the internet?

[LTE | TCP/IP | Bluetooth | ISO]

9. Which type of address is 48 bits long and is hard coded into a NIC? [IP | TCP | MAC | NAT]

10. Which type of address is called a Layer 3 address and needed to get to the internet? [IP | TCP | MAC | NAT]

11. Which type of IP address uses 128 bits? [IPv4 | IPv32 | IPv6 | IPv64]

12. Draw a vertical line between the network number and the host number for each of the following IP addresses (assuming the default subnet mask):

130.5.15.177	130.5.| 15.177
192.168.13.15	192.168.13.| 15
10.12.17.18	10.| 12.17.18

13. What protocol could be used to issue an IP address and the IP address of the DNS server to network devices?

[DNS | DHCP | ICMP | ARP]

14. What protocol is used to convert URLs to IP addresses?

[HTTP | SSH | SSL | UDP | DNS]

15. Two access points connect and extend *the same* wireless network. List the SSIDs for each access point in the following chart.

Access point	SSID
Access Point 1	
Access Point 2	

16. Two access points (AP1 and AP2) operating in the 2.4 GHz range have overlapping coverage areas. List the two channel IDs to assign to each access point by filling in the following chart.

Access point	Channel ID
AP1	
AP2	

17. Which connectors are commonly used on network ports that connect to a SAN? (Choose two.)

[RJ11 | RG-59 | FC | SATA | iSCSI]

18. A user has shared a folder with her corporate team. What information will the user need to give coworkers to enable them to easily access the shared documents across the network?

[UNC | IP address of the computer that has the shared folder | MAC address of the computer with the shared folder | Network path for shared folder]

19. Match each technology to the appropriate definition. Note that not all of the definitions are used.

____ 802.11a **a.** Operates in the 2.4 GHz range, with speeds up to 54 Mbps

____ 802.11b **b.** Operates in the 2.4 GHz range, with speeds up to 2 Mbps

____ 802.11g **c.** Operates in the 2.4 GHz range, with [illegible] Mbps

____ 802.11i **d.** Security specification

___ 802.11n **e.** Operates in the 5 GHz range, with speeds up to 54 Mbps

___ 802.11ac **f.** Specifies interoperability between access points

___ 802.11ax **g.** Standard for quality of service

h. Standard for wireless interference

i. Backward compatible with 802.11a, b, and g

j. Allows eight simultaneous data streams

k. Allows access to 6 GHz range with Wi-Fi 6E

20. In Figure 13.101, what IP address is the default gateway for host 203.145.15.2?

_____

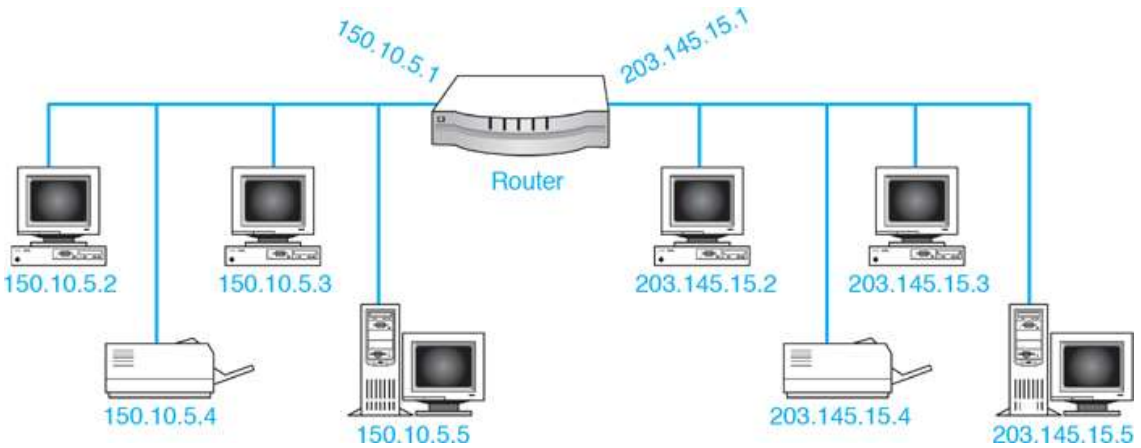


Figure 13.101 Review question network scenario

21. Which command determines whether another network device is reachable?

[`ping` | | | `ipconfig ipconfig /all arp -a`]

22. On which network device would VLANs be configured?

[Hub | Switch | Router | Firewall]

23. Which port numbers are used by a protocol whose purpose is to allow remote connectivity to a network device such as a server or router in order to make changes to the device? (Choose two.)

