Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**5**

**Cabling**

* [Module Introduction](javascript://)
* **5-1**[Transmission Basics](javascript://)
  + **5-1a**[Frequency, Bandwidth, and Throughput](javascript://)
  + **5-1b**[Transmission Flaws](javascript://)
  + **5-1c**[Duplex, Half-Duplex, and Simplex](javascript://)
  + **5-1d**[Multiplexing](javascript://)
* **5-2**[Copper Cable](javascript://)
  + **5-2a**[Coaxial Cable and Twinaxial Cable](javascript://)
  + **5-2b**[Twisted-Pair Cable](javascript://)
  + **5-2c**[STP (Shielded Twisted Pair)](javascript://)
  + **5-2d**[UTP (Unshielded Twisted Pair)](javascript://)
  + **5-2e**[Comparing STP and UTP](javascript://)
  + **5-2f**[Cable Pinouts](javascript://)
  + **5-2g**[PoE (Power over Ethernet)](javascript://)
  + **5-2h**[Ethernet Standards for Twisted-Pair Cable](javascript://)
* **5-3**[Fiber-Optic Cable](javascript://)
  + **5-3a**[SMF (Single Mode Fiber)](javascript://)
  + **5-3b**[MMF (Multimode Fiber)](javascript://)
  + **5-3c**[Fiber Connectors](javascript://)
  + **5-3d**[Media Converters](javascript://)
  + **5-3e**[Fiber Transceivers](javascript://)
  + **5-3f**[Ethernet Standards for Fiber-Optic Cable](javascript://)
  + **5-3g**[Common Fiber-Cable Problems](javascript://)
* **5-4**[Cable Troubleshooting Tools](javascript://)
  + **5-4a**[Toner and Probe Kit](javascript://)
  + **5-4b**[Multimeter](javascript://)
  + **5-4c**[Cable Continuity Tester](javascript://)
  + **5-4d**[Cable Performance Tester](javascript://)
  + **5-4e**[OPM (Optical Power Meter)](javascript://)
* **5-5**[Module Review](javascript://)
  + **5-5a**[Module Summary](javascript://)
  + **5-5b**[Key Terms](javascript://)
  + **5-5c**[Review Questions](javascript://)
  + **5-5d**[Hands-On Projects](javascript://)
  + **5-5e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Explain basic data transmission concepts, including frequency, bandwidth, throughput, multiplexing, and common transmission flaws
* **2**Describe the physical characteristics of and official standards for coaxial cable, twinaxial cable, twisted-pair cable, fiber-optic cable, and their related connectors
* **3**Compare the benefits and limitations of various networking media
* **4**Select and use the appropriate tool to troubleshoot common cable problems

**On the Job**

I was asked to consult on a network problem concerning slow speeds and dead network jacks. The business was located in a building that was configured for two rental spaces with a single entrance. After entering the front door, I encountered a door to one set of offices on the right and the same on the left. Straight ahead was a door to the mechanical rooms.

When I removed the wall plates, I found that the installer had untwisted the pairs by at least one inch on all the jacks. On some of the nonfunctional wall jacks, the pairs were untwisted three inches or more and stuffed haphazardly into the wall box.

The next mystery was the single 12-port switch, which didn’t make sense because I was now able to achieve link on 19 wall sockets. This meant that it was time to start removing ceiling tiles and following wires. Fortunately, all the wires came together in a bundle that exited into the ceiling above the entryway. From there, most of the bundle turned and went toward the mechanical room, where the fiber-modem and 12-port switch were located. Unfortunately, a few of the wires went toward the other rental space. The other set of offices was not currently rented, and so was not accessible without contacting the landlord. The landlord was hesitant to give access to the other space. He insisted that the problem could not have anything to do with the wiring in that part of the building because his nephew, who was an electrician, had done all the network cabling in the building. Instead, the landlord insisted that the tenants must have messed up the wall jacks on their side.

After tracing cable after cable above the suspended ceiling, I finally found another network switch hiding on top of one of the ceiling tiles. All the cable terminations had around two inches of the pairs untwisted to make it easier to install the RJ-45 terminals.

I reconnected all the wall jacks and replaced all the terminals on the cables at the hidden switch. All the client’s wall jacks were now able to achieve link and connect, transferring at 100 Mbps full-duplex.

**Todd Fisher Wallin**

**Operations Coordinator**

**Driftless Community Radio**

Just as highways and streets provide the foundation for automobile travel, networking media provides the physical foundation for data transmission. Networking media are the physical or atmospheric paths that signals follow. The first networks used thick coaxial cables. Today’s local area networks use copper or fiber cabling or wireless transmissions. This module focuses on wired networks. Wireless networking is covered in a later module.

Networking media technologies change rapidly because networks are always evolving to meet the demand for greater speed, versatility, and reliability. Understanding the characteristics of various networking media is critical to designing and troubleshooting networks. You also need to know how data is transmitted over these various media types. This module discusses the details of data transmission and physical networking media. You’ll learn what it takes to make data transmission dependable and how to correct some common transmission problems.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 5-1Transmission Basics

### Certification

* 1.3:

Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

* 2.1:

Compare and contrast various devices, their features, and their appropriate placement on the network.

* 2.3:

Given a scenario, configure and deploy common Ethernet switching features.

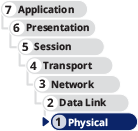
* 3.1:

Given a scenario, use the appropriate statistics and sensors to ensure network availability.

* 5.2:

Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

Average reading time: 21 minutes



The transmission techniques used on today’s networks are complex and varied. Through minor tweaks and major renovations, network administrators constantly seek ways to maximize the efficiency of their networks. In this section, you’ll first look at what measurements indicate network efficiency, and then you’ll explore obstacles to good network performance. Optimizing network performance is a more complex topic and is covered in later modules.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1aFrequency, Bandwidth, and Throughput

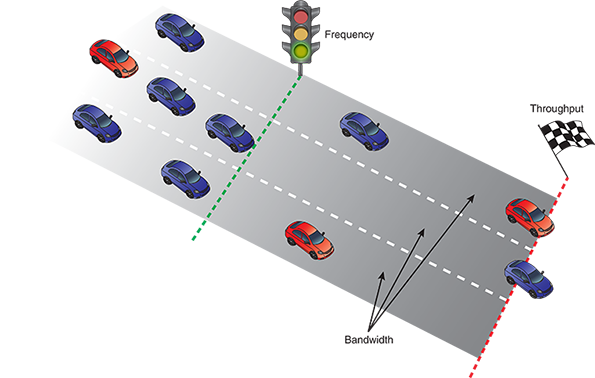
In networking and similar technologies, it’s common for one term to be used to refer to multiple concepts and principles. Often such terms are used incorrectly or inconsistently, even by corporations and professionals. As a networking professional, it’s important to understand both the technical meanings of essential terms and the more informal, common usages. These can be two very different things.

For example, the terms bandwidth and throughput are often confused. A networking professional needs to measure or make decisions based on these two transmission characteristics. People commonly think bandwidth and throughput are identical, but they are fundamentally different. To make things more complicated, the term bandwidth has additional meanings in relation to frequencies, electric circuits, radar, or other technologies. Let’s take a closer look at each of the terms needed for your work in networking, their definitions, and the various ways they’re used:

* [**Frequency**](javascript://) for today’s network cabling is typically measured in MHz (megahertz) or GHz (gigahertz), which indicates the number of times in a second that an electrical signal can change states (for example, change from a positive to a negative charge or vice versa). This is similar to the frequencies used in wireless networking, but it’s not quite the same. Wireless signals such as FM radio or Wi-Fi, where frequency is also measured in MHz or GHz, must be contained within a specific range of the electromagnetic spectrum to prevent the signal from interfering with other signals using nearby frequencies. By contrast, wired signals don’t have to be so tightly contained because the cable itself mostly limits the dispersion of the signal. Instead, a wired signal covers a wide spectrum of electromagnetic frequencies, and it’s rated for efficiency up to a specified maximum frequency. A cable’s maximum frequency is important to know because it affects how quickly you can transfer data over that cable. Imagine you are a traffic engineer overseeing traffic flowing onto a freeway via a system of green lights—one car per each green light, as shown in [Figure 5-1](javascript://). The current system flashes one green light a minute, therefore releasing one car per minute. If you want to release more cars onto the freeway in a shorter period of time, you could increase the number of green lights per minute. The number of light cycles per minute is an example of frequency. You’ll see maximum frequencies identified for different categories of copper cabling. Sometimes this maximum frequency is also called bandwidth to indicate the possible range of frequencies up to that maximum. In this case, bandwidth refers to a frequency in MHz or GHz. However, bandwidth can also refer to the transfer of data, as described next.

**Figure 5-1**

Freeway analogy for frequency, bandwidth, and throughput



Enlarge Image

* [**Bandwidth**](javascript://) for today’s networks is measured in Mbps (megabits per second) or Gbps (gigabits per second). The term refers to the amount of data you could theoretically transmit during a given period of time, taking into consideration factors such as frequency, distance, and SNR (signal-to-noise ratio). In the freeway analogy, bandwidth refers to the number of lanes on a freeway. You can increase bandwidth by adding more lanes to the freeway, which allows you to release more cars per green light—for example, three lanes on the freeway allows you to release three cars for every green light instead of just one. At the same time, consider that adding too many lanes for anticipated traffic, so that some lanes are never used, would be a waste of resources. Essentially, bandwidth refers to the number of lanes available for data transfer or, to use a different analogy, the size of the pipe through which water is pumped.
* [**Throughput**](javascript://) (also called payload rate or effective data rate) for today’s networks is also measured in Mbps (megabits per second) or Gbps (gigabits per second). The term refers to the number of data bits (0s and 1s) that are actually received across a connection each second. Throughput takes into consideration the reality of a network environment, including delays to cross interfaces, noise affecting signals, errors that result in lost data, and more. In the freeway analogy, throughput would measure the number of people who arrive at their destination per minute. This number might be different than the maximum number the freeway could possibly support and takes into account problems such as weather, traffic congestion, red lights at intersections, and different driving styles.

It helps to think of the term bandwidth as a range of possibilities, or as a definition of the maximum possible. When discussing frequencies, bandwidth identifies the full range of available frequencies (the width of the band) for a specific application. When discussing data rates, bandwidth identifies the theoretical maximum number of bits per second. You might even use bandwidth to identify how much work you can handle in a day or how much stress you can tolerate before you must make some scheduling or lifestyle changes. Be aware that many sources use these terms—frequency, bandwidth, and throughput—interchangeably in some contexts. This is why you’ll often see bandwidth measured in two ways: in MHz/GHz or in Mbps/Gbps.

At one time, the terms frequency, throughput, and bandwidth were directly related mathematically—a cable with a maximum frequency of 100 MHz could transmit a maximum of 100 Mbps: 100 MHz correlated with 100 Mbps. Today, however, additional layers of technology complicate the mathematical relationship between these measurements. For example, now you can find cables with a maximum frequency of 250 MHz rated for a maximum throughput of 1000 Mbps, which is a 400 percent increase in possible throughput.

New technologies such as modulation and encoding offer innovative methods for increasing theoretical bandwidth and effective data throughput given the same maximum frequency. For example, if you want to transport more people on a freeway during a given period of time, you can use larger vehicles like double-decker buses, which carry a lot more people per vehicle than small cars do. Using the same three lanes of traffic and the same green light frequency, you can now transport dozens more people per minute per lane of traffic. Similarly, using [**modulation**](javascript://) (sending data over an analog signal) and [**encoding**](javascript://) (converting data into a digital signal for transmission), you can pack a lot more bits of data into each signal’s state change.

Usually, a low-cost residential broadband Internet connection that is rated for a maximum bandwidth of 3 Mbps has an actual throughput that is lower than the advertised maximum, perhaps even much lower. This explains why providers often advertise “up to 3 Mbps.” For a network connection to achieve an actual throughput of 1 Gbps, it might require a transmission rate of 1.25 Gbps or more because of the overhead used by Ethernet frames, delays crossing interfaces, noise in the environment, and other factors. Applications that require significant throughput like this include videoconferencing, telephone signaling, and multimedia streaming. By contrast, instant messaging and email, for example, require much less bandwidth. [Table 5-1](javascript://) summarizes the terminology and abbreviations used when discussing different throughput rates.

**Table 5-1**

### Throughput Measures

| **Quantity** | **Prefix** | **Abbreviation** |
| --- | --- | --- |
| 1 bit per second | n/a | ‍‍ |
| 1000 bits per second | kilo | ‍‍ |
| 1,000,000 bits per second | mega | ‍‍ |
| 1,000,000,000 bits per second | giga | ‍‍ |
| 1,000,000,000,000 bits per second | tera | ‍‍ |

**Note 5-1**

Be careful not to confuse bits and bytes when discussing throughput and bandwidth:

* Data storage quantities are typically expressed in multiples of bytes.
* Data transmission quantities (in other words, throughput) are more commonly expressed in multiples of bits per second.

When representing different data quantities, a small b represents bits, while a capital B represents bytes. To put this into context, a fast Internet connection might transmit data at 1 Gbps (gigabit per second), while an SD movie file might be 1–2 GB (gigabytes) in size.

Another difference between data storage and data throughput measures is that, with data storage, the prefix kilo means 2 to the 10th power (written as ), or 1024. With data throughput, kilo means 10 to the 3rd power (written as ), or 1000. In other words, data storage measurements use powers of 2 while data throughput measurements use powers of 10.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1bTransmission Flaws

On a busy network, why is actual throughput less than the potential bandwidth of the network? Three factors that can degrade network performance are noise, attenuation, and latency.

### Noise

Noise, or interference, can degrade or distort a signal and, on a network, is measured in [**dB (decibel) loss**](javascript://). A decibel is a relative measure of signal loss (a negative number) or gain (a positive number). In other words, the loss or gain is measured as a comparison between the signal’s strength at transmission versus its strength when it arrives at its destination. The signal might get weaker due to noise (interference), or it might get stronger with help from an amplifier.

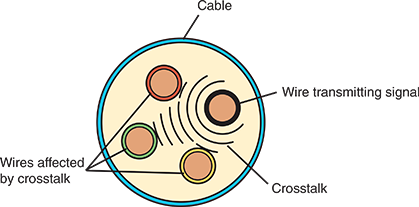
So how much power change is indicated by each dB up or down? As a general rule, a loss of 3 dB between the transmitter and receiver indicates the signal has lost half its power. But again, dB loss or gain is a relative measure. Therefore, a loss of 3 dB on a 10-watt signal means the signal arrives at 5 watts. But a loss of 3 dB on a 1000-watt signal means the signal arrives at 500 watts. A 1000-watt signal with a 6-dB loss arrives at 250 watts (half of half the original signal strength, or one quarter). That’s a big loss! You can see why noise on the network can be problematic.

Two common sources of noise are the following:

* **EMI (electromagnetic interference)**—Caused by motors, power lines, televisions, copiers, fluorescent lights, microwave ovens, manufacturing machinery, and other sources of electrical activity (including a severe thunderstorm). One type of EMI is RFI (radio frequency interference), or electromagnetic interference caused by radio waves. (Often, you’ll see EMI referred to as EMI/RFI.) Strong broadcast signals from radio or TV antennas can generate RFI.
* **Crosstalk**—Occurs when a signal traveling on one wire or cable infringes on the signal traveling over an adjacent wire or cable, as shown in [Figure 5-2](javascript://). The resulting noise, or crosstalk, is equal to a portion of the second line’s signal. If you’ve ever been on a traditional, landline phone and heard the conversation on a second line in the background, you have heard the effects of crosstalk.

**Figure 5-2**

Crosstalk between wires in a cable



In data networks, crosstalk can be extreme enough to prevent the accurate delivery of data. Three common types are the following:

* **Alien crosstalk**—Crosstalk that occurs between two cables
* **NEXT (near end crosstalk)**—Crosstalk that occurs between wire pairs near the source of a signal
* **FEXT (far end crosstalk)**—Crosstalk measured at the far end of the cable from the signal source

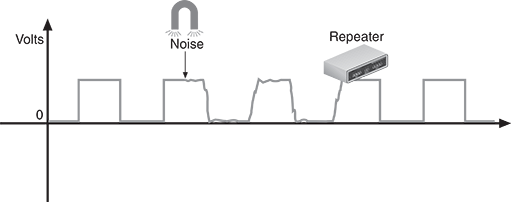
In every signal, a certain amount of noise is unavoidable. However, engineers have devised several ways to limit the potential for noise to degrade a signal. One way is simply to ensure that the strength of the signal exceeds the strength of the noise. Proper cable design and installation are also critical for protecting against noise effects.

### Attenuation

Another transmission flaw is [**attenuation**](javascript://), or the loss of a signal’s strength as it travels away from its source. Just as your voice becomes fainter as it travels farther, so do signals fade with distance. To compensate for attenuation, signals are boosted en route using a [**repeater**](javascript://), which regenerates a digital signal in its original form without the noise it might have previously accumulated. [Figure 5-3](javascript://) shows a digital signal distorted by noise and then regenerated by a repeater. A switch on an Ethernet network works as a multiport repeater, as the bits transmitted “start over” at each port on the switch.

**Figure 5-3**

A digital signal distorted by noise and then repeated



### Latency

Although electrons travel rapidly, they still must travel, and a brief delay takes place between the instant when data leaves the source and when it arrives at its destination. This delay is called [**latency**](javascript://).

The length of the cable affects latency, as does the existence of any intervening connectivity device, such as a router. Different devices affect latency to different degrees. For example, modems convert, or modulate, both incoming and outgoing signals for transmission over a network. Thus, they increase a connection’s latency far more than switches, which simply repeat a signal. Other factors can also increase latency, such as cable limitations, number of transfers between devices, noise in the network, traffic congestion overwhelming network devices, processing delays (such as analysis by intervening firewalls or DNS resolution), collisions with other messages, and conversion from one type of transmission to another (such as converting from wired to wireless transmission). The most common way to measure latency on data networks is by calculating a packet’s [**RTT (round trip time)**](javascript://), or the length of time it takes for a packet to go from sender to receiver and then back from receiver to sender. RTT is usually measured in milliseconds.

Latency causes problems when a receiving node is expecting some type of communication, such as the rest of a data stream it has begun to accept. If packets experience varying amounts of delay, they can arrive out of order—a problem commonly called [**jitter**](javascript://), or more precisely, PDV (packet delay variation). This might cause streaming video or voice transmissions to pause repeatedly, jump around, or stall out completely. Another latency-related problem occurs if the node does not receive the rest of the data stream within a given time, and it, therefore, assumes no more data is coming. In this case, transmission errors are returned to the sender.