[21 | 22 | 23 | 53 | 69 | 80 | 443]

24. What command can be used to see a computer's MAC address?

[`netdom` | | | `net netstat ipconfig /all`]

25. A technician is setting up a new printer and notices that the computer is running unusually slowly. The technician decides to not only do the job that was logged (install the new printer) but also investigate the computer issue. Is the technician being reactive or proactive?

[Proactive | Reactive]

Exercises

Exercise 13.1 Understanding Wireless AP Paper Configuration

Objective: To determine what menu items would be used for specific functions

Procedure: Use the given menu options to determine which one would be used to perform a common configuration task on a wireless AP.

Note: Many times an IT professional must
or a particular model that is unfami

less AP menus are similar, so practicing which menu option might be the one chosen is a good activity.

Wireless AP sample menu and submenu options:

a. *Setup:* Language, Date/Time

b. *Wireless:* Basic Wireless Settings, Wireless Security, Wireless MAC Filter, Advanced Wireless Settings

c. *WAN/LAN:* Internet Setup and Network Setup

d. *Administration:* Management, Access, Security, Factory Defaults, Firmware Upgrade

e. *Status:* Access Point, Wireless Network, About

Select which menu option would be used to do each of the following tasks:

____ **1.** Change the password used to access the AP menu.

____ **2.** Configure UPnP.

____ **3.** Configure to only allow 802.11n 2.4 GHz devices to attach (not 802.11b or g).

____ **4.** Check connectivity with another device.

____ **5.** Change the SSID.

____ **6.** Disable SSID broadcasting.

____ **7.** Configure the device as a DHCP server for v

____ **8.** Set the year.

____ **9.** Reset the device.

___ **10.** Determine how many wireless hosts are currently attached to the AP.

Exercise 13.2 Understanding T568B Color Sequence

Objective: To articulate the proper color order of a T568B straight-through cable

Procedure: Use the given graphic to denote which color of cable goes into the connector from left to right.

Use Figure 13.102 to designate which colors of vinyl insulator should go into making a T568B connector.

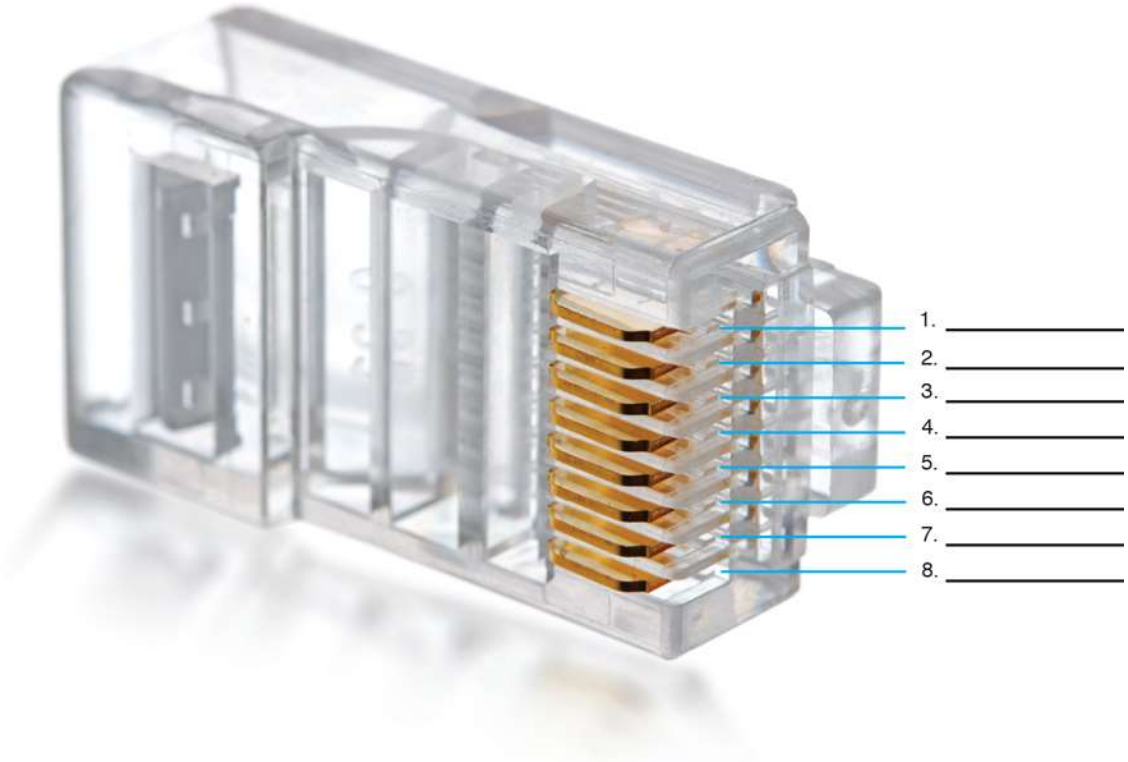


Figure 13.102 RJ45 connector/cabling exercise

Exercise 13.3 Recognizing Network Devices

Objective: To recognize a network device on si

Procedure: Use Figure 13.103 to identify each n

Note: Possible answers could include the following. Note that not all devices are used. No device is shown twice.

Possible devices:

Internet router	Termination plate	Switch
Hub	Patch panel	Repeater
Bridge	Wireless router	Firewall

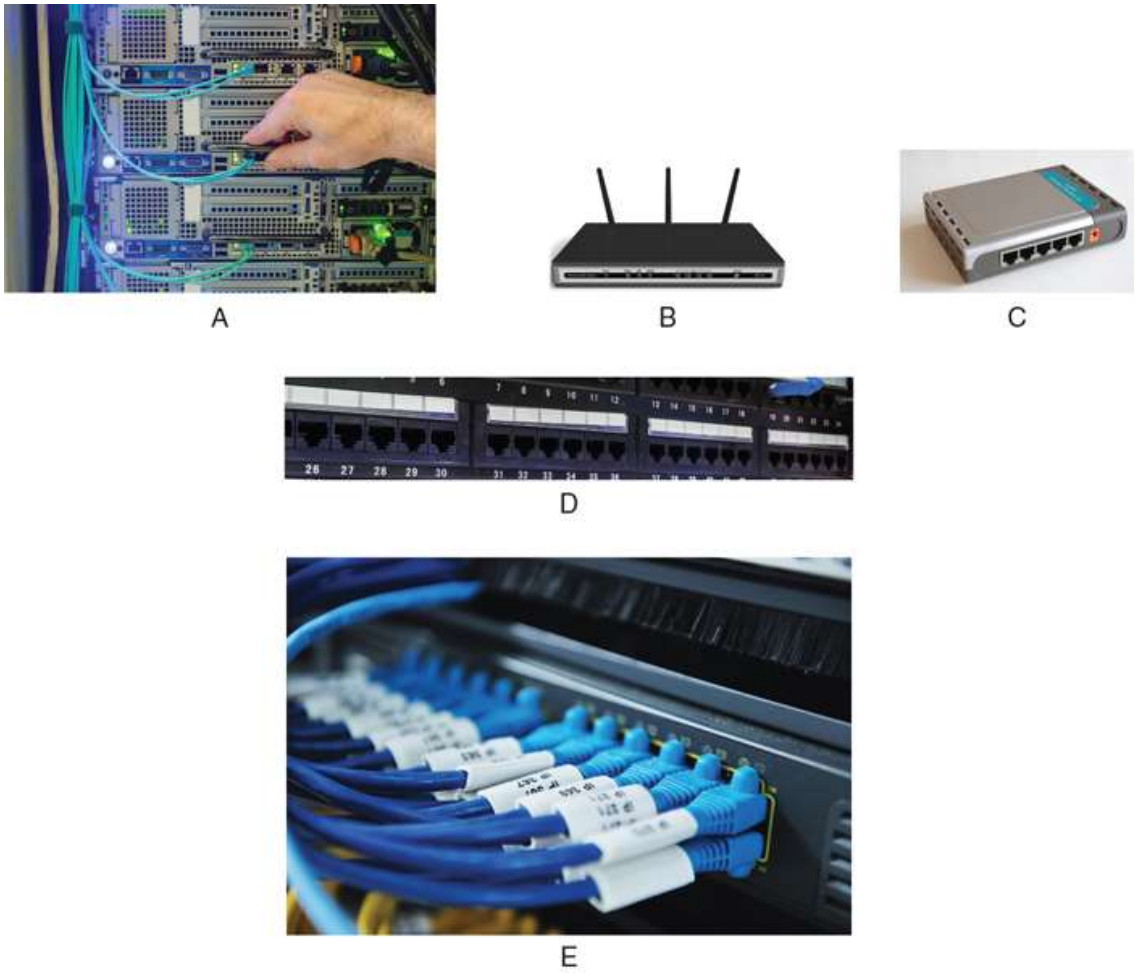


Figure 13.103 Network device identification

a.