While noise, attenuation, and latency degrade a network’s efficiency, there are some changes you can make to the network to increase efficiency. First, let’s consider settings on a device’s NIC.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1cDuplex, Half-Duplex, and Simplex

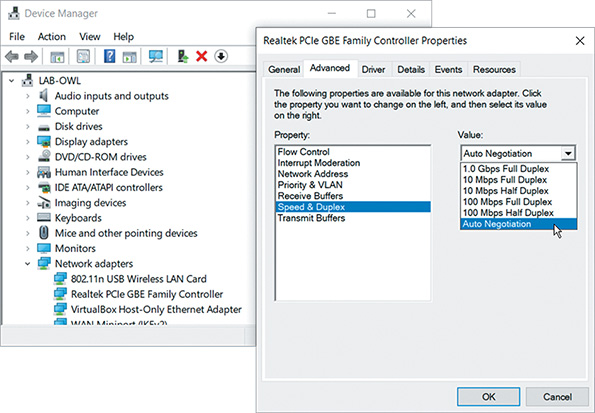
Network connections perform best when network devices are properly configured. Two important NIC settings include the direction in which signals travel over the media and the number of signals that can traverse the media at any given time. These two settings are combined to create different methods of communication as follows:

* [**Full-duplex**](javascript://), also called [**duplex**](javascript://)—Signals are free to travel in both directions over a medium simultaneously. As an analogy, talking on the telephone is a full-duplex transmission because both parties in the conversation can speak at the same time. Modern NICs use a full-duplex configuration by default.
* **Half-duplex**—Signals may travel in both directions over a medium but in only one direction at a time. For example, an apartment building’s intercom system might be half-duplex if only one person can speak at a time.
* **Simplex**—Signals may travel in only one direction, and this is sometimes called one-way, or unidirectional, communication. Broadcast radio and garage door openers are examples of simplex transmissions.

In Windows, you can use Device Manager to configure a NIC, including speed and duplex settings. For example, notice in [Figure 5-4](javascript://) that you can choose Full Duplex, Half Duplex, or Auto Negotiation, which allows the NIC to select the best link speed and duplex that is also supported by a neighboring device. However, if you specify a particular speed and duplex that’s not supported by the neighboring device, the result is a [**speed and duplex mismatch**](javascript://) and, therefore, slow or failed transmission.

**Figure 5-4**

A network adapter’s Speed & Duplex configuration can be changed



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1dMultiplexing

Duplexing allows a signal to travel in both directions in a cable at one time. This might be achieved by pairing two wires together inside the cable, where one wire transmits and the other receives. Or it might be accomplished by transmitting two or more signals on the same wire. A form of transmission that allows multiple signals to travel simultaneously over one medium is known as [**multiplexing**](javascript://).

Networks rely on multiplexing to increase the amount of data that can be transmitted in a given timespan over a given bandwidth. To carry multiple signals, the medium’s channel is logically separated into multiple smaller channels, or subchannels. Many different types of multiplexing are available, and the type used in a situation depends on what the media, transmission, and reception equipment can handle. For each type of multiplexing, a device that can combine many signals on a channel, a multiplexer (mux), is required at the transmitting end of the channel. At the receiving end, a demultiplexer (demux) separates the combined signals.

Different types of multiplexing manipulate signals in different ways. Three common types of multiplexing used on copper lines are the following:

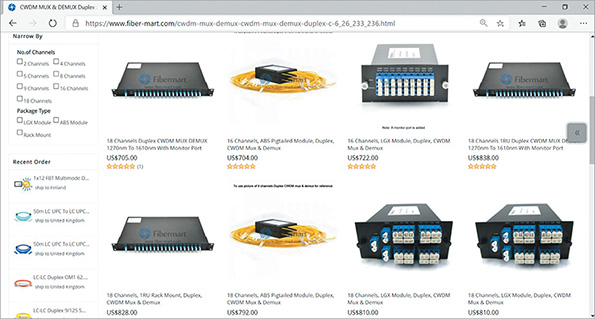
* [**TDM (time division multiplexing)**](javascript://)—Divides a channel into multiple intervals of time, or time slots. Time slots are reserved for their designated nodes regardless of whether the node has data to transmit. This can be inefficient if some nodes on the network rarely send data.
* [**STDM (statistical time division multiplexing)**](javascript://)—Assigns time slots to nodes (similar to TDM), but it then adjusts these slots according to priority and need. This approach uses all slots rather than leaving some unused, which provides improved efficiency in using available bandwidth on a network. Still, neither TDM nor STDM allows multiple signals on a line at the exact same time.
* [**FDM (frequency division multiplexing)**](javascript://)—Assigns different frequencies to create multiple frequency bands, each used by a subchannel, so that multiple signals can transmit on the line at one time. Signals are modulated into different frequencies, then multiplexed to simultaneously travel over a single channel, and demultiplexed at the other end. Telephone companies once used FDM for all phone lines and still multiplex signals on residential phone lines for the last leg before entering a residence. (The last leg is sometimes referred to as the last mile even though it’s not necessarily a mile long.)

Three types of multiplexing technologies used with fiber-optic cable include the following:

* [**WDM (wavelength division multiplexing)**](javascript://)—Works with any fiber-optic cable to carry multiple light signals simultaneously by dividing a light beam into different wavelengths, or colors, on a single fiber. The technology works similar to how a prism spreads white light into various colors. Original WDM provided only two wavelengths or channels per strand of fiber in only one direction at a time. Newer [**bidirectional WDM**](javascript://) supports full-duplex light transmissions in both directions at the same time.
* [**DWDM (dense wavelength division multiplexing or dense WDM)**](javascript://)—Increases the number of channels provided by normal WDM to between 80 and 320 channels. Dense WDM can be amplified en route and is typically used on high-bandwidth or long-distance WAN links, such as the connection between a large ISP and its (even larger) NSP (network service provider).
* [**CWDM (coarse wavelength division multiplexing or coarse WDM)**](javascript://)—Lowers cost by spacing frequency bands wider apart to allow for cheaper transceiver equipment. CWDM multiplexers typically can support several channels per fiber, such as 4, 8, 16, or 18, as you can see on this manufacturer’s website in [Figure 5-5](javascript://). The effective distance of CWDM is more limited because the signal is not amplified.

**Figure 5-5**

CWDM multiplexers available in 16-channel, 18-channel, and other varieties



Enlarge Image

Source: [Fiber-MART.com](http://fiber-mart.com/" \t "_blank)

Monitoring and optimizing network performance is a substantial part of network administration. You’ll revisit this topic more extensively later.

**Remember This…**

* Compare frequency, bandwidth, and throughput.
* Describe how to minimize noise, attenuation, and latency problems.
* Configure speed and duplex settings on a NIC.
* Explain how WDM, bidirectional WDM, DWDM, and CWDM work.

**Self-Check**

1. When you measure the amount of data coming into your home network, what metric are you identifying?

Answer

* 1. Duplex
  2. Bandwidth
  3. Noise
  4. Throughput

1. Which of the following improves overall network performance?

Answer

* 1. Jitter
  2. Multiplexing
  3. Attenuation
  4. Latency

**You’re Ready**

You’re now ready to complete [Project 5-1: Latency around the World](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 5-2Copper Cable

### Certification

* 1.3:

Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

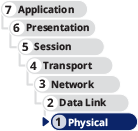
* 2.3:

Given a scenario, configure and deploy common Ethernet switching features.

* 5.2:

Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

Average reading time: 44 minutes



Now that you understand some of the basics of data transmission on a network, you’re ready to learn about different types of transmission media. Let’s begin with a relatively simple cable type, coaxial cable, and then you’ll explore how newer media improve upon this older technology.

### Exam Tip

The CompTIA Network+ exam expects you to know the characteristics and limitations of each type of media covered here, how to install and design a network with each type, how to troubleshoot networking media problems, and how to provide for future network growth with each option.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2aCoaxial Cable and Twinaxial Cable

Coaxial cable and twinaxial cable are good examples of how solid technology continues to find its niche in modern networks even as the network itself transforms through the years. Let’s look at what role each of these cable types plays in a modern network.

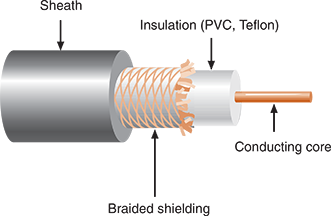
### Coaxial Cable

[**Coaxial cable**](javascript://), called “coax” for short, was the foundation for Ethernet networks in the 1980s. You’ll most likely never see a coaxial cable network for computers, as coax has been replaced by newer media types; however, a form of coax is still used for cable Internet, cable TV, and some multimedia connection types.

Coaxial cable has a central metal core (often copper) surrounded by an insulator, a braided metal shielding, and an outer cover, called the sheath or jacket (see [Figure 5-6](javascript://)). The core can have a solid metal wire or several thin strands of metal wire and carries the electromagnetic signal. The shielding protects the signal against noise and is a ground for the signal. The plastic insulator can be PVC (polyvinyl chloride) or Teflon and protects the core from the metal shielding because if the two made contact, the wire would short-circuit. The sheath protects the cable from physical damage and might be PVC or a more expensive fire-resistant plastic.

**Figure 5-6**

Coaxial cable



Coaxial cabling comes in hundreds of specifications, which are all assigned an RG specification number. RG stands for radio guide, which is appropriate because coaxial cabling can be used by radio frequencies in broadband transmission. The RG ratings measure the materials used for shielding and conducting cores, which in turn influence their transmission characteristics, such as attenuation, throughput, and [**impedance**](javascript://) (a measure of the opposition to a current’s flow through a cable, as expressed in ohms).

Each type of coax is suited to a different purpose. A cable’s AWG (American Wire Gauge) refers inversely to the size of the conducting core. In other words, the larger the AWG, the smaller the diameter of the core wire. Coax cable is also categorized according to its impedance rating, meaning, its efficiency at transferring power and data over a distance. Lower impedance results in better power transfer, and higher impedance yields less attenuation of the data signal over a distance. An impedance of 50 ohms was determined to be a good compromise in these factors for computer networks and CB (citizens band) or ham radio connections where the effectiveness of the cable is more focused on a device’s ability to transmit a signal. In contrast, 75 ohms better sustains the strength of a signal and, therefore, yields better performance for receiving devices, such as satellite and cable TV receiver boxes, televisions, radio receivers, police scanners, and audio connections in a home theater system. [Table 5-2](javascript://) lists the two most common coaxial cable specifications still in use today.

**Table 5-2**

### Coaxial Cable Specifications

| **Type** | **Impedance** | **Core** | **Uses** |
| --- | --- | --- | --- |
| RG-59 | 50 ohms or  75 ohms | 20 or 22 AWG core, usually made of braided copper | Still used for relatively short connections, for example, when distributing video signals from a central receiver to multiple monitors within a building.  RG-59 is less expensive than the more common RG-6 but suffers from greater attenuation. |
| [**RG-6**](javascript://) | 50 ohms or  75 ohms | 18 AWG conducting core, usually made of solid copper | Used to deliver broadband cable Internet service and cable TV, particularly in the last stretch to the consumer’s location; also widely used for inexpensive cabling in AV systems. Cable Internet service entering a home is RG-6. |

### Exam Tip

The CompTIA Network+ exam expects you to know about RG-6 cables and F-connectors.

These two coaxial cable types, RG-6 and RG-59, can terminate with one of two connector types:

* An [**F-connector**](javascript://) attaches to coaxial cable so that the core in the center of the cable extends into the center of the connector. After being attached to the cable by crimping or compression, connectors are threaded and screwed together like a nut-and-bolt assembly. A male F-connector, or plug, attached to coax is shown in [Figure 5-7](javascript://). A corresponding female F-connector, or jack, would be coupled with the male connector. F-connectors are most often used with RG-6 cables.

**Figure 5-7**

F-connector



Source: MCM Electronics, Inc

* A [**BNC connector**](javascript://) is crimped, compressed, or twisted onto a coaxial cable. BNC stands for Bayonet Neill-Concelman, a term that refers to both an older style of connection and its two inventors. (Sometimes the term British Naval Connector is also used.) A BNC connector connects to another BNC connector via a turn-and-lock mechanism—this is the bayonet coupling referenced in its name. Unlike an F-connector, a male BNC connector provides its own conducting pin. BNC connectors are used with RG-59 coaxial cables, and less commonly, with RG-6. [Figure 5-8](javascript://) shows a BNC connector.

**Figure 5-8**

BNC connector



Igor Smichkov/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

**Note 5-2**

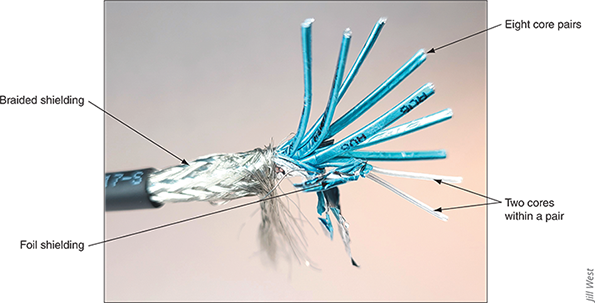
When sourcing connectors for coaxial cable, you need to specify the type of cable you are using. For instance, when working with RG-6 coax, choose an F-connector made specifically for RG-6 cables. That way, you’ll be certain that the connectors and cable share the same impedance rating. If impedance ratings don’t match, data errors will occur and transmission performance will suffer.

### Twinaxial Cable

[**Twinaxial cable**](javascript://), called “twinax” for short, looks very similar to coax cable except that there are two cores, or conductors, inside the cable. The two cores cooperate in a half-duplex fashion to transmit data, and so twinax is capable of supporting much higher throughput than coax. More recent twinax cables contain multiple pairs of these cores to carry even more data (see [Figure 5-9](javascript://)). In fact, given the right circumstances, twinax might be a better choice than fiber to carry 10-Gigabit signals or higher over very short distances. This makes twinax an inexpensive option for short, high-speed connections, such as when connecting switches to routers or servers in a data center. For this reason, twinax is also called a DAC (direct attach copper) cable, which is a copper cable designed to handle very high-speed connections at very short distances. While limited in distance, installing twinax is significantly cheaper than installing fiber, consumes less power, and provides excellent protection from possible sources of interference. Because it’s made from 26 or 28 AWG copper, twinax is also particularly resistant to damage from rough handling.

**Figure 5-9**

Twinax cable contains two cores in each pair



Enlarge Image

Jill West

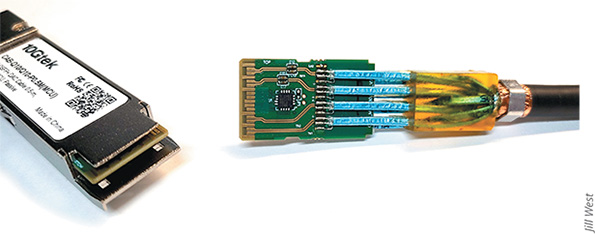
The type of twinax cable determines its maximum supported distances, as described next:

* **Passive**—Does not contain internal electrical components and is sufficient for the shortest distances of less than about 5 or 7 meters.
* **Active**—Contains internal electrical components to strengthen signals over slightly longer distances, up to 10 meters.

Twinax is factory terminated (see [Figure 5-10](javascript://)), usually with some of the same kinds of modular transceivers as what fiber terminations use, which you’ll learn more about later in this module. This means twinax cable lengths are fixed with a preinstalled transceiver on each end. Depending on the connector type, twinax can support throughput up to 100 Gbps. However, the higher data rates require even shorter distance limitations.

**Figure 5-10**

Twinax cable is factory terminated with transceivers; each core pair is welded to a circuit board inside the transceiver



Enlarge Image

Jill West

Next, you’ll learn about a medium you’re more likely to find throughout a modern computer network: twisted-pair cable.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2bTwisted-Pair Cable

[**Twisted-pair**](javascript://) cable consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm (approximately the diameter of a sewing pin). Every two wires are twisted around each other to form pairs, and all the pairs are encased in a plastic sheath, as shown in [Figure 5-11](javascript://).

**Figure 5-11**

Twisted-pair cable



**Note 5-3**

The terms wire and cable are often used synonymously. Strictly speaking, wire is a subset of cabling because the cabling category also includes fiber-optic cable, which is almost never called wire. The exact meaning of the term wire depends on context. For example, if you said, in a somewhat casual way, “We had 6 gigs of data go over the wire last night,” you would be referring to whatever transmission media helped carry the data—whether fiber cable, radio waves, or copper cable.

Twisted-pair cabling in Ethernet networks contains four wire pairs. On [**Fast Ethernet**](javascript://) networks, which have a maximum data rate of 100 Mbps, one pair sends data, another pair receives data, and the other two pairs are not used for data transmission. Networks using [**Gigabit Ethernet**](javascript://) and higher standards, with a data rate of 1000 Mbps or more, use all four pairs for both sending and receiving. You’ll learn more about Ethernet standards later in this module.

**Note 5-4**

The more twists per foot in a pair of wires, the more resistant the pair will be to crosstalk or noise. Higher-quality, more-expensive twisted-pair cable contains more twists per foot. The number of twists per meter or foot is known as the [**twist ratio**](javascript://). Because twisting the wire pairs more tightly requires more cable, however, a high twist ratio can result in greater attenuation. For optimal performance, cable manufacturers must strike a balance between minimizing crosstalk and reducing attenuation. Interestingly, there are no imposed standards for twist ratio. What matters in qualifying a manufacturer’s cable for a particular standard is its effective throughput (no matter how that effect is achieved), not specifically the number of twists in the wires.

In 1991, the TIA/EIA organizations finalized their specifications for twisted-pair wiring in a standard called “TIA/EIA-568.” The TIA/EIA 568 standard divides twisted-pair wiring into several categories. The categories you might see on a computer network are Cat (category) 3, 5, 5e, 6, 6a, 7, 7a, and 8, all of which are described in [Table 5-3](javascript://). (Cat 4 cabling exists, too, but it is rarely used.) Modern LANs use Cat 5e or higher wiring, which is the minimum required to support Gigabit Ethernet. Cat 6 and above are certified for multigigabit transmissions, although Cat 6 cable has shorter distance limitations when supporting 10 Gbps. While Cat 7/7a cables never gained significant popularity, Cat 8 cables are already widely available even for home networks.