_____

b.

_____

c.

d.

e.

Exercise 13.4 Identifying Basic Wireless Network Parts

Objective: To identify basic parts of a wireless network and determine the type of wireless network used

Procedure: Using Figure 13.104, identify the major parts of a wireless network. For the number 5 blank, document whether this network would most likely be for a home or a corporate network and explain why.

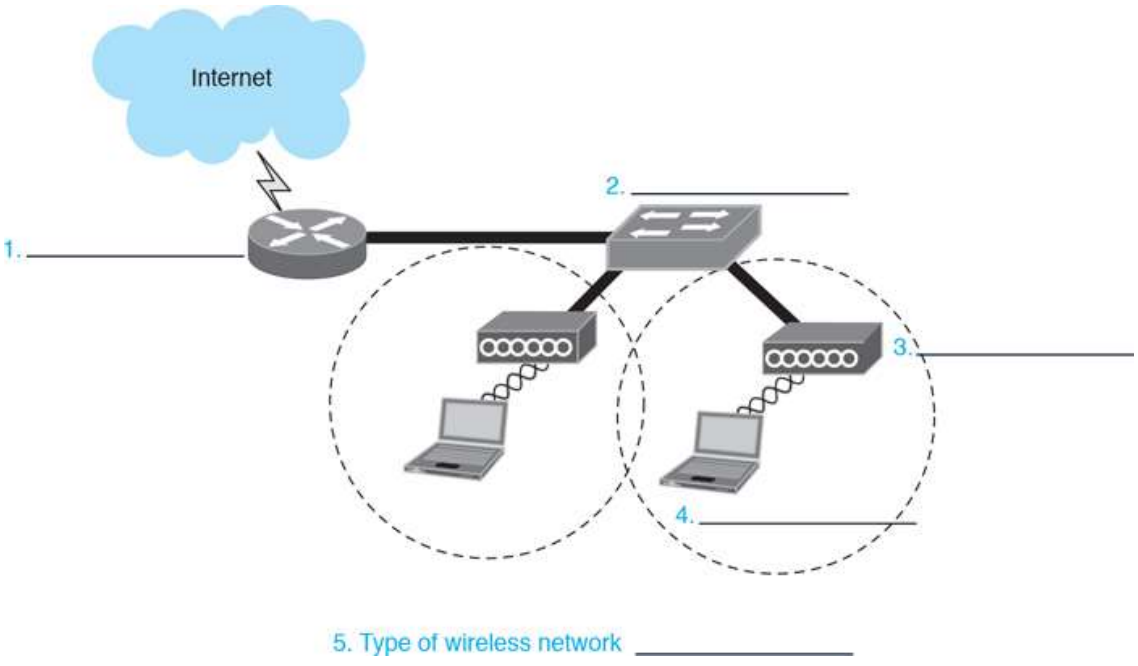


Figure 13.104 Wireless network components

1.

2.

3.

4.

5.

Exercise 13.5 Creating a Wireless Network

Objective: To design and price a wireless network based on the parameters given

Parts: Computer with internet access

Note: The instructor or lab assistant can speak on behalf of the faculty members if any design questions arise.

Scenario: A building has just been renovated to include corporate offices, as shown in Figure 13.105. The only wired network connections are the two stations in the reception area and the plotter in the leftmost office area. All other connections are wireless.

Figure 13.105 Building floor plan for wireless design

Tasks:

1. Design a 2.4 GHz wireless network plan that will cover the reception area and all office stations to the right. Draw a circle over each coverage area and label each circle with a 2.4 GHz channel ID.

2. Design a 5 GHz wireless network plan that will cover the conference room and all remaining office areas. Draw a circle over each coverage area and label each circle with a 5 GHz channel ID.

3. Provide a detailed list of wireless network parts, part numbers, and prices, as well as a web link where the prices were obtained. Be sure to include the antenna type, a printout of the wireless antenna radiation pattern, and antenna coverage range.

4. Provide the instructor with a typewritten list of policies and configuration settings for the wireless network you have designed. You are the designer and implementer, and what you decide goes.

Exercise 13.6 Practicing with Network Numbers ar Addresses

Objective: To determine the subnet numbers, broadcast addresses, and IP addresses that can be assigned to network devices

Procedure: Complete the following procedure and answer the accompanying questions.

1. Determine the network address for each of the following IP addresses, assuming that the default subnet mask is used.

   210.141.254.122 _____

   206.240.195.38 _____

   14.130.188.213 _____

   129.89.5.224 _____

   110.113.71.66 _____

2. Determine the broadcast address for each of the following IP addresses, assuming that the default subnet mask is used.

   166.215.207.182 _____

   198.94.140.121 _____

   97.57.210.192 _____

   133.98.227.36 _____

   14.89.203.133 _____

Exercise 13.7 Practicing with CIDR Notation

Objective: To determine the appropriate CIDR a given subnet mask

Procedure: Complete the following procedure and answer the accompanying questions.

For each subnet mask given in dotted decimal notation, determine the equivalent CIDR notation.

255.255.255.0 _____

255.255.255.224 _____

255.255.255.252 _____

255.255.254.0 _____

255.255.0.0 _____

255.255.255.128 _____

255.255.255.192 _____

255.0.0.0 _____

255.255.240.0 _____

255.255.255.240 _____

Exercise 13.8 Determining the Default Gateway

Objective: To determine the appropriate default gateway for a PC based on a given situation.

Procedure: Complete the following procedure a
companying questions.

1. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 1 shown in Figure 13.106.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

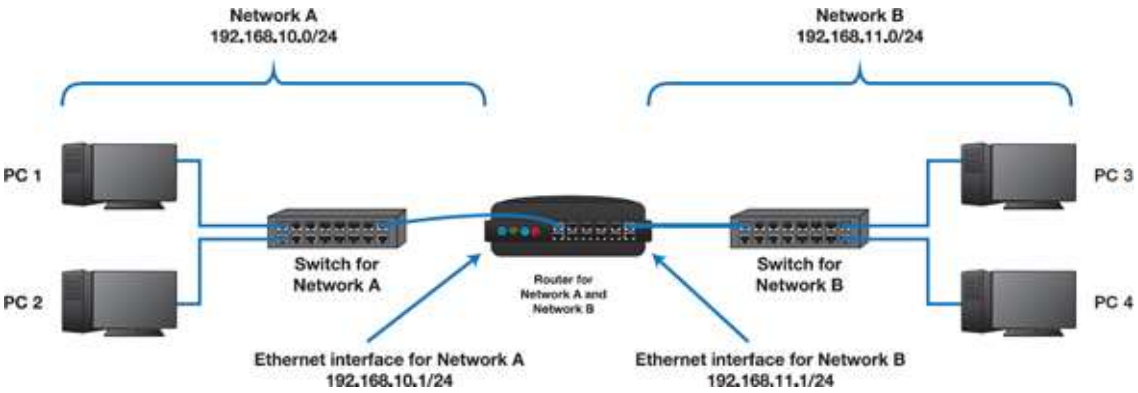


Figure 13.106 Network Topology 1

2. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 2 shown in Figure 13.106.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

3. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 3 shown in Figure 13.106.

   IP address: _____

   Subnet mask: _____

Default gateway: _____

4. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 4 shown in Figure 13.106.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

5. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 1 shown in Figure 13.107.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