**Table 5-3**

### Twisted-Pair Cabling Standards

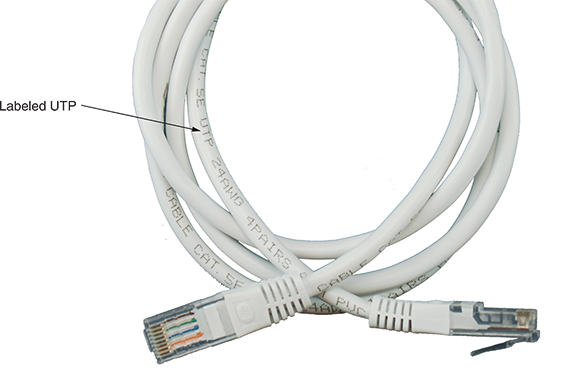
| **Standard** | **Maximum supported bandwidth** | **Maximum rated frequency** | **Description** |
| --- | --- | --- | --- |
| Cat 3 (Category 3) | 10 Mbps | Up to 16 MHz | Used more commonly for wired telephone connections and should never be used for a modern computer network. |
| [**Cat 5 (Category 5)**](javascript://) | 100 Mbps  (Fast Ethernet) | 100 MHz | Required minimum standard for Fast Ethernet. |
| [**Cat 5e (Enhanced Category 5)**](javascript://) | 1000 Mbps  (1 Gbps, Gigabit Ethernet) | 350 MHz | A higher-grade version of Cat 5 wiring that contains high-quality copper, offers a higher twist ratio, and uses slightly more advanced methods for reducing crosstalk. |
| [**Cat 6 (Category 6)**](javascript://) | 1 Gbps or, at shorter distances, 10 Gbps | 250 MHz | Includes a plastic core to prevent crosstalk between twisted pairs in the cable. Can also contain foil insulation covering each bundle of wire pairs and a fire-resistant plastic sheath. |
| [**Cat 6a (Augmented Category 6)**](javascript://) | 10 Gbps | 500 MHz | Reduces attenuation and crosstalk and allows for potentially exceeding traditional network segment length limits. Can reliably transmit data at multigigabit per second rates.  Backward-compatible with Cat 5, Cat 5e, and Cat 6 cabling, which means that it can replace lower-level cabling without requiring connector or equipment changes. |
| [**Cat 7 (Category 7)**](javascript://) Not included in TIA/EIA standards | 10 Gbps or, at shorter distances, up to 100 Gbps | 600 MHz | Supports higher frequencies because each wire pair is wrapped in its own shielding, then packaged in additional shielding beneath the sheath.  To reach its fullest potential, it requires more sophisticated connectors, either GG45, which is backward-compatible with RJ-45, or TERA, which is not. It’s thicker and less flexible than earlier versions and is also less common. |
| [**Cat 7a (Augmented Category 7)**](javascript://) Not included in TIA/EIA standards | 40–100 Gbps at very short distances | 1000 MHz | Uses increased bandwidth to offer higher data rates than Cat 7 but still requires specialized connectors to reach full potential. |
| [**Cat 8 (Category 8)**](javascript://)  Class I (Cat 8.1) and  Class II (Cat 8.2) | 25 Gbps and 40 Gbps at longer distances than Cat 7 | 2 GHz | Already widely available for purchase by consumers for home networks. Relies on further improved and extensive shielding. Optimized for short-distance backbone connections within the data center and supports up to 40 Gbps over 30 meters (98 feet), which rivals fiber-optic cables at these distances. Cat 8 Class I offers the advantage of using connectors that are backward-compatible with Cat 5e and Cat 6 standards, which reduces the cost and complexity of installation. Cat 8 Class II cables are backward-compatible with Cat 7/7a specialty connectors. |

Enlarge Table

In [Figure 5-12](javascript://), notice the reference on the cable to UTP. All twisted-pair cable falls into one of two classifications: STP (shielded twisted pair) or UTP (unshielded twisted pair). Let’s look at characteristics of each type.

**Figure 5-12**

A Cat 5e data cable



**Note 5-5**

To identify the category of a twisted-pair cable, check for information stamped on the jacket, as shown in [Figure 5-12](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2cSTP (Shielded Twisted Pair)

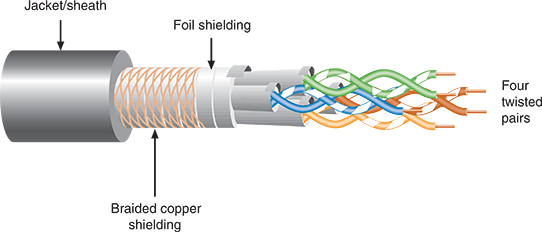
Recall that STP (shielded twisted pair) cable consists of twisted-pair wires that are not only individually insulated but might also be surrounded by a shielding made of a metallic substance such as a foil. Some STP cables use a braided copper shielding. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. It also contains the electrical energy of the signals inside. The shielding must be grounded to enhance its protective effects and prevent reflection issues. The effectiveness of STP’s shield depends on these characteristics:

* Level and type of environmental noise
* Thickness and material used for the shield
* Grounding mechanism
* Symmetry and consistency of the shielding

[Figure 5-13](javascript://) depicts an STP cable.

**Figure 5-13**

depicts an STP cable.



Newer types of cables, such as Cat 8, incorporate more sophisticated shielding materials, more tightly twisted wires, and higher bandwidths to offer data rates rivaling fiber-optic cable at short distances. [Figure 5-14](javascript://) shows a consumer-grade Cat 8 cable cut open so you can see the layers of shielding. Notice the braided shielding under the jacket, the foil shielding around all four twisted pairs, and the individual foil shielding around each twisted pair.

**Figure 5-14**

The insides of a Cat 8 cable



Go to pg.

[**help**](javascript://)

Application Opened

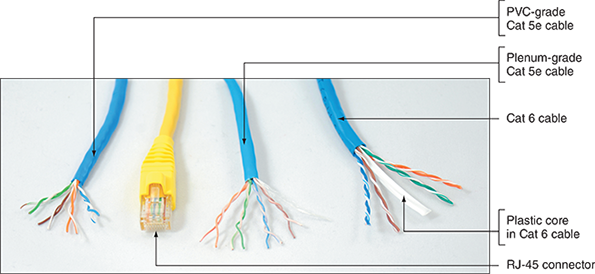
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2dUTP (Unshielded Twisted Pair)

UTP cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP. Historically, UTP was more popular than STP due to its lower price. However, modern cable prices have dropped low enough that it might only cost a few pennies more per foot for high quality shielding. [Figure 5-15](javascript://) depicts three types of UTP cable: PVC-grade Cat 5e, plenum-grade Cat 5e, Cat 6 with its plastic core, and a UTP cable with an RJ-45 connector attached. Recall that a plenum-grade cable’s jacket is flame-resistant, while the PVC cable’s coating is toxic when burned.

**Figure 5-15**

Various UTP cables and RJ-45 connector



Enlarge Image

**Note 5-6**

More specifically, [**plenum-grade cable**](javascript://) is designed to withstand high temperatures, such as would be experienced in an attic space; it offers a highly fire-retardant jacket to reduce the spread of flames in areas with air circulation; and it burns with less smoke that is nontoxic. A similar cable type, [**riser-rated cable**](javascript://), is also coated with a fire-retardant jacket and is a thicker cable to make it easier to push or pull through risers in buildings or between floors. A riser is a vertical space in a building that is not designed for managing airflow, such as elevators, pipes, conduits, or ducts intended for pipes and cables. These are two similar cable types that are best suited to different circumstances.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

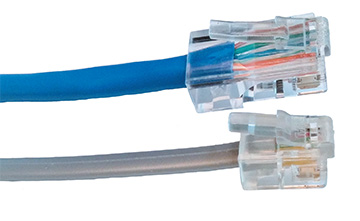
## 5-2eComparing STP and UTP

STP and UTP share several characteristics. The following list highlights their similarities and differences:

* **Throughput**—STP and UTP can both transmit data at 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps, depending on the grade of cabling and the transmission method in use. Only STP can transmit at rates faster than 10 Gbps. Note that the speed of the signal crossing the cable isn’t the point. Electrical signals travel at a speed supported by the conductor material, such as copper, and can approach the speed of light. However, shielding, data transmission methods, signal frequencies, number of wires used, errors, and other factors can affect the rate of data transfer across a cable’s length. This characteristic might be referred to as bandwidth, throughput, data rate, bit rate, data transfer speed, or simply “speed.”
* **Cost**—STP and UTP vary in cost, depending on the grade of copper used, the category rating, and any enhancements. Typically, STP is more expensive than UTP because it contains more materials. It also requires grounding, which can lead to more expensive installation. High-grade UTP can be expensive, too, however.
* **Connector**—STP and UTP use [**RJ-45 (registered jack 45)**](javascript://) modular connectors and data jacks, which look similar to analog telephone connectors and jacks, only larger. However, telephone connections follow the [**RJ-11 (registered jack 11)**](javascript://) standard. [Figure 5-16](javascript://) shows a close-up of an RJ-45 connector for a cable containing four wire pairs. For comparison, this figure also shows a traditional RJ-11 phone line connector. Most types of Ethernet that rely on twisted-pair cabling use RJ-45 connectors.

**Figure 5-16**

RJ-45 and RJ-11 connectors



* **Noise immunity**—Because of its shielding, STP is more noise resistant than UTP. On the other hand, noise on UTP cable can be reduced with filtering and balancing techniques.
* **Size and scalability**—The maximum segment length for both STP and UTP is 100 meters, or 328 feet, on Ethernet networks that support data rates from 1 Mbps to 10 Gbps. Some categories of STP require shorter segment lengths to achieve maximum throughput.

Go to pg.

[**help**](javascript://)

Application Opened

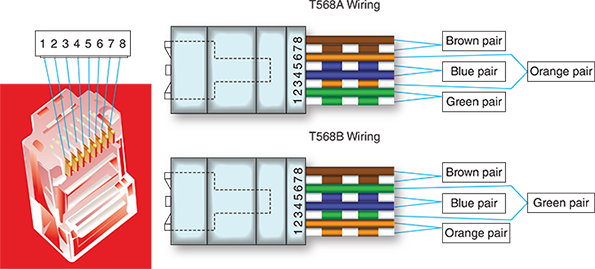
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2fCable Pinouts

Proper cable termination is a basic requirement for two nodes on a network to communicate. Poor terminations, as you read in the [On the Job](javascript://) story at the beginning of this module, can lead to power loss or noise—and consequently, errors—in a signal. Closely following termination standards is critical.

TIA/EIA has specified two methods of inserting twisted-pair wires into RJ-45 plugs: [**TIA/EIA-568A**](javascript://) and [**TIA/EIA-568B**](javascript://) (also known as T568A and T568B, respectively). Functionally, there is very little difference between these two standards. You only must be certain that you use the same standard on every RJ-45 plug and jack on your network so data is transmitted and received correctly. T568B is more common and is likely what you’ll find on home and business networks. However, the federal government requires T568A on all federal contracts for backward-compatibility.

[Figure 5-17](javascript://) depicts pin numbers and assignments (called [**pinouts**](javascript://)) for both standards. Tx refers to transmit, and Rx refers to receive. Standard pinouts are designed with the avoidance of crosstalk in mind.



Enlarge Image

**Figure 5-17**

*T568A and T568B standard terminations for Fast Ethernet and Gigabit Ethernet*

| **Pin #** | **T568A Color** | **T568B Color** | **Fast Ethernet function** | **Gigabit Ethernet function** |
| --- | --- | --- | --- | --- |
| 1 | White/green | White/orange | Tx+ | Bidirectional+ |
| 2 | Green | Orange | Tx− | Bidirectional− |
| 3 | White/orange | White/green | Rx+ | Bidirectional+ |
| 4 | Blue | Blue | Unused | Bidirectional+ |
| 5 | White/blue | White/blue | Unused | Bidirectional− |
| 6 | Orange | Green | Rx− | Bidirectional− |
| 7 | White/brown | White/brown | Unused | Bidirectional+ |
| 8 | Brown | Brown | Unused | Bidirectional− |

With Fast Ethernet, only the orange and green pairs are used: One pair transmits and one pair receives. The difference between pinouts in T568A and T568B is that these two pairs are reversed. For Gigabit Ethernet, all four pairs are used for transmitting and receiving. This more efficient use of wires helps account for the higher bandwidth of Gigabit connections.

The most common type of networking cable is a [**straight-through cable**](javascript://), also called a [**patch cable**](javascript://). To create one, terminate the RJ-45 plugs at both ends of the cable identically, following one of the TIA/EIA-568 standards. It’s called a straight-through cable because it allows signals to pass “straight through” from one end to the other.

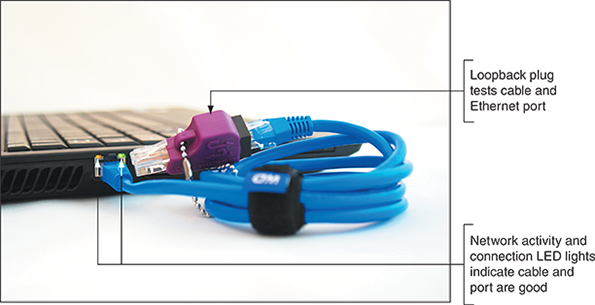
These straight-through cables are designed for most connections you’ll need in a network, such as connecting a workstation to a switch or a switch to a router. Computers and routers are intended to send and receive signals on the wires as identified in [Figure 5-17](javascript://); this port configuration is called [**MDI (medium dependent interface)**](javascript://). In contrast, switches use an alternate port configuration called [**MDI-X (MDI crossover)**](javascript://), which ensures that switches are listening on the MDI transmit wires and transmitting on the MDI receive wires. For typical network connections, this works well—most workstations and servers connect to switches, and most switches connect to routers. However, to connect like devices (MDI to MDI or MDI-X to MDI-X) requires a different kind of cable called a crossover cable, which you’ll learn about shortly. Newer devices, however, typically have [**auto-MDI-X**](javascript://) ports, which automatically negotiate the transmit and receive wires between devices, even if you’re not using the correct cable for the application. While using the wrong cable can still cause problems or increased crosstalk, the connection will work.

**Note 5-7**

A [**loopback adapter**](javascript://) attaches to a port, such as an RJ-45 port, or a cable connector. It crosses the transmit line with the receive line to create a closed loop, tricking a host into thinking it’s connected to a network as it “hears” its own data transmission. This is one way to test a port or cable for connectivity. See [Figure 5-18](javascript://). Inserting a loopback plug directly into a port will test for a bad port. Inserting a cable connector into a loopback jack will additionally test the cable for continuity (but not performance).

**Figure 5-18**

A loopback plug verifies the cable and network port are good



Enlarge Image

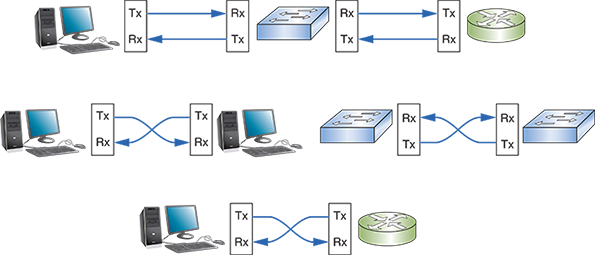
You’ll create your own loopback plug and jack in projects at the end of this module.

### Legacy Networking: Crossover Cable

With older networking devices that did not support Gigabit Ethernet, each wire could only be used to either transmit or receive, not both. A straight-through cable was always used to connect two unlike devices—for example, to connect a server transmitting on the wire a switch received on, or a switch transmitting on the wire a router received on. When you needed to connect two like devices (for example, a switch to a switch), a problem occurred because the two switches were both transmitting on the same wire and both listening to receive on the same wire. The solution was to use a crossover cable. A [**crossover cable**](javascript://) has the transmit and receive wires reversed and was used to connect a computer to a computer or a switch to a switch. See [Figure 5-19](javascript://). Notice in the figure a crossover cable was also needed to connect a computer to a router because legacy routers are expected to connect only to switches. As you read earlier, modern devices have an autosense function that enables them to detect the way wires are terminated in a plug and then adapt their transmit and receive signaling accordingly. This means crossover cables are now largely obsolete, except when they are needed to support older devices.

**Figure 5-19**

On legacy networks, straight-through cables connect unlike devices and crossover cables connect like devices

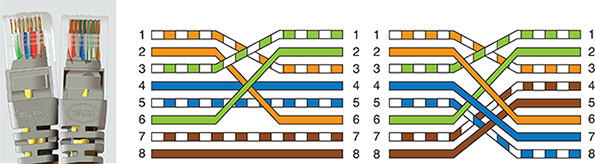


Enlarge Image

In a straight-through cable, each wire connects to the same pin on each end. For example, the orange/white wire goes straight through from pin 1 to pin 1. In a crossover cable, the transmit and receive wires are reversed, as shown in [Figure 5-20](javascript://). The diagram on the left in [Figure 5-20](javascript://) has the orange and green pairs reversed and will work with Fast Ethernet because this Ethernet standard requires only two pairs. The diagram on the right in [Figure 5-20](javascript://) has all four pairs reversed (blue, orange, green, and brown pairs) and will work with Gigabit Ethernet because Gigabit Ethernet transmits on four pairs. (However, Gigabit Ethernet devices almost never need a crossover cable.)

**Figure 5-20**

Two crossed pairs in a crossover cable are compatible with Fast Ethernet; four crossed pairs are compatible with Gigabit Ethernet



Enlarge Image

### Exam Tip

One potential cause of NEXT (near end crosstalk) is an improper termination—for example, one in which wire insulation has been damaged, where wire pairs have been untwisted too far, or where straight-through or crossover standards have been mismatched on older devices. This last problem can happen when the TX (transmission) and RX (receive) wires are crossed, which, on the CompTIA Network+ exam, is called a [**TX/RX reverse**](javascript://).

### Rollover Cable

Whereas a crossover cable reverses the transmit and receive wire pairs, a rollover cable reverses all the wires without regard to how they are paired. With a rollover cable, it’s as if the cable terminations are a mirror image of each other, as shown in [Figure 5-21](javascript://). [**Rollover cables**](javascript://), also called [**console cables**](javascript://), are used to connect a computer to the console port of a router. Routers generally have two different kinds of ports: Ethernet ports and the console port. Ethernet ports allow for network communications and are the type of port used to create LANs through the router. A router’s console port is used to communicate with the router itself, such as when making configuration changes to the device.

**Figure 5-21**

RJ-45 terminations on a rollover cable



Enlarge Image

### Exam Tip

The CompTIA Network+ exam expects you to be able to choose the correct cable type (straight-through, crossover, rollover, or console) for a given cable application.