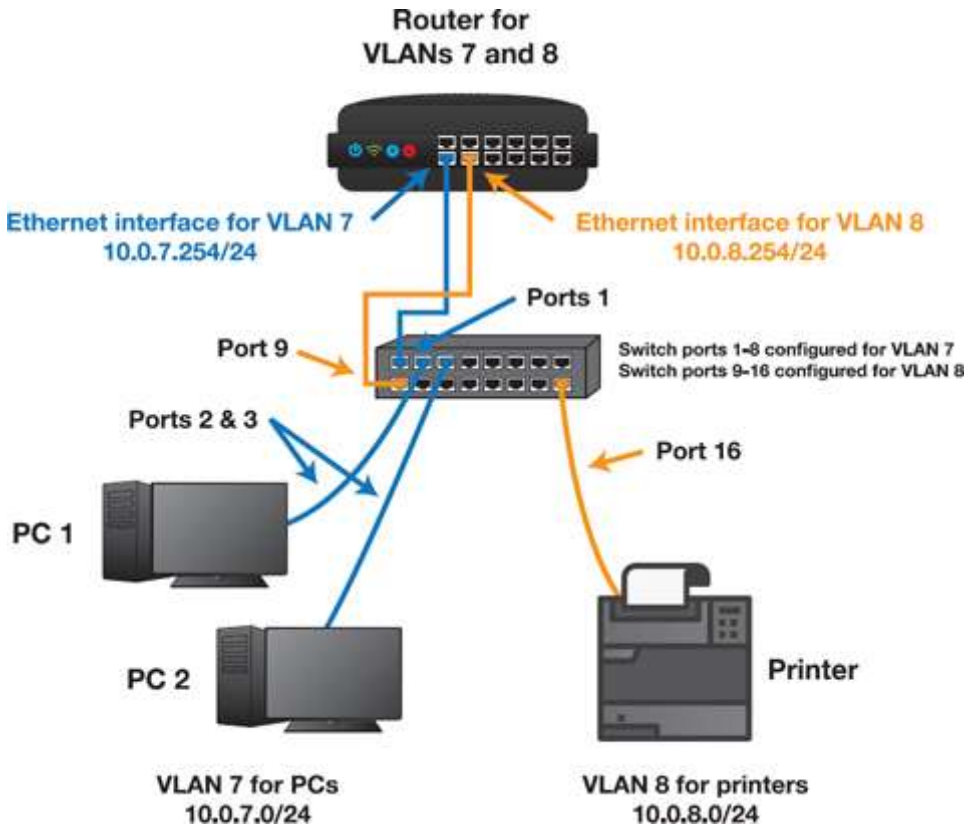


Figure 13.107 Network Topology 2

6. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for PC 2 shown in Figure 13.107.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

7. Determine the appropriate IP address, subnet mask (in dotted decimal notation, x.x.x.x), and default gateway for the printer shown in Figure 13.107.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

Activities

Internet Discovery

Objective:	To obtain specific information regarding a computer or its associated parts on the internet
Parts:	Computer with internet access
Procedure:	Complete the following procedure a companying questions.

1. On an HP ProBook 650 Windows 10 laptop, you cannot get the wireless NIC to attach to the wireless network. What are some steps you can take, as recommended by HP, to help in this situation?

   Write at least three solutions as well as the URL where you found the solution.

2. What does the term Wake on Wireless mean, and at what URL did you locate the answer?

3. Locate a website that describes how to reserve an IP address on a Netgear router. Write the one router model the answer applies to, the menu option used to configure it, and the URL where you found this information.

4. Find an internet forum that discusses Bluetooth and Windows 7 on Lenovo laptops. Write one key piece of information you found about configuring Bluetooth. Write the URL where you found the information.

_____

_____

5. Find a website that explains the differences between Cat 5e and Cat 6a UTP cable. Write which standard you would recommend to the CIO of your company and why. List the URL where you found this information.

_____

_____

_____

_____

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. Using the internet, find and access a utility that tests your soft skills. Compare your scores with those of others in the class. Discuss how you might improve in specific weak areas.

2. In groups of two, one person inserts a network problem in a computer while the other person is out of the room. When the other person comes back, they troubleshoot the problem by asking questions of the user (as if they were on the phone helping them). The person performing the troubleshooting cannot touch the computer. Discuss strategies for improving this troubleshooting process before swapping roles.

3. In groups of two or three, brainstorm three examples of a technician being reactive rather than proactive. List ways the technician could be more proactive for each example. Share your findings with other teams.

_____

_____

_____

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. A home user connects to the internet. The ISP provides hard drive space for the user's web page. Is this a network? Why or why not? Write your answer in a well-written paragraph using good grammar, capitalization, and punctuation.

_____

_____

_____

2. Use the internet, magazines, newspapers, or books to find a network installation case study. Make a table of terms the case study uses that were introduced in this chapter. On the left side, list the term, and on the right side, define or describe how the term relates to the network installation. Analyze the installation and discuss with a team. Make a checklist of approved processes and of recommended changes to implemented processes. Share your team findings with the class.

3. In a team environment, design a wired and wireless network for a small business with 10 computers. Name the business, provide a design and implementation plan, and provide a list of items for which you should do more research. Share your plan with the class.