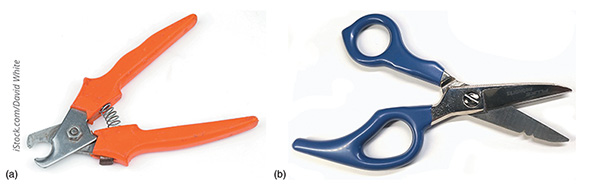
**Applying Concepts 5-1**

### Terminate Twisted-Pair Cable

It’s likely that at some point in your career, you will have to replace an RJ-45 connector on an existing cable, such as when a wire inside the cable is damaged or if pins in the connector are bent. This section describes how to terminate twisted-pair cable. The tools you’ll need—a wire cutter or snips, cable stripper, and cable crimper—are pictured in [Figures 5-22](javascript://), [5-23](javascript://), and [5-24](javascript://), respectively. Alternatively, you can use a single device that contains all three of these tools. A [**wire cutter**](javascript://) is a pliers-shaped tool, and [**snips**](javascript://) are more like heavy-duty scissors; both can make a clean cut through a cable. A [**cable stripper**](javascript://) pulls off the protective covering without damaging the wires inside. A [**cable crimper**](javascript://) pushes on the pins inside an RJ-45 connector so they pierce the wire’s insulation, thus creating contact between the two conductors. You’ll also need an RJ-45 connector, which might come with a boot. A boot is a plastic cover to protect the wires where they enter the connector.

**Figure 5-22**

(a) Wire cutter and (b) snips



Enlarge Image

[iStock.com](http://istock.com/" \t "_blank)/David White

**Figure 5-23**

Cable stripper



Francesco Ocello/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

**Figure 5-24**

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



Enlarge Image

Following are the steps to create a straight-through patch cable using Cat 5e twisted-pair cabling. To create a crossover cable or rollover cable, you would simply reorder the wires in [Step 4](javascript://) to match [Figure 5-20](javascript://) or [Figure 5-21](javascript://), respectively. The process of fixing wires inside the connector is called crimping, and it is a skill that requires practice—so don’t be discouraged if the first cable you create doesn’t reliably transmit and receive data. You’ll get more practice terminating cables in two Hands-On projects at the end of this module. To create a straight-through patch cable using Cat 5e twisted-pair cabling, complete the following steps:

1. 1

Using the wire cutter or snips, make a clean cut at both ends of the twisted-pair cable. Cut the cable the length you want the final cable to be, plus a few extra inches. If you’re using a boot, slide one onto each end of the cable with the smaller opening facing the length of the cable and the larger opening facing the cut end that you’re terminating.

1. 2

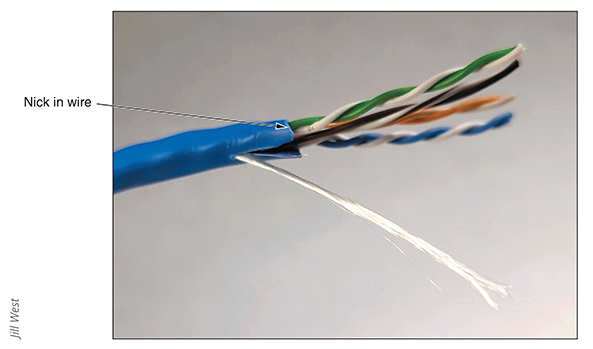
Using the cable stripper, remove the sheath off one end of the twisted-pair cable, beginning at approximately 1 inch from the end. This is easier if you first score the sheath with a pair of scissors or a small knife. Be careful to neither damage nor remove the insulation that’s on the twisted-pair wires inside.

1. 3

In addition to the four wire pairs, inside the sheath you’ll find a string. This string, known as a rip cord, is included to make it possible to remove an additional length of the outer sheath beyond the point where your cutting tool might have nicked the wire pairs. Use a pocketknife, cable cutters, or snips to start a new cut at the edge of the sheath and then pull the string through the cut to expose an additional inch of the inner wires, as shown in [Figure 5-25](javascript://). Cut off the excess string and sheath.

**Figure 5-25**

Pull back the sheath an inch beyond any damage to the inner wires, then cut off the extra sheath and string



Jill West

1. 4

Carefully untwist each pair and straighten each wire. Make a clean cut evenly across the wires about an inch from the opening in the sheath.

1. 5

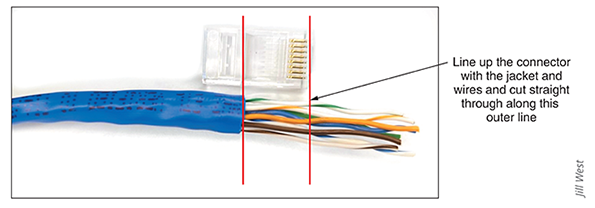
To make a straight-through cable, align all eight wires on a flat surface, one next to the other, ordered according to their colors and positions listed earlier in [Figure 5-17](javascript://). It might be helpful first to groom—or pull steadily across the length of—the unwound section of each wire to straighten it out and help it stay in place. Which T568 standard are you using? In what order will you need to place each wire in the connector?

1. 6

Measure 1/2 inch from the end of the wires and cleanly cut the wires straight across at this length. As you can see in [Figure 5-26](javascript://), it might help to hold the RJ-45 connector next to the wires to determine how short to cut the wires.

**Figure 5-26**

Straighten the wires, arrange them in order, and cut them to the appropriate length



Enlarge Image

Jill West

1. 7

Keeping the wires in line and in order, gently slide them into their positions in the RJ-45 plug. The plug should be positioned with the flat side facing toward you and the pin side facing away from you, so the appropriate wires enter the correct slots for the wiring standard. The sheath should extend into the plug about 3/8 of an inch.

1. 8

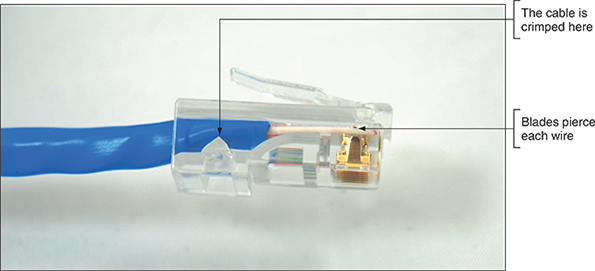
After the wires are fully inserted, place the RJ-45 plug in the crimping tool and press firmly to crimp the wires into place. Be careful not to rotate your hand or the wires as you do this, otherwise only some of the wires will be properly terminated.

1. 9

Remove the RJ-45 connector from the crimping tool. Look through the clear plastic connector to make sure each wire appears to be in contact with its pin (see [Figure 5-27](javascript://)). It might be difficult to tell simply by looking at the connector. To test the connection, try to pull the plug off the wire. If it comes out, start over. However, the real test is whether your cable will successfully transmit and receive signals. If the connection appears solid, slide the boot over the connector so it fits snugly over the clip.

**Figure 5-27**

Blades in the connector pierce the insulation of each individual copper wire



Enlarge Image

1. 10

Repeat [Steps 2](javascript://), [3](javascript://), [4](javascript://), [5](javascript://), [6](javascript://), [7](javascript://), [8](javascript://), and [9](javascript://) for the other end of the cable. After completing [Step 9](javascript://) for the other end, use a cable tester to test the signal through the cable, or connect a computer to a switch and see if they can successfully communicate. You’ll learn more about cable testers later in this module. If the cable transmits on all wires as expected, you will have created a straight-through patch cable.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2gPoE (Power over Ethernet)

In 2003, IEEE released its 802.3af standard, which specifies a method for supplying electrical power over twisted-pair Ethernet connections, also known as [**PoE (Power over Ethernet)**](javascript://). Although the standard is relatively new, the concept is not. In fact, home telephones have long received power from the telephone company over the line that enters a residence. This power is necessary for dial tone and ringing.

On an Ethernet network, carrying power over network connections can be useful for nodes that are located far from traditional power receptacles or that need a constant, reliable power source, such as security cameras placed on exterior walls. The amount of power provided is relatively small—15.4 watts for standard PoE devices and 25.5 watts for the newer [**PoE+**](javascript://) devices, defined by the 802.3at standard. But that’s enough to power a wireless access point, an IP telephone, or a security camera mounted high on a wall.

The PoE standard specifies two types of devices:

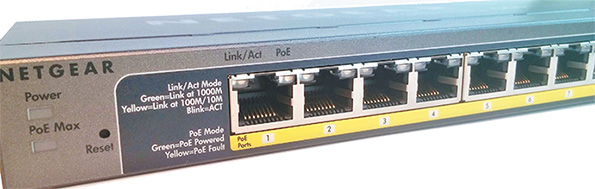
* **PSE (power sourcing equipment)**—The device that supplies the power
* **PDs (powered devices)**—Devices that receive power from the PSE

PoE requires Cat 5 or better copper cable. Inside the cable, electric current may run over an unused pair of wires or over the pair of wires used for data transmission. The standard allows for both approaches; however, on a single network, the choice of current-carrying pairs should be consistent between all PSE and PDs.

A switch or router that is expected to provide power over Ethernet must support the technology. The switch shown in [Figure 5-28](javascript://) indicates PoE is available on all 8 of its ports.

**Figure 5-28**

PoE-capable switch



Enlarge Image

Also, the end node must be capable of receiving PoE. The PSE device first determines whether a node is PoE-capable before attempting to supply it with power. While the security camera in [Figure 5-29](javascript://) includes an optional power adapter connector, its Ethernet connector is designed to optionally receive PoE instead.

**Figure 5-29**

PoE-capable security camera

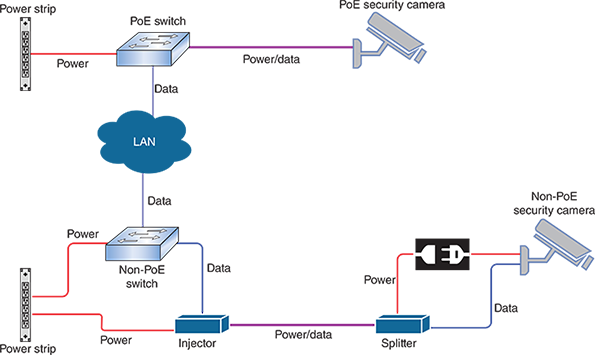


Enlarge Image

Let’s look at how these devices might be arranged on a network. The top part of [Figure 5-30](javascript://) shows a PoE-capable switch providing power and data connections to a PoE-capable security camera.

**Figure 5-30**

PoE adapters can add PoE functionality to non-PoE devices on a network



Enlarge Image

On networks that demand PoE but don’t have PoE-capable equipment, you can add PoE adapters, like the one shown in [Figure 5-31](javascript://). One type of adapter, called an injector or midspan and shown in the bottom left of [Figure 5-30](javascript://), connects to a non-PoE switch or router to inject power onto the network. Another type of adapter, called a splitter and shown in the bottom right of [Figure 5-30](javascript://), attaches to a non-PoE client, such as an outdoor camera, to receive power over the Ethernet connection. Use one or both, depending on the needs of the devices being installed.

**Figure 5-31**

Power and data separately enter this PoE injector through ports shown on the right and exit together through the port shown on the left



Source: D-Link North America

You’ve now explored copper cabling at the physical layer, but the data link layer is also affected by the physical media that make up a network. Let’s see how this works.

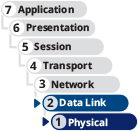
Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-2hEthernet Standards for Twisted-Pair Cable



A cable’s category (such as Cat 5e or Cat 6) determines the fastest network speed it can support. This is a layer 1 characteristic. A device’s NIC is also rated for maximum network speeds, which are defined by various [**Ethernet standards**](javascript://). Although Ethernet is generally thought of as a layer 2 protocol, it also has layer 1 functions that determine a transmission’s frequency and other electrical characteristics. Other familiar layer 2 technologies, such as USB and Wi-Fi, also include physical layer components. Part of the function of this layer is to provide signaling between two nodes as they negotiate a common language by which to communicate. As for Ethernet, most LANs today use devices and NICs that can support Fast Ethernet and Gigabit Ethernet. When they first connect, devices auto-negotiate for the fastest standard they have in common. However, the network must be wired with cabling that is capable of supporting those speeds. [Table 5-4](javascript://) lists the various Ethernet standards supported by the different categories of twisted-pair cabling.

**Table 5-4**

### Ethernet Standards Used with Twisted-Pair Cabling

| **Standard** | **Maximum transmission throughput (Mbps)** | **Maximum distance per segment (m)** | **Physical media** | **Pairs of wires used for transmission** |
| --- | --- | --- | --- | --- |
| [**10BASE-T**](javascript://) | 10 | 100 | Cat 3 or better UTP | 2 pair |
| [**100BASE-T**](javascript://)  or [**100BASE-TX**](javascript://)  (Fast Ethernet) | 100 | 100 | 100BASE-T: Cat 5 or better  100BASE-TX: Cat 6 or better | 2 pair |
| [**1000BASE-T**](javascript://) (Gigabit Ethernet) | 1000 | 100 | Cat 5 or better (Cat 5e is preferred) | 4 pair |
| [**10GBASE-T**](javascript://)  (10-Gigabit Ethernet) | 10,000 | 100 | Cat 6a or Cat 7 (Cat 7 is preferred) | 4 pair |
| [**40GBASE-T**](javascript://) | 40,000 | 30 | Cat 8 | 4 pair |

Enlarge Table

### Exam Tip

Memorize every detail in [Table 5-4](javascript://). You’ll need them to pass the exam.

**Note 5-8**

Two new standards were recently ratified by IEEE:

* **2.5GBASE-T**—2500 Mbps, requires Cat 5e or better
* **5GBASE-T**—5000 Mbps, requires Cat 6 or better

These new standards provide intermediate steps between Gigabit Ethernet and 10-Gigabit Ethernet. A network can support a variety of Ethernet standards at once. When matched with the proper twisted-pair category of cable, it’s possible to progressively upgrade a network, one device or NIC at a time.

The fastest Ethernet standard currently is 100GBASE-T, which achieves dramatic transmission rates on twisted-pair cabling that is comparable to fiber-optic cabling and is less expensive than fiber-optic. Still, as with other twisted-pair Ethernet standards, the maximum segment length for 100GBASE-T is 100 meters. This limitation means that 100GBASE-T is not appropriate for long-distance WANs, but could easily support the use of converged services, such as video and voice, at every desktop in a LAN.

Now that you’ve learned about the capabilities of copper wires to conduct signals, let’s explore the possibilities when light signals are transmitted over glass fibers.

**Remember This…**

* Identify RG-6 coaxial cable, F-connectors, and twinaxial cable.
* Compare the categories of twisted pair cable: Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7, and Cat 8.
* Memorize the T568A and T568B pinouts.
* Given a scenario, choose the correct cable: straight-through, crossover, rollover, and console.
* Explain the primary Ethernet standards for copper cabling: 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T, and 40GBASE-T.
* Describe how to incorporate PoE and PoE+ devices in a network.
* Use common network cabling tools: cable crimper, loopback adapter, snips/cutters, and cable stripper.

**Self-Check**

1. What is the minimum twisted-pair category required for 10-Gigabit Ethernet at 100 meters?

Answer

* 1. Cat 5e
  2. Cat 6a
  3. Cat 7
  4. Cat 8

1. Pin 1 on one end of a cable is orange and white striped. What color should Pin 1 be on the other end of the cable to create a crossover cable?

Answer

* 1. Orange and white striped
  2. Solid blue
  3. Solid brown
  4. Green and white striped

1. What is the typical maximum segment length for Ethernet networks?

Answer

* 1. 10 meters
  2. 100 meters
  3. 1000 meters
  4. 10,000 meters

**You’re Ready**

You’re now ready to complete [Project 5-2: Create a Loopback Plug](javascript://), or you can wait until you’ve finished reading this module.

**You’re Ready**

You’re now ready to complete [Project 5-3: Create a Loopback Jack](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 5-3Fiber-Optic Cable

### Certification

* 1.3:

Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

* 2.1:

Compare and contrast various devices, their features, and their appropriate placement on the network.

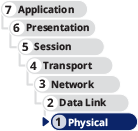
* 5.2:

Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

* 5.5:

Given a scenario, troubleshoot general networking issues.

Average reading time: 27 minutes



Fiber-optic cable, or simply fiber, contains one or several glass or plastic fibers at its center, or **core**. Data is transmitted through the central fibers via pulsing light typically sent from one of two possible sources:

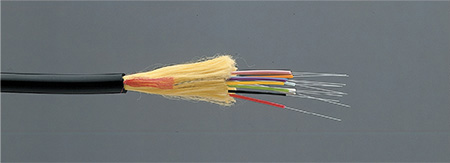
* **Laser**—An intense, focused light that can travel extremely long distances with very high data throughput
* [**LED (light-emitting diode)**](javascript://)—A cool-burning, long-lasting technology used on shorter fiber-optic connections, such as between floors in a building or between a switch and a router

Surrounding the fibers is a layer of glass or plastic called [**cladding**](javascript://). The cladding is less dense than the glass or plastic in the strands and so reflects light back to the core in patterns that vary depending on the transmission mode. This reflection allows the fiber to bend around corners without diminishing the integrity of the light-based signal (although bend radius limitations do apply).

Outside the cladding, a plastic buffer protects the cladding and core. Because the buffer is opaque, it also absorbs any light that might escape. To prevent the cable from stretching, and to protect the inner core further, strands of Kevlar (a polymeric fiber) surround the plastic buffer. Finally, a plastic sheath covers the strands of Kevlar. [Figure 5-32](javascript://) shows a fiber-optic cable with multiple, insulated fibers. The clear strands you see protruding from each line are not the actual cores—these are the visible cladding around each core. A core itself is microscopic in width.

**Figure 5-32**

A fiber-optic cable



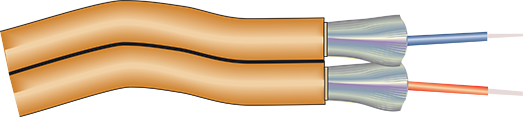
Source: Optical Cable Corporation

Like twisted-pair and coaxial cabling, fiber-optic cabling comes in a number of varieties, depending on its intended use and the manufacturer. For example, fiber-optic cables used to connect the facilities of large telephone and data carriers may contain as many as 1000 fibers and be heavily sheathed to prevent damage from extreme environmental conditions. At the other end of the spectrum, fiber-optic patch cables for use on LANs might contain only two strands of fiber and be pliable enough to wrap around your hand.

Because each strand of glass in a fiber-optic cable usually transmits in one direction only—in simplex fashion—two strands are often needed for full-duplex communication. One solution is to use a zipcord cable, in which two strands are combined side by side in conjoined jackets, as depicted in [Figure 5-33](javascript://). You’ll find zipcords where fiber-optic cable spans relatively short distances, such as connecting a server and switch. A zipcord may come with one of many types of connectors on its ends, as described later in this section.

**Figure 5-33**

Zipcord fiber-optic patch cable



With a zipcord cable, full-duplex communication is achieved by sending data on one port and receiving data through the other. A newer technology allows bidirectional transmission on both ports, which means each fiber cable carries data in both directions. It uses the newer bidirectional WDM technology to separate the data traveling in each direction on different wavelengths of light, or colors. To work, it requires special equipment on each end of the connection called a BiDi (pronounced bye-dye) transceiver, also called a WDM transceiver. BiDi transceivers are more expensive than their standard, duplex cousins, but they reduce by half the amount of fiber cabling needed for the same data throughput, making them more economical.

Fiber-optic cable is the industry standard for high-speed networking and provides the following benefits over copper cabling:

* Extremely high throughput
* Very high resistance to noise
* Excellent (though not perfect) security
* Ability to carry signals for much longer distances before requiring repeaters

While fiber cable itself is not hugely more expensive than comparable copper cable, the most significant drawback to fiber is that it is more expensive to install, and fiber equipment is pricier. Fiber-optic cable requires special equipment for splicing, or joining, which means that quickly repairing a fiber-optic cable in the field (given little time or resources) can be difficult. Fiber’s characteristics are summarized in the following list:

* **Throughput**—Fiber has proven reliable in transmitting data at rates that can reach 100 gigabits (or 100,000 megabits) per second per channel. Fiber’s amazing throughput is partly due to the physics of light traveling through glass. Unlike electrical pulses traveling over copper, light experiences virtually no resistance. Therefore, light-based signals can be transmitted at faster rates and with fewer errors than electrical pulses. In fact, a pure glass strand can accept up to 1 billion laser light pulses per second. Its high throughput capability makes it suitable for network backbones and for supporting applications that generate a great deal of traffic, such as video or audio conferencing.
* **Cost**—Fiber-optic cable is the most expensive wired transmission medium. Because of its cost, most organizations find it impractical to run fiber to every desktop. Not only is the cable itself more expensive than copper cabling, but fiber-optic transmitters and connectivity equipment can cost as much as five times more than those designed for UTP networks. In addition, hiring skilled fiber-cable installers costs more than hiring twisted-pair cable installers.
* **Noise immunity**—Because fiber does not conduct electrical current to transmit signals, it is unaffected by EMI. Its impressive noise resistance is one reason why fiber can span such long distances.
* **Size and scalability**—Depending on the type of fiber-optic cable used, segment lengths vary from 2 to 40,000 meters. The maximum limit is due primarily to [**optical loss**](javascript://), or the degradation of the light signal after it travels a certain distance away from its source (just as the light of a flashlight dims after a certain number of feet). Optical loss accrues over long distances and grows with every connection point in the fiber network. Dust or oil in a connection (for example, from people handling the fiber while splicing it) can further exacerbate optical loss.

While the distance a cable can carry light depends partly on the light’s wavelength, it also depends on whether the cable is single mode or multimode. Let’s see what the primary differences are between these two types of fiber cable.

Go to pg.

[**help**](javascript://)

Application Opened

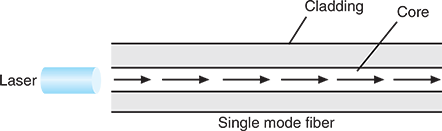
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3aSMF (Single Mode Fiber)

[**SMF (single mode fiber)**](javascript://) consists of a narrow core of 8 to 10 microns in diameter. Laser-generated light travels a single path over the core, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows SMF to accommodate the highest bandwidths and longest distances (without requiring repeaters) of all wired network transmission media. [Figure 5-34](javascript://) depicts a simplified version of how signals travel over single mode fiber.

**Figure 5-34**

Transmission over single mode fiber-optic cable



The Internet backbone depends on single mode fiber. However, because of its relatively high cost, SMF is rarely used for short connections, such as those between a server and switch.

Go to pg.

[**help**](javascript://)

Application Opened

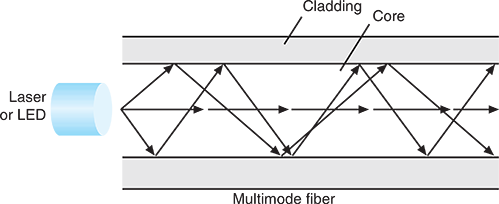
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3bMMF (Multimode Fiber)

[**MMF (multimode fiber)**](javascript://) contains a core with a larger diameter than SMF, usually 50 or 62.5 microns, over which many pulses of light generated by a laser or LED light source travel at various angles. Signals traveling over multimode fiber experience greater attenuation than those traversing single mode fiber. Therefore, MMF is not suited to distances longer than a few kilometers. On the other hand, MMF is less expensive to install and, therefore, is typically used to connect routers, switches, and servers on the backbone of a network or to connect a desktop workstation to the network. [Figure 5-35](javascript://) depicts a simplified view of how signals travel over multimode fiber.

**Figure 5-35**

Transmission over multimode fiber-optic cable



The transition between SMF and MMF cabling might occur at an [**FDP (fiber distribution panel)**](javascript://), which is usually a case on a rack where fiber cables converge, connect with each other, and connect with fiber-optic terminal equipment from the ISP. Splices at the FDP (or elsewhere on the network) might be accomplished by joining two fiber cables in a permanent bond using a [**fusion splicer**](javascript://), which melts the tips of two fibers together so light can pass cleanly through the joint, or various connectors might be used to create temporary splices.

**Note 5-9**

Although the process is a bit more sensitive to error than terminating copper cable, you can also terminate fiber-optic cable. A typical fiber termination kit might include the following tools:

* **Fiber stripper**—Strips off the outer layers of a fiber-optic cable
* **Fiber cleaver**—Cuts a clean slice through the fiber strands

If you don’t have this equipment on hand, you can find a few videos on the web that demonstrate the process and tools.

Go to pg.

[**help**](javascript://)

Application Opened

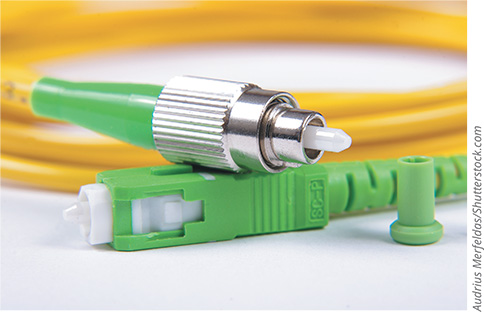
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3cFiber Connectors

Just as fiber cables are classified by SMF or MMF, fiber-cable connectors are also grouped along these lines. MMF connectors can be classified by the number of fibers they connect, and SMF connectors are classified by the size and shape of the ferrule. The [**ferrule**](javascript://) is the extended tip of a connector that makes contact with the receptacle in the jack or other connector, as you can see in [Figure 5-36](javascript://).

**Figure 5-36**

A cap protects the ferrule when the connector is not in use



Audrius Merfeldas/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

SMF connectors are designed to reduce [**back reflection**](javascript://), which is the return of the light signal back into the fiber that is transmitting the signal. Back reflection is measured as optical loss in dB (decibels). Shapes and polishes currently used on SMF ferrules to reduce back reflection include the following:

* [**UPC (ultra-physical contact)**](javascript://)—Extensive polishing of the tips creates a rounded surface, which allows the two internal fibers to meet and increases efficiency over older types of connections.
* [**APC (angled physical contact)**](javascript://)—Uses a polished curved surface, but the end faces are placed at an angle to each other; the industry standard for this angle is 8 degrees.

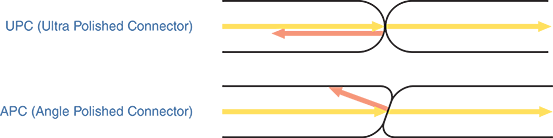
**Note 5-10**

UPC adapters and connectors are often blue, and APC adapters and connectors are often green. But not always.

You can see how these two types of ferrule shapes compare in [Figure 5-37](javascript://). The red arrows indicate the back reflection for each connection. Notice how the APC connection reflects any signal loss in a different direction than the source of the signal. Back reflection worsens in UPC connections over time, but APC connections are not as sensitive to degradation from repeatedly disconnecting and reconnecting cables.

**Figure 5-37**

Two types of mechanical connections in fiber-optic connectors



[Table 5-5](javascript://) summarizes the fiber connectors you’ll need to know for the CompTIA Network+ exam. SMF connectors are typically available with a 1.25-mm ferrule or a 2.5-mm ferrule, though other sizes can be found. The most common 1.25-mm ferrule connector is [**LC (local connector)**](javascript://). Two 2.5-mm ferrules are [**SC (subscriber connector or standard connector)**](javascript://) and [**ST (straight tip)**](javascript://). The most common type of MMF connector is [**MT-RJ (mechanical transfer-registered jack)**](javascript://).

**Table 5-5**

### Characteristics of Fiber Connectors

| **Photo** | **Connector** | **Polish** | **Ferrule characteristics** | **Full-duplex?** |
| --- | --- | --- | --- | --- |
| LC  A photograph of a 1.25 millimeter local connector.  Source: Senko Advanced Components, Inc. | LC | UPC, APC | 1.25 mm | Yes |
| ST  A photograph of a 2.5 millimeter straight-tip connector.  Source: Senko Advanced Components, Inc. | ST | UPC | 2.5 mm | No |
| SC  A photograph of a 2.5 millimeter subscriber connector.  Source: Senko Advanced Components, Inc. | SC | UPC, APC | 2.5 mm | Can be |
| MT-RJ  A photograph of a mechanical transfer-registered jack which is the most common type of M M F connector.  Source: Senko Advanced Components, Inc. | MT-RJ | N/A | 2 fibers | Yes |

Enlarge Table

Older fiber networks might use ST or SC connectors. However, LC and MT-RJ connectors are now more common because of their smaller sizes, which allows for a higher density of connections at each termination point. The MT-RJ connector is unique in that it contains two strands of fiber in a single ferrule. With two strands per ferrule, a single MT-RJ connector provides full-duplex signaling. SC and LC connectors are also available in full-duplex mode.

### Exam Tip

You’ve read about several cable connectors in this module. You can see a list of all the ones you’ll need to know for the CompTIA Network+ exam, along with images to help you identify them visually, in Appendix B.

Go to pg.

[**help**](javascript://)

Application Opened

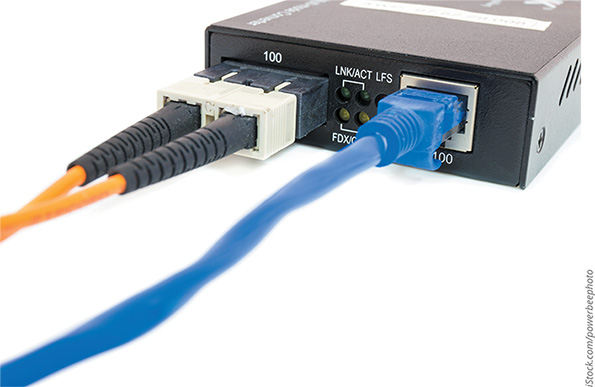
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3dMedia Converters

As long as networks contain both copper and fiber media, some kind of conversion must take place. A [**media converter**](javascript://) is hardware that enables networks or segments running on different media to interconnect and exchange signals. For example, suppose an Ethernet segment leading from your company’s data center uses fiber-optic cable to connect to a workgroup switch that only accepts twisted-pair (copper) cable. In that case, you could use a media converter to interconnect the switch with the fiber-optic cable. The media converter completes the physical connection and also converts the electrical signals from the copper cable to light wave signals that can traverse the fiber-optic cable, and vice versa. Such a media converter is shown in [Figure 5-38](javascript://).

**Figure 5-38**

Copper wire-to-fiber media converter



Enlarge Image

[iStock.com](http://istock.com/" \t "_blank)/powerbeephoto

You must select the correct media converter for the type of fiber being connected, whether it’s SMF to copper or MMF to copper. Converters are also needed to connect networks using MMF with networks using SMF. [Figure 5-39](javascript://) shows a converter that connects single mode and multimode portions of a network.

**Figure 5-39**

Single mode to multimode converter



Courtesy of Omnitron Systems Technology

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3eFiber Transceivers

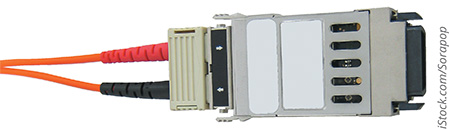
Suppose you are purchasing a switch that will be part of a network for a new, fast-growing business. The current requirements for the switch might be two fiber-optic connections for the network backbone and 24 RJ-45 Gigabit Ethernet connections for clients and servers. For the future, however, you are considering fiber-optic connectivity to every desktop.

Rather than ordering a switch that contains exactly the currently needed number and type of onboard interfaces, you could order a switch that allows you to change and upgrade its interfaces at any time. These switches contain sockets where one of many types of modular interfaces, called [**transceivers**](javascript://), can be plugged in. Such transceivers are easily inserted into the sockets to connect with its motherboard and upgraded later as technology improves. A hardware component that can be changed in this manner, without disrupting operations, is called [**hot-swappable**](javascript://). Using hot-swappable transceivers means you don’t have to purchase a new switch, open the chassis of the existing switch (causing network downtime and risking hardware damage), or even turn off the switch to upgrade the network. Modular interfaces can also be installed on some expansion board NICs and media converters.

GBIC (Gigabit interface converter), pronounced jee-bick, was a standard type of transceiver designed in the 1990s for Gigabit Ethernet connections. GBICs might contain RJ-45 ports for copper cables or SC ports for fiber-optic connections. [Figure 5-40](javascript://) shows a GBIC that can be used on a Gigabit Ethernet fiber network.

**Figure 5-40**

GBIC (Gigabit interface converter) with dual SC ports



[iStock.com/Sorapop](http://istock.com/Sorapop" \t "_blank)

Newer transceivers that have made the GBIC obsolete include the following:

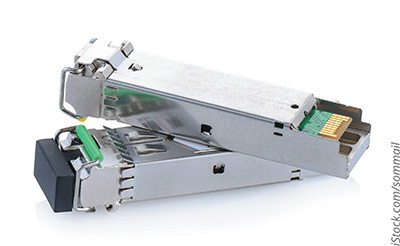
* [**SFP (small form-factor pluggable)**](javascript://)—Provides the same function as GBICs and is more compact, allowing more ports per linear inch. Also known as mini GBICs or SFP GBICs. Typically used for 1 Gbps connections, but theoretically capable of 5 Gbps.
* [**XFP (10 Gigabit small form-factor pluggable)**](javascript://)—Supports up to 10 Gbps and is slightly larger than SFP with lower power consumption than SFP+.
* [**SFP+**](javascript://)—Developed later than XFP and is the same module size as SFP; theoretical maximum transmission speed is 16 Gbps. SFP+ transceivers are still widely used today.
* [**QSFP (quad small form-factor pluggable)**](javascript://)—Complies with the 802.3ba standard, squeezing four channels in a single transceiver and supporting data rates up to 40 Gbps (4 x 10 Gbps).
* [**QSFP+**](javascript://)—Generally the same technology as QSFP while supporting data rates over 40 Gbps. Highest speed format at the time of this writing is QSFP56-DD, which doubles the data lanes to eight and supports a total theoretical maximum data rate of 400 Gbps (8 x 50 Gbps). The twinax cable you saw earlier in [Figure 5-10](javascript://) is terminated with QSFP+ transceivers.
* [**CFP (centum form-factor pluggable)**](javascript://)—Intended for 100-Gbps network connections, with each succeeding generation (CFP2, CFP4, CFP8) becoming smaller and more energy-efficient. Centum is Latin for 100.

To avoid using the incorrect transceiver, you must pair these devices based on supported speeds and protocols. Also consider the cable connectors you’ll be using. Most modern transceivers support LC or, occasionally, RJ-45 connectors.

[Figure 5-41](javascript://) shows two SFPs. The black dust plug on the left side of the bottom transceiver is covering two ports for fiber-optic cable connectors, one for transmitting and another for receiving data. [Figure 5-42](javascript://) shows two transceivers installed in a media converter. The transceiver on the left is an SFP+, and the transceiver on the right is an XFP.

**Figure 5-41**

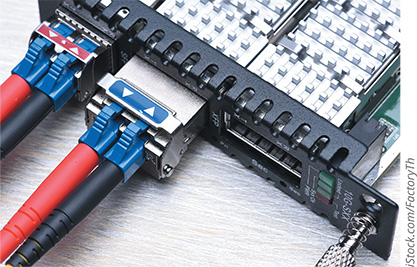
These SFPs slide into a switch to add fiber-optic connectivity



[iStock.com/sommail](http://istock.com/sommail" \t "_blank)

**Figure 5-42**

This media converter supports both SFP+ and XFP

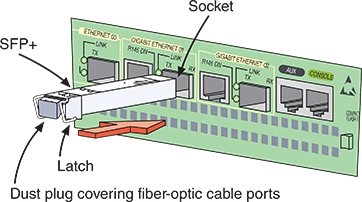


[iStock.com/FactoryTh](http://istock.com/FactoryTh" \t "_blank)

Installing a transceiver of any of these types is simply a matter of sliding it into a compatible socket on the connectivity device. Most transceivers come with a tab or latch system to lock them into place. They are also keyed so that they will slide into the socket only when aligned properly. The switch or router need not be powered down when you add or remove transceivers. However, do not attach cables before inserting a transceiver, and always remove the cables before removing a transceiver. [Figure 5-43](javascript://) illustrates how a fiber-optic SFP+ is installed in a switch.

**Figure 5-43**

Installing an SFP+ in a switch



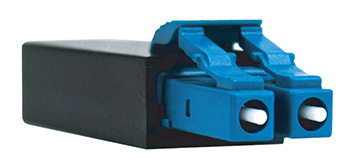
Some transceivers contain management interfaces separate from the switch’s configuration utility. For example, a 16-Gbps SFP+ on a router could have its own IP address. A network administrator could use the Telnet utility to connect to the transceiver and configure its ports for a particular speed or routing protocol without accessing the router’s operating system. Earlier in [Figure 5-10](javascript://), if you look closely, you can see a small chip on the circuit board. This chip allows the transceiver to communicate with the device into which it is installed.

**Note 5-11**

A helpful tool when testing a transceiver’s functionality or checking for a mismatch is a loopback adapter. Recall from earlier in this module that a loopback adapter can create a closed loop to trick a device into thinking it’s connected to a network. A loopback adapter can do much the same thing with a transceiver, although a fiber-optic loopback adapter is specifically needed for use on a fiber connector. [Figure 5-44](javascript://) shows a fiber-optic loopback adapter with two LC fiber-cable connectors.

**Figure 5-44**

Fiber-optic loopback adapter



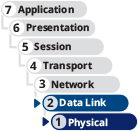
Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3fEthernet Standards for Fiber-Optic Cable



Long before IEEE developed a 10GBASE-T standard for twisted-pair cable, it established standards for achieving high data rates over fiber-optic cable. In fact, fiber optic is the best medium for delivering high throughput. [Table 5-6](javascript://) lists various Ethernet standards established by IEEE for fiber-optic cabling and covered in the CompTIA Network+ objectives. Notice in the table there are Ethernet standards for Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet that all use fiber-optic cables. As you saw when discussing transceivers, even faster Ethernet standards are available, up to 100-Gigabit Ethernet.

**Table 5-6**

### Ethernet Standards Using Fiber-Optic Cable

| **Standard** | **Maximum transmission bandwidth (Mbps)** | **Maximum distance per segment (m)** | **Physical media** |
| --- | --- | --- | --- |
| [**100BASE-SX**](javascript://)  (Fast Ethernet) | 100 | Up to 300, depending on modal bandwidth and fiber core diameter | MMF |
| [**100BASE-FX**](javascript://)  (Fast Ethernet) | 100 | Up to 2000, depending on modal bandwidth and fiber core diameter | MMF |
| [**1000BASE-SX**](javascript://)  (Gigabit Ethernet) | 1000 | Up to 550, depending on modal bandwidth and fiber core diameter | MMF |
| [**1000BASE-LX**](javascript://)  (Gigabit Ethernet) | 1000 | 550 for MMF, 5000 for SMF | MMF or SMF |
| [**10GBASE-SR**](javascript://)  (10-Gigabit Ethernet) | 10,000 | Up to 300, depending on modal bandwidth and fiber core diameter | MMF |
| [**10GBASE-LR**](javascript://)  (10-Gigabit Ethernet) | 10,000 | 10,000 | SMF |

For the CompTIA Network+ exam, you need to know these six fiber Ethernet standards. Here are some important details about each:

* 100BASE-SX is a low-cost solution for Fast Ethernet and uses a short 850-nanometer wavelength light signal, hence the S in its name SX. (A nanometer equals 0.000000001 meters, or about the width of six carbon atoms in a row.) The maximum segment length for 100BASE-SX and other MMF cables depends on two things: the diameter of the fiber and the modal bandwidth used to transmit signals. [**Modal bandwidth**](javascript://) is a measure of the highest frequency of signal a multimode fiber can support over a specific distance and is measured in MHz-km. It is related to the distortion that occurs when multiple pulses of light, although issued at the same time, arrive at the end of a fiber at slightly different times. The higher the modal bandwidth, the longer a multimode fiber can carry a signal reliably. Only one repeater may be used between segments. At most, segment lengths for this standard are limited to a short 300-meter distance.
* 100BASE-FX also offers Fast Ethernet speeds (thus the F in its name FX), uses a longer wavelength of 1300 nanometers, and is rated up to 2 kilometers. 100BASE-FX still uses MMF cable, but similar standards, 100BASE-LX and 100BASE-BX, offer even longer distances (10 kilometers) over SMF instead.
* 1000BASE-SX is a form of Gigabit Ethernet and uses short wavelengths of 850 nanometers. 1000BASE-SX is best suited for short network runs—for example, connecting a data center with a data closet in an office building.
* 1000BASE-LX is the more common fiber version of Gigabit Ethernet and uses long wavelengths (hence the L in its name LX) of 1300 nanometers. Because of its long segments, it’s used for long backbones connecting buildings in a MAN or for connecting an ISP with its telecommunications carrier.
* 10GBASE-SR is the “short range” standard for 10-Gigabit Ethernet. Using 850 nanometer wavelengths and MMF, the maximum supported distances vary according to the type of cabling used and max out around 400 meters.
* 10GBASE-LR uses lasers emitting 1310 nanometer light. This “long range” version of 10-Gigabit Ethernet can extend as far as 10 kilometers.

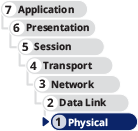
Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3gCommon Fiber-Cable Problems



Working with fiber cable presents a set of troubleshooting challenges that don’t arise when you are working with copper cables. Problems unique to fiber cable include the following:

* **Fiber type mismatch**—This term is misleading because a fiber type mismatch is actually more of a fiber core mismatch. Connecting an SMF cable to an MMF cable will prevent the transmission from traversing the connection successfully, though some of the signal can get through. However, even same-mode cables can be mismatched if the cores have different widths. A cable with a 50-micron core, for example, should not be connected to a cable with a 62.5-micron core, even though they’re both MMF.
* **Wavelength mismatch**—SMF, MMF, and POF (Plastic Optical Fiber) each use different wavelengths for transmissions. A wavelength mismatch occurs when transmissions are optimized for one type of cable but sent over a different type of cable.
* **Dirty connectors**—If fiber connectors get dirty or just a little dusty, signal loss and other errors can start to cause problems. Always keep protectors on fiber connectors and dust covers over fiber jacks when they’re not in use.
* **Link loss**—As with most things, networks rarely function in an ideal environment. The power of a light signal emitted at one end of a connection is subjected to many losses along its way to the other end, including losses from distance along the cable, losses from multiplexing, and losses from imperfect connections, patches, or splices. A transceiver must offer a sufficient power budget to overcome all these losses (measured in dB) and still produce a strong-enough signal at the receiving end. This calculation is called an [**optical link budget**](javascript://), and it considers all anticipated losses along the length of the connection. A low optical link budget results in link loss issues, including reduced transmission efficiency and downtime.

**Remember This…**

* Explain the differences between SMF and MMF fiber cable.
* Identify common fiber connectors and ferrule types: LC, ST, SC, MT-RJ, APC, and UPC.
* Compare fiber transceiver types: SFP, SFP+, QSFP, and QSFP+.
* Explain common fiber Ethernet standards: 100BASE-SX, 100BASE-FX, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, and 10GBASE-LR.

**Self-Check**

1. Which of the following statements is not true?

Answer

* 1. SMF has a thinner core than MMF.
  2. SMF supports lower bandwidths than MMF.
  3. MMF is better suited than SMF to backbone connections within the data center.
  4. MMF signals experience greater reflection within the core than SMF signals.

1. Which fiber connector does not support full-duplex transmissions?

Answer

* 1. LC
  2. MT-RJ
  3. SC
  4. ST

1. What is the earliest transceiver type to support four channels on a single transceiver to increase throughput?

Answer

* 1. QSFP
  2. SFP+
  3. SFP
  4. QSFP+

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

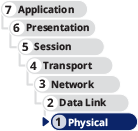
# 5-4Cable Troubleshooting Tools

### Certification

* 5.2:

Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

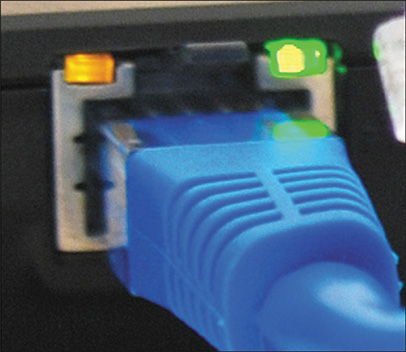
Average reading time: 14 minutes



Symptoms of cabling problems can be as elusive as occasional lost packets or as obvious as a break in network connectivity. You can start troubleshooting a network connection problem by checking the network connection LED status indicator lights on the network ports of the devices involved. A steady light indicates connectivity, and a blinking light indicates activity. A red or amber light, as shown in [Figure 5-45](javascript://), might indicate a problem. Check the device NICs and make sure cable connections are solid.

**Figure 5-45**

Status indicator lights for an onboard network port



If all the devices check out and you suspect a cabling issue, you need to know which tools are designed to analyze and isolate problems related to particular types of network media. Several tools are available, ranging from simple continuity testers that indicate whether a cable is faulty, to sophisticated cable performance testers that graphically depict a cable’s attenuation and crosstalk characteristics over the length of the cable. Knowing the specific tool to use for a particular troubleshooting scenario can help you quickly zero in on the problem and the solution. The following sections describe a variety of cable troubleshooting tools, their functions, and their relative costs.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4aToner and Probe Kit

Ideally, you and your networking colleagues would label each port and wire termination in a data room so that problems and changes can be easily managed. However, because of personnel changes and time constraints, a data room might be disorganized and poorly documented. If this is the case where you work, a tone generator and a tone locator can help you determine where a wire, possibly out of hundreds, terminates:

* [**Tone generator (or toner)**](javascript://)—A small, electronic device that issues a signal on a wire
* [**Tone locator (or probe)**](javascript://)—A device that emits an audible tone when it detects electrical activity on a wire

They are sold together as a set, often called a toner and probe kit or just toner probe (see [Figure 5-46](javascript://)).

**Figure 5-46**

A toner and probe kit by Fluke Corporation



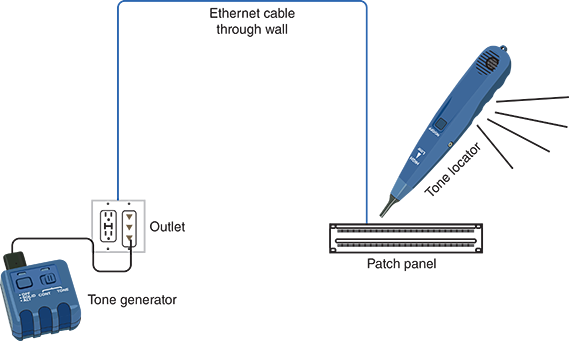
Enlarge Image

Place the tone generator at one end of a wire using the appropriate connector. Swipe the tone locator over each of the terminations you suspect to be the other end of that wire. You can verify the location of the wire’s termination when you hear the tone.

[Figure 5-47](javascript://) depicts the use of a tone generator and a tone locator. Work by trial and error, guessing which termination corresponds to the wire over which you’ve generated a signal until the tone locator indicates the correct choice.

**Figure 5-47**

A toner and probe kit locates the termination of a wire



Tone generators and tone locators cannot be used to determine any characteristics about a wire, such as whether it’s defective or whether its length exceeds IEEE standards for a certain type of network. They are only used to determine where a wire terminates.

### Caution

A tone generator should never be used on a wire that’s connected to a device’s port or network adapter. Because a tone generator transmits electricity over the wire, it could damage the device or network adapter.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4bMultimeter

A [**multimeter**](javascript://) is a simple instrument that can measure many characteristics of an electric circuit, including its resistance, voltage, and impedance (see [Figure 5-48](javascript://)). Although you could use separate instruments for measuring impedance on an AC (alternating current) circuit, resistance (opposition to electrical current) on a DC (direct current) circuit, and voltage on an AC or DC circuit, it is more convenient to have one instrument that accomplishes all these functions.

**Figure 5-48**

A multimeter



Enlarge Image

Recall that impedance is a measure of the opposition to a current’s flow through a cable and is expressed in ohms. Lower impedance results in better power transfer, and higher impedance yields less attenuation of the data signal over a distance. Impedance is the telltale factor for ascertaining where faults in a cable lie. A certain amount of impedance is required for a signal to be properly transmitted and interpreted. However, very high or low levels of impedance can signify a damaged wire, incorrect pairing, or a termination point. In other words, changes in impedance can indicate where current is stopped or inhibited.

As a network professional, you might use a multimeter to do the following:

* Measure voltage to verify that a cable is properly conducting electricity—that is, whether its signal can travel unimpeded from one node on the network to another.
* Check for the presence of noise on a wire (by detecting extraneous voltage).
* Test for short or open circuits in the wire (by detecting unexpected resistance or loss of voltage).
  + A [**short circuit**](javascript://) is an unwanted connection, such as when exposed wires touch each other.
  + An [**open circuit**](javascript://) is one where needed connections are missing, such as when a wire breaks.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4cCable Continuity Tester

In troubleshooting a physical layer problem, you might find the cause of a problem by simply testing a cable’s [**continuity**](javascript://)—that is, whether it is carrying a signal to its destination. Tools used to test the continuity of the cable might be called cable checkers, [**continuity testers**](javascript://), or cable testers. The term [**cable tester**](javascript://), however, is a general term that might also refer to more sophisticated tools that measure cable performance.

A cable continuity tester (see [Figure 5-49](javascript://)) is battery operated and has two parts:

* The base unit connects to one end of the cable and generates voltage.
* The remote unit connects to the other end of the cable and detects the voltage.

**Figure 5-49**

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

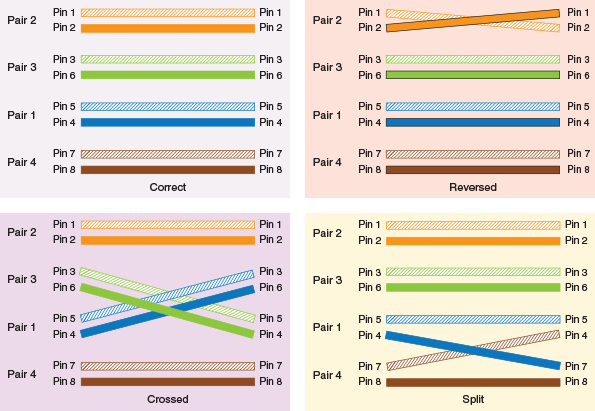


Most cable testers provide a series of lights that signal pass/fail or other information, and some units also emit an audible tone. Here are some additional characteristics to consider when selecting a cable tester:

* Some continuity testers will verify that the wires in a UTP or STP cable are paired correctly following TIA/EIA 568 standards and that they are not shorted, exposed, or crossed. This is called a [**wire map test**](javascript://), and it indicates that each pin on one end is paired with the appropriate pin on the other end. It might seem like mixing colors wouldn’t matter on a cable so long as both ends of the cable match. However, an incorrect pinout can cause excessive crosstalk issues, voltage spikes, reduced performance, and problematic connections, especially with older devices. Make sure that the cable tester you purchase can test the type of network you use—for example, 1000BASE-T or 10GBASE-T Ethernet. Common problems a wire map test can detect are illustrated in [Figure 5-50](javascript://) and include the following:
  + **Reversed pair**—The wires of one pair (for example, the orange pair) are reversed with each other when they shouldn’t be. For example, perhaps the solid orange wire is inserted into the pin where the striped orange wire should go, and the striped orange wire is inserted where the solid orange wire should go.
  + **Crossed pair**—Two pairs are reversed with each other when they shouldn’t be. For example, perhaps the wires of the green pair are inserted where the wires of the blue pair should go, and vice versa.
  + **Split pair**—One wire from each of two pairs are reversed with each other when they shouldn’t be. For example, perhaps the solid blue wire from the blue pair is inserted where the striped brown wire from the brown pair should go, and vice versa. This is one of the most difficult wire map issues to detect as this wiring could still pass a simple continuity test.

**Figure 5-50**

Common problems detected by a wire map test



Enlarge Image

* Continuity testers for fiber-optic cables issue light pulses on the fiber and determine whether they reach the other end of the fiber. Some continuity testers offer the ability to test both copper and fiber-optic cables.
* Most continuity testers are portable and lightweight, and typically use one 9-volt battery. A continuity tester can cost between $10 and $300 and can save many hours of work. Popular manufacturers of these cable testing devices include Belkin, Fluke, and Greenlee.

### Caution

Do not use a continuity tester on a live network cable. Disconnect the cable from the network and then test its continuity.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4dCable Performance Tester

Whereas continuity testers can determine whether a single cable is carrying current, more sophisticated equipment is needed to measure the overall performance of a cabling structure. A device used for this sophisticated testing is called a [**cable performance tester**](javascript://), line tester, certifier, or network tester. It allows you to perform the same continuity and fault tests as a continuity tester, but can also be used to:

* Measure the distance to a connectivity device, termination point, or damage in a cable
* Measure attenuation along a cable
* Measure NEXT (near end crosstalk) between wires as well as alien crosstalk
* Measure termination resistance and impedance
* Issue pass/fail ratings for various categories of cabling standards
* Store and print cable testing results or directly save data to a computer database
* Graphically depict a cable’s attenuation and crosstalk characteristics over the length of the cable

A sophisticated performance tester will include a [**TDR (time domain reflectometer)**](javascript://). A TDR issues a signal on a cable and then measures the way the signal bounces back (or reflects) to the TDR. Bad connectors, crimps, bends, short circuits, cable mismatches, bad wiring, or other defects modify the signal’s amplitude before it returns to the TDR, thus changing the way it reflects. The TDR analyzes the return signal and, based on its condition and the amount of time the signal took to return, determines cable imperfections.

Performance testers for fiber-optic connections use [**OTDRs (optical time domain reflectometers)**](javascript://). Rather than issue an electrical signal over the cable as twisted-pair cable testers do, an OTDR transmits light-based signals of different wavelengths over the fiber. Based on the type of return light signal, the OTDR can do the following:

* Accurately measure the length of the fiber
* Determine the location of faulty splices, breaks, bad or mismatched connectors, or bends
* Measure attenuation over the cable

Because of their sophistication, performance testers for both copper and fiber-optic cables cost significantly more than continuity testers. A high-end kit could cost up to $50,000, while a very low-end unit could sell for a few hundred dollars. [Figure 5-51](javascript://) shows an example of a high-end cable performance tester that can measure the characteristics of both copper and fiber-optic cables.

**Figure 5-51**

The DTX-1800 device by Fluke Networks is a high-end cable performance tester designed to certify structured cabling



Courtesy of Fluke Networks

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4eOPM (Optical Power Meter)

An [**OPM (optical power meter)**](javascript://), also called a [**fiber light meter**](javascript://), measures the amount of light power transmitted on a fiber-optic line. The device must be calibrated precisely, following highly accurate optical power standards set by the NIST (National Institute of Standards and Technology), which is a nonregulatory agency of the U.S. Department of Commerce. However, the surrounding room temperature, connection type, and skill of the technician conducting the test all affect the accuracy of the final test results. A simple light meter is pictured in [Figure 5-52](javascript://). More sophisticated and accurate meters are available at much higher price points.

**Figure 5-52**

This optical power meter measures light power transmitted on a fiber-optic line



As you conclude your exploration of various cable testing tools, consider that the time it takes to test a cable before installation could save many hours of troubleshooting after the network is in place. Recall the [On the Job](javascript://) story at the beginning of this module where the consultant spent many unpleasant hours tracing poorly installed cables and devices. Whether you make your own cables or purchase cabling from a reputable vendor, test the cable to ensure that it meets your network’s required standards. Just because a cable is labeled “Cat 6a,” for example, does not necessarily mean that it will live up to that standard.

**Remember This…**

* Describe the purpose of common troubleshooting tools: toner and probe kit, multimeter, cable tester, cable performance tester (including an OTDR), and a fiber light meter.
* Explain how to troubleshoot common cabling issues, such as incorrect pinout and open or short circuits.

**Self-Check**

1. Which tool could you use to determine if a laptop’s power cable is working properly?

Answer

* 1. Continuity tester
  2. Cable performance tester
  3. Toner and probe kit
  4. Multimeter

1. Which tool could you use to test a twisted-pair cable’s pinout?

Answer

* 1. OTDR
  2. Toner probe
  3. OPM
  4. Continuity tester

**You’re Ready**

You’re now ready to complete [Project 5-4: Test a LAN’s Speed and Throughput](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 5 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 5-5a**Module Summary**

### Transmission Basics

* Frequency is typically measured in MHz (megahertz) or GHz (gigahertz), which indicates the number of times in a second that an electrical signal can change states (for example, change from a positive to a negative charge or vice versa). You’ll see maximum frequencies identified for different categories of copper cabling, but sometimes this maximum frequency is also called bandwidth to indicate the possible range of frequencies up to that maximum. Bandwidth is measured in Mbps (megabits per second) or Gbps (gigabits per second) and refers to the amount of data you could theoretically transmit during a given period of time, taking into consideration factors such as frequency, distance, and SNR (signal-to-noise ratio). Throughput (also called payload rate or effective data rate) is also measured in Mbps (megabits per second) or Gbps (gigabits per second) and refers to the number of data bits (0s and 1s) that are actually received across a connection each second. Throughput takes into consideration the reality of a network environment.
* Noise, or interference, can degrade or distort a signal and, on a network, is measured in dB (decibel) loss. EMI (electromagnetic interference) is caused by motors, power lines, televisions, copiers, fluorescent lights, microwave ovens, manufacturing machinery, and other sources of electrical activity (including a severe thunderstorm). Crosstalk occurs when a signal traveling on one wire or cable infringes on the signal traveling over an adjacent wire or cable.
* Attenuation is the loss of a signal’s strength as it travels away from its source. To compensate for attenuation, signals are boosted en route using a repeater, which regenerates a digital signal in its original form without the noise it might have previously accumulated.
* Latency is the brief delay between the instant when data leaves the source and when it arrives at its destination. The most common way to measure latency on data networks is by calculating a packet’s RTT (round trip time), or the length of time it takes for a packet to go from sender to receiver, then back from receiver to sender. RTT is usually measured in milliseconds. If packets experience varying amounts of delay, they can arrive out of order—a problem commonly called jitter, or more precisely, PDV (packet delay variation).
* Two important NIC settings include the direction in which signals travel over the media (duplex) and the number of signals that can traverse the media at any given time (multiplexing). To carry multiple signals, the medium’s channel is logically separated into multiple smaller channels, or subchannels. FDM (frequency division multiplexing) on copper cables assigns different frequencies to create multiple frequency bands, each used by a subchannel.
* Fiber-optic cables typically use WDM (wavelength division multiplexing), which divides a light beam into different wavelengths, DWDM (dense WDM), which increases the number of channels provided by normal WDM, and CWDM (coarse WDM), which lowers cost by spacing frequency bands wider apart to allow for cheaper transceiver equipment.

### Copper Cable

* Coaxial cable, called “coax” for short, was the foundation for Ethernet networks in the 1980s. Coax has been replaced by twisted-pair cable and fiber; however, RG-6 coax is still used for cable Internet, cable TV, and some multimedia connection types. An F-connector attaches to coaxial cable so that the pin in the center of the cable extends into the center of the connector. A BNC connector connects to another BNC connector via a turn-and-lock mechanism.
* Twinaxial cable, called “twinax” for short, looks very similar to coax cable except that there are two cores, or conductors, inside the cable. More recent twinax cables contain multiple pairs of these cores to carry even more data. Twinax is an inexpensive option for short, high-speed connections, such as when connecting switches to routers or servers in a data center. For this reason, twinax is also called a DAC (direct attach copper) cable. Twinax is factory terminated, usually with some of the same kinds of modular transceivers as what fiber terminations use. Depending on the connector type, twinax can support throughput up to 100 Gbps. However, the higher data rates require even shorter distance limitations in the range of 5–10 meters.
* Twisted-pair cabling in Ethernet networks contains four wire pairs. On Fast Ethernet networks, which have a maximum speed of 100 Mbps, one pair sends data, another pair receives data, and the other two pairs are not used for data transmission. Networks using Gigabit Ethernet and higher standards, with a speed of at least 1000 Mbps, use all four pairs for both sending and receiving.
* The TIA/EIA 568 standard divides twisted-pair wiring into several categories: Cat (category) 3, 5, 5e, 6, 6a, 7, 7a, and 8. Modern LANs use Cat 5e or higher wiring, which is the minimum required to support Gigabit Ethernet. Cat 6 and above are certified for multigigabit transmissions, although Cat 6 cable has shorter distance limitations when supporting 10 Gbps. While Cat 7/7a cables never gained significant popularity, Cat 8 cables are already widely available even for consumers and their home networks.
* STP (shielded twisted pair) cable consists of twisted-pair wires that are not only individually insulated, but might also be surrounded by a shielding made of a metallic substance such as a foil. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. UTP cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.
* TIA/EIA has specified two methods of inserting twisted-pair wires into RJ-45 plugs: TIA/EIA-568A and TIA/EIA-568B (also known as T568A and T568B, respectively). Functionally, there is very little difference between these two standards. You only must be certain that you use the same standard on every RJ-45 plug and jack on your network so data is transmitted and received correctly. T568B is more common and is likely what you’ll find on home and business networks. However, the federal government requires T568A on all federal contracts.
* The most common type of networking cable is a straight-through cable, also called a patch cable. To create one, terminate the RJ-45 plugs at both ends of the cable identically, following one of the TIA/EIA-568 standards. A crossover cable has the transmit and receive wires reversed and was used to connect a PC to a PC or a switch to a switch. Rollover cables, also called console cables, are used to connect a computer to the console port of a router.
* PoE (Power over Ethernet) is a method for supplying electrical power over twisted-pair Ethernet connections. The amount of power provided is relatively small—15.4 watts for standard PoE devices and 25.5 watts for the newer PoE+ devices. The PoE standard specifies two types of devices: PSE (power sourcing equipment) and PDs (powered devices). A switch or router that is expected to provide power over Ethernet must support the technology. Also, the end node must be capable of receiving PoE. On networks that demand PoE but don’t have PoE-capable equipment, you can add PoE adapters.
* A device’s NIC is rated for maximum network speeds, which are defined by various Ethernet standards. When two devices first connect, they auto-negotiate for the fastest standard they have in common, such as 10BASE-T, 100BASE-TX, 1000BASE-T, or 10GBASE-T.

### Fiber-Optic Cable

* Fiber-optic cable, or simply “fiber,” contains one or several glass or plastic fibers at its center, or core. Data is transmitted through the central fibers via pulsing light typically sent from a laser or an LED (light-emitting diode). SMF (single mode fiber) consists of a narrow core of 8 to 10 microns in diameter. Laser-generated light travels a single path over the core, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows SMF to accommodate the highest bandwidths and longest distances (without requiring repeaters) of all network transmission media.
* MMF (multimode fiber) contains a core with a larger diameter than SMF, usually 50 or 62.5 microns, over which many pulses of light generated by a laser or LED light source travel at various angles. Signals traveling over multimode fiber experience greater attenuation than those traversing single mode fiber. Therefore, MMF is not suited to distances longer than a few kilometers. On the other hand, MMF is less expensive to install and, therefore, typically used to connect routers, switches, and servers on the backbone of a network or to connect a desktop workstation to the network.
* The transition between SMF and MMF cabling might occur at an FDP (fiber distribution panel), which is usually a case on a rack where fiber cables converge, connect with each other, and connect with fiber-optic terminal equipment from the ISP. Splices at the FDP (or elsewhere on the network) might be accomplished by joining two fiber cables in a permanent bond using a fusion splicer, which melts the tips of two fibers together so light can pass cleanly through the joint, or various connectors might be used to create temporary splices.
* SMF connectors are designed to reduce back reflection, which is the return of the light signal back into the fiber that is transmitting the signal. Shapes and polishes currently used on SMF ferrules to reduce back reflection include UPC (ultra-physical contact) and APC (angled physical contact).
* SMF connectors are typically available with a 1.25-mm ferrule or a 2.5-mm ferrule, though other sizes can be found. The most common 1.25-mm ferrule connector is LC (local connector). Two 2.5-mm ferrules are SC (subscriber connector or standard connector) and ST (straight tip). The most common type of MMF connector is MT-RJ (mechanical transfer-registered jack).
* Common fiber transceivers include SFP (small form-factor pluggable), SFP+, QSFP (quad small form-factor pluggable), and QSFP+. SFP was the first to offer Gigabit Ethernet speeds with SFP+ improving on those speeds. QSFP was the first to squeeze four channels in a single transceiver to support significantly higher data rates. QSFP+ improved on this technology to offer even higher data rates.
* Long before IEEE developed a 10GBASE-T standard for twisted-pair cable, it had established standards for achieving high data rates over fiber-optic cable, which is the best medium for delivering high throughput. Common fiber Ethernet standards include 100BASE-FX, 100BASE-SX, 1000BASE-LX, 1000BASE-SX, 10GBASE-SR, and 10GBASE-LR.

### Cable Troubleshooting Tools

* You can start troubleshooting a network connection problem by checking the network connection LED status indicator lights on the network ports of the devices involved. A steady light indicates connectivity, and a blinking light indicates activity. A red or amber light might indicate a problem.
* A toner and probe kit can help determine where a wire, possibly out of hundreds, terminates. Tone generators and tone locators cannot be used to determine any characteristics about a wire, such as whether it’s defective or whether its length exceeds IEEE standards for a certain type of network. They are only used to determine where a wire terminates.
* A multimeter is a simple instrument that can measure many characteristics of an electric circuit, including its resistance, voltage, and impedance. You might use a multimeter to measure voltage to verify that a cable is properly conducting electricity, to check for the presence of noise on a wire, or to test for short or open circuits in the wire.
* A continuity tester determines whether a cable is carrying a data signal to its destination. Some continuity testers will verify that the wires in a UTP or STP cable are paired correctly following TIA/EIA 568 standards and that they are not shorted, exposed, or crossed. Continuity testers for fiber-optic cables issue light pulses on the fiber and determine whether they reach the other end of the fiber.
* A sophisticated cable performance tester measures the overall performance of a cabling structure. It allows you to perform the same continuity and fault tests as a continuity tester, but it can also be used to measure the distance to a connectivity device, termination point, or damage in a cable; measure attenuation along a cable; measure NEXT (near end crosstalk) between wires as well as alien crosstalk; measure termination resistance and impedance; issue pass/fail ratings for various categories of cabling standards; store and print cable testing results or directly save data to a computer database; and graphically depict a cable’s attenuation and crosstalk characteristics over the length of the cable.
* A sophisticated performance tester will include a TDR (time domain reflectometer). A TDR issues a signal on a cable and then measures the way the signal bounces back (or reflects) to the TDR. Performance testers for fiber-optic connections use OTDRs (optical time domain reflectometers). Rather than issue an electrical signal over the cable as twisted-pair cable testers do, an OTDR transmits light-based signals of different wavelengths over the fiber.
* An OPM (optical power meter), also called a fiber light meter, measures the amount of light power transmitted on a fiber-optic line. The device must be calibrated precisely, following highly accurate optical power standards set by the NIST. However, the surrounding room temperature, connection type, and skill of the technician conducting the test all affect the accuracy of the final test results.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 5-5b**Key Terms**

* [**1000BASE-LX**](javascript://)
* [**1000BASE-SX**](javascript://)
* [**1000BASE-T**](javascript://)
* [**100BASE-FX**](javascript://)
* [**100BASE-SX**](javascript://)
* [**100BASE-T**](javascript://)
* [**100BASE-TX**](javascript://)
* [**10BASE-T**](javascript://)
* [**10GBASE-LR**](javascript://)
* [**10GBASE-SR**](javascript://)
* [**10GBASE-T**](javascript://)
* [**40GBASE-T**](javascript://)
* [**APC (angled physical contact)**](javascript://)
* [**attenuation**](javascript://)
* [**auto-MDI-X**](javascript://)
* [**back reflection**](javascript://)
* [**bandwidth**](javascript://)
* [**bidirectional WDM**](javascript://)
* [**BNC connector**](javascript://)
* [**cable crimper**](javascript://)
* [**cable performance tester**](javascript://)
* [**cable stripper**](javascript://)
* [**cable tester**](javascript://)
* [**Cat 5 (Category 5)**](javascript://)
* [**Cat 5e (Enhanced Category 5)**](javascript://)
* [**Cat 6 (Category 6)**](javascript://)
* [**Cat 6a (Augmented Category 6)**](javascript://)
* [**Cat 7 (Category 7)**](javascript://)
* [**Cat 7a (Augmented Category 7)**](javascript://)
* [**Cat 8 (Category 8)**](javascript://)
* [**CFP (centum form-factor pluggable)**](javascript://)
* [**cladding**](javascript://)
* [**coaxial cable**](javascript://)
* [**console cable**](javascript://)
* [**continuity**](javascript://)
* [**continuity tester**](javascript://)
* [**crossover cable**](javascript://)
* [**CWDM (coarse wavelength division multiplexing or coarse WDM)**](javascript://)
* [**dB (decibel) loss**](javascript://)
* [**duplex**](javascript://)
* [**DWDM (dense wavelength division multiplexing or dense WDM)**](javascript://)
* [**encoding**](javascript://)
* [**Ethernet standards**](javascript://)
* [**Fast Ethernet**](javascript://)
* [**F-connector**](javascript://)
* [**FDM (frequency division multiplexing)**](javascript://)
* [**FDP (fiber distribution panel)**](javascript://)
* [**ferrule**](javascript://)
* [**fiber light meter**](javascript://)
* [**frequency**](javascript://)
* [**full-duplex**](javascript://)
* [**fusion splicer**](javascript://)
* [**Gigabit Ethernet**](javascript://)
* [**hot-swappable**](javascript://)
* [**impedance**](javascript://)
* [**jitter**](javascript://)
* [**latency**](javascript://)
* [**LC (local connector)**](javascript://)
* [**LED (light-emitting diode)**](javascript://)
* [**loopback adapter**](javascript://)
* [**MDI (medium dependent interface)**](javascript://)
* [**MDI-X (MDI crossover)**](javascript://)
* [**media converter**](javascript://)
* [**MMF (multimode fiber)**](javascript://)
* [**modal bandwidth**](javascript://)
* [**modulation**](javascript://)
* [**MT-RJ (mechanical transfer-registered jack)**](javascript://)
* [**multimeter**](javascript://)
* [**multiplexing**](javascript://)
* [**open circuit**](javascript://)
* [**OPM (optical power meter)**](javascript://)
* [**optical link budget**](javascript://)
* [**optical loss**](javascript://)
* [**OTDR (optical time domain reflectometer)**](javascript://)
* [**patch cable**](javascript://)
* [**pinout**](javascript://)
* [**plenum-grade cable**](javascript://)
* [**PoE (Power over Ethernet)**](javascript://)
* [**PoE+**](javascript://)
* [**QSFP (quad small form-factor pluggable)**](javascript://)
* [**QSFP+**](javascript://)
* [**repeater**](javascript://)
* [**RG-6**](javascript://)
* [**riser-rated cable**](javascript://)
* [**RJ-11 (registered jack 11)**](javascript://)
* [**RJ-45 (registered jack 45)**](javascript://)
* [**rollover cable**](javascript://)
* [**RTT (round trip time)**](javascript://)
* [**SC (subscriber connector or standard connector)**](javascript://)
* [**SFP (small form-factor pluggable)**](javascript://)
* [**SFP+**](javascript://)
* [**short circuit**](javascript://)
* [**SMF (single mode fiber)**](javascript://)
* [**snips**](javascript://)
* [**speed and duplex mismatch**](javascript://)
* [**ST (straight tip)**](javascript://)
* [**STDM (statistical time division multiplexing)**](javascript://)
* [**straight-through cable**](javascript://)
* [**TDM (time division multiplexing)**](javascript://)
* [**TDR (time domain reflectometer)**](javascript://)
* [**throughput**](javascript://)
* [**TIA/EIA-568A**](javascript://)
* [**TIA/EIA-568B**](javascript://)
* [**tone generator (or toner)**](javascript://)
* [**tone locator (or probe)**](javascript://)
* [**transceiver**](javascript://)
* [**twinaxial cable**](javascript://)
* [**twist ratio**](javascript://)
* [**twisted-pair**](javascript://)
* [**TX/RX reverse**](javascript://)
* [**UPC (ultra-physical contact)**](javascript://)
* [**WDM (wavelength division multiplexing)**](javascript://)
* [**wire cutter**](javascript://)
* [**wire map test**](javascript://)
* [**XFP (10 Gigabit small form-factor pluggable)**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 5-5c**Review Questions**

1. Which transmission characteristic is never fully achieved?
   1. Latency
   2. Throughput
   3. Bit rate
   4. Bandwidth
2. Which kind of crosstalk occurs between wire pairs near the source of the signal?
   1. Alien
   2. TX/RX reverse
   3. FEXT
   4. NEXT
3. Which kind of multiplexing assigns slots to nodes according to priority and need?
   1. WDM (wavelength division multiplexing)
   2. STDM (statistical time division multiplexing)
   3. TDM (time division multiplexing)
   4. CWDM (coarse wavelength division multiplexing)
4. Which cable is best suited for ultra-high-speed connections between a router and a switch on the same rack?
   1. RG-6 coaxial cable
   2. Cat 5e twisted-pair cable
   3. Cat 6 twisted-pair cable
   4. Passive twinaxial cable
5. Which of these categories of twisted-pair cable can support Gigabit Ethernet?
   1. Cat 5, cat 6, cat 7
   2. Cat 5e, cat 6, cat 3
   3. Cat 5e, cat 6a, cat 7
   4. Cat 6, cat 7a, cat 5
6. Suppose you’re creating patch cables to be used in a government office. What color wire goes in the first pin?
   1. White/orange
   2. White/green
   3. Brown
   4. Blue
7. What is the earliest twisted-pair cabling standard that meets the minimum requirements for 10GBASE-T transmissions at 100 meters?
   1. Cat 5e
   2. Cat 6
   3. Cat 6a
   4. Cat 7
8. What type of fiber-cable problem is caused when pairing a 50-micron core cable with a 62.5-micron core cable?
   1. Dirty connectors
   2. Wavelength mismatch
   3. Fiber type mismatch
   4. TX/RX reverse
9. Which part of a toner and probe kit emits an audible tone when it detects electrical activity on a wire pair?
   1. TDR
   2. Tone generator
   3. Tone locator
   4. Toner
10. Which fiber connector contains two strands of fiber in each ferrule?
    1. MT-RJ
    2. SC
    3. ST
    4. LC
11. How is latency measured, and in what unit?
12. What is a twist ratio, and why is it important?
13. What fiber is used in fiber-optic cabling to protect the inner core and prevent the cable from stretching?
14. What characteristic of optical transmission is primarily responsible for the distance limitations of fiber-optic cabling?
15. Why is SMF more efficient over long distances than MMF?
16. Why do APC ferrules create less back reflection than UPC ferrules?
17. Which fiber transceiver is the same size as SFP transceivers, but can support network speeds over 10 Gbps?
18. Suppose you’re assisting with a cable installation using fiber-optic cabling that will support Gigabit Ethernet. You’re approved to install segments up to 4000 m in length. What mode of fiber cable are you using?
19. What is the difference between short circuits and open circuits?
20. What kind of tool can measure the distance to the location of damage in a cable?

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 5-5d**Hands-On Projects**

**Note 5-12**

Websites and applications change often. While the instructions given in these projects were accurate at the time of writing, you might need to adjust the steps or options according to later changes.

**Note to Instructors and Students:** A rubric is provided for evaluating student performance on these projects. Please see Appendix D.

**Project 5-1**

### Latency around the World

* **Estimated Time:** 20 minutes (+5 minutes for group work, if assigned)
* **Objective:** Given a scenario, use the appropriate network software tools and commands. (Obj. 5.3)
* **Group Work:** This project includes enhancements when assigned as a group project.
* **Resources:**
  + Internet access
* **Context:** In [Module 4](javascript://), you learned that IP tracks the number of times a message jumps or hops from one router to another on its way to its destination. Each of these hops requires a tiny bit of time—the more routers a message must traverse, the longer it will take to reach its destination. In this module, you learned that latency is the delay caused by the time it takes messages to travel over network media from one place to another. This concept is easy to see in the real world, where it takes longer, for example, for you to travel across the country than it does to go down the street to the grocery store. Even though network messages travel much faster than a car or a jet plane, it still takes time for them to get from one place to another. And then the response must also travel across a similar number of hops, resulting in a longer RTT (round trip time). To see how distance affects a message’s RTT, complete the following steps:
  + 1

**For group assignments:** Open a PowerShell or Command Prompt window and run tracert on the IP address of one of your group members. If your group member is on the same LAN as you are, use their private IP address. If your group member is on a different network than you are, run tracert on their network’s public IP address. You and they both can discover your respective network’s public IP address using an IP address lookup tool online. Go to [google.com](http://google.com/" \t "_blank) and search for **What is my IP address**. The search results will list your network’s public IP address at the top. Now that you know your public IP address, share that information with your group member and get their public IP address as well. How many hops did it take for your tracert messages to reach your group member’s computer or network?

**Note 5-13**

For an Ubuntu or other Linux installation, use traceroute rather than tracert for this project. You might need to first install the traceroute utility. On Ubuntu, run this command:

The command used to install the trace route utility on Ubuntu operating system. sudo apt hyphen get install trace route.

* + 2

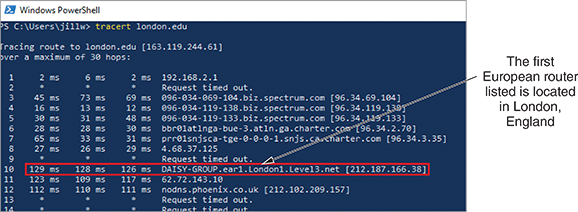
In a PowerShell or Command Prompt window, run tracert on a website whose servers are located on a different continent from your location—across one ocean. For example, if you’re located in the Midwest or Eastern United States, you can run the command **tracert london.edu** (London Business School). If you are on the West Coast, however, you might get more useful results for this step by targeting a server across the Pacific Ocean, such as **tracert** [www.tiu.ac.jp](http://www.tiu.ac.jp/" \t "_blank) (Tokyo International University). What command did you use?

* + 3

Examine the output and find the point in the route when messages started jumping across the ocean. By what percentage does the RTT increase after the jump compared with before it? You can see an example in [Figure 5-53](javascript://).

**Figure 5-53**

The latency time increases significantly as messages start to cross the ocean



To calculate the percentage for this jump, select a time from just after the jump (129, for example) and divide it by a time from just before the jump (such as 27), then multiply by 100 percent: . In this case, the sample data yields a 478 percent increase. It takes nearly five times as long for a message to go round-trip across the Atlantic from the United States to London, England (the location of this first European router), as it does for a message to travel round trip between two servers that are both located on the U.S. East Coast (this local computer and the last U.S. router in the route).

* + 4

Choose a website whose servers are on a continent even farther away from you. For example, if you are in the United States, you could trace the route to the University of Delhi in India at the address du.ac.in. What command did you use? How many hops did it take until the route crossed an ocean? What other anomalies do you notice about this global route?

* + 5

Choose one more website as close to directly across the globe from you as possible. U.S. locations might want to use the University of Western Australia at uwa.edu.au. What command did you use? How many hops are in the route? Did the route go east or west around the world from your location? How can you tell?

* + 6

Scott Base in Antarctica runs several webcams from various research locations. Run a trace to the Scott Base website at **antarcticanz.govt.nz**. What’s the closest router to Scott Base’s web server that your trace reached? If you can’t tell from the command output where the last response came from, go to [iplocation.net](http://iplocation.net/" \t "_blank) in your browser. Enter the final hop’s IP address to determine that router’s location.

* + 7

Think about other locations around the world that might be reached through an interesting geographical route, such as traversing a place you would like to visit or tapping routers in an exotic location. Find a website hosted in that location and trace the route to it. Which website did you target? Where is it located? What are some router locations along the route of your trace? **Take a screenshot** of the output for your trace; submit this visual with your answers to this project’s questions.

* + 8

Try the ping command on several of these same IP addresses. Did it work? Why do you think this is the case?

**Project 5-2**

### Create a Loopback Plug

* **Estimated Time:** 30 minutes
* **Objective:** Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. (Obj. 5.2)
* **Resources:**
  + 6-inch length of UTP cabling (Cat 5 or Cat 5e)
  + Unused RJ-45 plug
  + Wire cutters, snips, or heavy-duty scissors
  + Cable crimper

**Note:** This hardware can be purchased in bulk and distributed to students. Alternatively, students can purchase their own supplies at stores such as Lowe’s, Home Depot, [Amazon.com](http://amazon.com/" \t "_blank), or [Newegg.com](http://newegg.com/" \t "_blank).

* **Context:** In this module, you practiced terminating an Ethernet cable by attaching an RJ-45 connector. You also learned that a loopback plug crosses the transmit line with the receive line to trick a device into thinking it’s connected to a network. You can create your own loopback plug by altering the pinout on the connector and forcing the transmissions to loop back in on themselves. A loopback plug is helpful for determining if a NIC on a workstation or a port on a switch is working or not. Complete the following steps:
  + 1

Cut to loosen the cable’s covering, then slide the covering off the cable to separate the wire pairs into four groups. Flatten the wire pairs but do not untwist them. Select one wire pair (one solid and one striped) and lay the other pairs aside because you won’t need them. Which wire pair did you choose?

* + 2

Untwist the wires on each end an inch or less and straighten the tips. If needed, give each wire a clean cut to make sure the two wires on each end are even with each other.

* + 3

Insert one end of the twisted pair into the RJ-45 plug, making sure the solid color wire goes into slot 1, and the striped wire goes into slot 2. Push the wires all the way into the slots. Make sure the wire tips touch the plastic surface at the front end inside the plug.

* + 4

Loop the wire pair around and insert the other end into the plug. The solid color wire goes into slot 3, and the striped wire goes into slot 6. (Slots 4, 5, 7, and 8 are not needed unless you’ll be testing Gigabit Ethernet equipment.)

**Note 5-14**

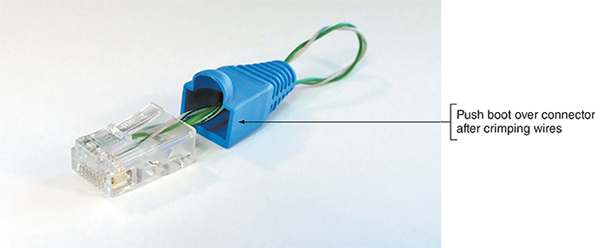
If you want to include the other two pins in the adapter so you can test VoIP and similar Gigabit Ethernet equipment, you’ll need to use a second twisted pair from your original cable. Before crimping, insert one end of the second pair into the plug. Press the solid color wire into slot 4 and the striped wire into slot 5. Loop the wire around and press the solid color wire into slot 7 and the striped wire into slot 8.

* + 5

Push the wires all the way in and then use the crimper to secure the wires in the plug. If a boot came with the plug, you can insert it over the wire loop and push it all the way through to cover the wire/plug connection, as shown in [Figure 5-54](javascript://). **Take a photo of your loopback plug**; submit this visual with your answers to this project’s questions.

**Figure 5-54**

Adding the boot to the loopback plug is optional



Enlarge Image

* + 6

Insert the loopback plug into a device’s Ethernet port that is known to be working correctly and has LED indicator lights. If the port’s link indicator lights up (this might take a minute), you’ve successfully created a loopback plug.

* + 7

Working with the actual hardware can be an enlightening experience as you work to get each wire lined up with the correct pin or realize how much force is required to crimp a cable inside the connector. What was the most difficult part of this project for you? What was the most satisfying part of the project?

**Project 5-3**

### Create a Loopback Jack

* **Estimated Time:** 20 minutes
* **Objective:** Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. (Obj. 5.2)
* **Resources:**
  + 2-inch length of UTP cabling (Cat 5 or Cat 5e)
  + Unused RJ-45 data/phone jack
  + Punchdown tool

**Note:** This hardware can be purchased in bulk and distributed to students. Alternatively, students can purchase their own supplies at home improvement stores such as Lowe’s, Home Depot, [Amazon.com](http://amazon.com/" \t "_blank), or [Newegg.com](http://newegg.com/" \t "_blank).

* **Context:** A loopback plug can be used to test a port on a switch or a workstation’s NIC. A loopback jack, however, can be used to test a cable or to identify which port a cable is connected to. This is especially helpful when the cable is already run through the wall or is tangled up with other cables. Creating a loopback plug is pretty straightforward, and wiring a loopback jack is even easier. Complete the following steps:
  + 1

Cut to loosen the cable’s covering, then slide the covering off the cable to separate the wire pairs into four groups. Flatten the wire pairs but do not untwist them. Select one wire pair (one solid and one striped) and lay the other pairs aside because you won’t need them. Which wire pair did you choose?

* + 2

Turn the jack so the slots are easily accessible. Take a single wire and press one end into the slot next to the “A–green/white” icon. Press the other end into the slot with the “A–orange/white” icon.

**Note 5-15**

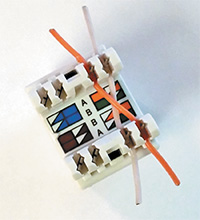
There is some variation in how RJ-45 jacks are designed. If these generic directions don’t match the jack you’re using, check the documentation that came with the jack.

* + 3

Take the other, single wire, press one end into the slot next to the “A–orange” icon, and press the other end into the slot next to the “A–green” icon. In some cases, depending on the actual jack you use, the two wires will create an “X” shape through the center of the jack between the slots, as shown in [Figure 5-55](javascript://). With other jacks, the wires might cross over each other on one side only. **Take a photo of the pinout for your loopback jack**; submit this visual with your answers to this project’s questions.

**Figure 5-55**

With this jack, the wires cross in the middle

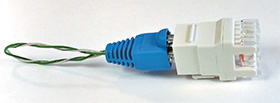


* + 4

Use the punchdown tool to punch the wires all the way into their respective slots. The punchdown tool will also clip the excess length off the wires. Make sure to orient the punchdown tool so the cutting side will slice the outside length of the wire and not the inside length. If a cover came with the jack, place it over the wires.

* + 5

To test your loopback jack, plug a patch cable you know to be good into a device’s Ethernet port that you know works, then plug the jack onto the other end of the cable. Wait up to a minute to give the link sufficient time to be established. If the port’s link indicator lights up, you’ve successfully created a loopback jack.

* For storage, you can plug your loopback plug into your loopback jack (see [Figure 5-56](javascript://)), giving you a handy two-in-one tool for your toolkit.
* **Figure 5-56**
* Attach the plug and jack together to protect their connections when storing them
* 

**Project 5-4**

### Test a LAN’s Speed and Throughput

* **Estimated Time:** 45 minutes (+5 minutes for group work, if assigned)
* **Objective:** Given a scenario, use the appropriate statistics and sensors to ensure network availability. (Obj. 3.1)
* **Resources:**
  + Windows 10 or macOS computer with administrative access

Internet access

* + A second Windows 10 or macOS computer on the LAN with administrative access and with a shared folder

**Note:** At least one of these two computers should have a wired connection to the network. Optionally, to test a fully wired network connection between two computers, make sure both computers have a wired connection to the network rather than a Wi-Fi connection on one of them.

**Note:** For the second part of this project, the second device could instead be an Android or iOS mobile device. For students who are working from home and don’t have a second computer, they can complete Steps 8-13.

* **Context:** A variety of software and web-based tools are available to help you establish baseline measurements—and later, detect fluctuations and problems—in the efficiency of your network and Internet connections. This project walks you through two different tests you can perform on your school’s lab network or at home on your own LAN. Complete the following steps:
  + 1

TotuSoft’s LAN Speed Test is a simple, free program that only needs access to a shared folder on the local area network to test throughput speeds on the network. The Public Users folder on another workstation meets this requirement. Check to make sure you have access to a shared folder on another computer on your network. For example, on a Windows 10 computer, open File Explorer and click **Network** in the navigation pane. If you have access to a shared folder, the computer should appear in the list of networked devices. You should be able to navigate into that computer’s folders to locate the shared folder. If you don’t already have a shared folder on another computer, do some research online for that computer’s OS to determine how to share a folder with everyone on the local network.

* + 2

**For group assignments:** Create a folder on your computer for a group member to test against. Share that folder with your group member. Check to make sure you have access to their shared folder.

* + 3

Go to [totusoft.com](http://totusoft.com/" \t "_blank). Download and install the latest version of **LAN Speed Test**.

* + 4

Launch LAN Speed Test. Close the screen asking you to register—registration is not required to use the free version. The app will automatically detect your own computer’s IP address. Note that if your computer also has a hypervisor installed, you might need to change the MAC field to the physical NIC’s MAC address in order to see the computer’s IPv4 address on the physical network.

* + 5

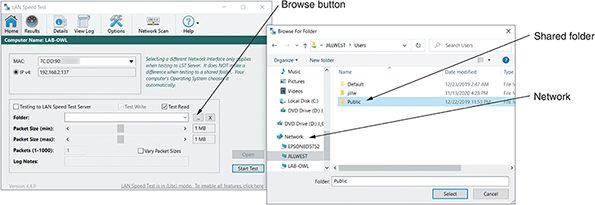
Before running the test, answer the following questions:

* + 1. What network media connects your computer to your network?
    2. If this is a wired connection, what is the cable’s category rating? Based on this information, what is the maximum throughput the cable supports?
    3. What network media connects the target computer to your network?
    4. If this is a wired connection, what is the cable’s category? Based on this information, what is the maximum throughput the cable supports?
  + 6

Next to the Folder field, click the **Choose Folder/Server to test** to button (which contains three dots), and locate the shared folder on another workstation or server on your network, as shown in [Figure 5-57](javascript://). Select the folder as the target and click **Start Test**.

**Figure 5-57**

Browse to a shared folder on another computer on your network



Enlarge Image

Source: TotuSoft

* + 7

When the test has finished running, answer the following questions:

* + 1. How do your test results for upload and download speeds compare with the maximum supported throughput for your cables?
    2. If your test results differ from the standards you were expecting, how do you explain these results?

TamoSoft, another security and network monitoring software company, offers a free Throughput Test that works on both wired and wireless LAN connections on computers (Windows and macOS) or mobile devices (Android and iOS). Complete the following steps:

* + 1

Go to [tamos.com](http://tamos.com/" \t "_blank) and find the free Throughput Test on the Download page. Download and install it on two devices (computer or mobile device) on the same LAN, accepting default settings in the setup wizard.

* + 2

One device will act as the client and one as the server.

* + 1. On the server device, click **Start** and, in the Start menu, click **Run Server**. If necessary, click **Yes** in the UAC dialog box.
    2. On the client device, click **Start** and, in the Start menu, click **Run Client**. If necessary, click **Yes** in the UAC dialog box.

**Note 5-16**

If Run Server and Run Client are not visible at the top of the Start menu on a Windows 10 computer, scroll down and click to expand TamoSoft Throughput Test. Then click Run Server or Run Client, respectively.

* + 3

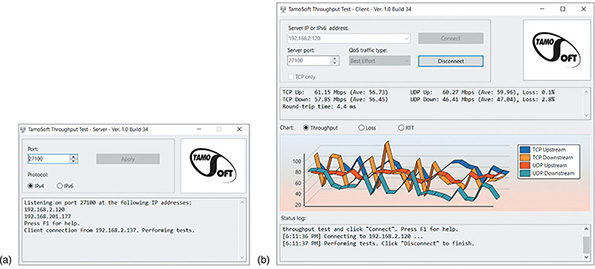
On the device acting as the server, note its IP address, which is reported automatically in the TamoSoft Throughput Test window. Note that if you’re running the server software on a computer with Hyper-V activated, you might see two IP addresses: one for the physical network and one for the virtual network. You need the IP address for the physical network for this project. Nothing more is needed on this end of the connection because the server only needs to listen for the client.

* + 4

On the device acting as the client, enter the server’s IP address, then click **Connect**. [Figure 5-58](javascript://) shows the server and client consoles side by side. **Take a screenshot** of your client console while the test is running; submit this visual with your answers to this project’s questions.

**Figure 5-58**

Server (a) and client (b) consoles for Throughput Test, with results showing on the client side



Enlarge Image

Source: TamoSoft

* + 5

In the Chart pane, TCP and UDP throughput are monitored. Upstream refers to traffic moving from the client device to the server device. Downstream refers to traffic moving from the server device to the client device. Other charts include Loss and RTT. Let the test run for a couple of minutes, then click **Disconnect**. Examine the results and answer the following questions.

* + 1. On the Throughput chart, what was the highest reading obtained, and what kind of traffic was it?
    2. On the Loss chart, were there any significant loss results, and what kind of traffic was involved? What theories do you have about why this might be? Where would you look next to resolve this problem?
    3. On the RTT (round trip time) chart, were there any spikes? Do you notice any correlation between the timing of the spikes on this chart and the timing of problem indicators on the other two charts?
  + 6

Document both these application installations in your wikidot website.

Go to pg.

[**help**](javascript://)