Solution and Answer Guide

Jill West, CompTIA Network+ Guide to Networks, 9th Edition, ISBN: 9780357508138; Module 5: Cabling

Table of Contents

Text

Applying Concepts

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, 5-23, and 5-24, respectively. Alternatively, you can use a single device that contains all three of these tools. A wire cutter is a pliers-shaped tool, and snips are more like heavy-duty scissors; both can make a clean cut through a cable. A cable stripper pulls off the protective covering without damaging the wires inside. A cable crimper 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.

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 to match Figure 5-20 or Figure 5-21, 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. 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.
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.
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. Cut off the excess string and sheath.

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.

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. 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?

   Answer: Either T568A or T568B may be chosen. Wire positions should follow the standard chosen:

   T568A: White/green, green, white/orange, blue, white/blue, orange, white/brown, brown

   T568B: White/orange, orange, white/green, blue, white/blue, green, white/brown, brown

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, it might help to hold the RJ-45 connector next to the wires to determine how short to cut the wires.

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.

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.

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). 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.

10. Repeat Steps 2 through 9 for the other end of the cable. After completing Step 9 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.

Review Questions

1. Which transmission characteristic is never fully achieved?

a. Latency

b. Throughput

c. Bit rate

d. Bandwidth

Answer: d. Bandwidth

Explanation: **Bandwidth** refers to the amount of data you could theoretically transmit during a given period of time but is never fully achieved. Latency describes the brief delay that takes place between the instant when data leaves the source and when it arrives at its destination. Throughput refers to the number of data bits (0s and 1s) that are actually received across a connection each second. Throughput is also called bit rate.

2. Which kind of crosstalk occurs between wire pairs near the source of the signal?

   a. Alien

   b. TX/RX reverse

   c. FEXT

   d. NEXT

   Answer: d. NEXT

   Explanation: **NEXT (near end crosstalk)** occurs between wire pairs near the source of a signal. Alien crosstalk occurs between two cables. FEXT (far end crosstalk) is measured at the far end of the cable from the signal source. A TX/RX (transmission/receive) reverse occurs when the TX and RX wires are crossed.

3. Which kind of multiplexing assigns slots to nodes according to priority and need?

   a. WDM (wavelength division multiplexing)

   b. STDM (statistical time division multiplexing)

   c. TDM (time division multiplexing)

   d. CWDM (coarse wavelength division multiplexing)

   Answer: b. STDM (statistical time division multiplexing)

   Explanation: **STDM (statistical time division multiplexing)** assigns time slots to nodes (similar to TDM) but then adjusts these slots according to priority and need. TDM (time division multiplexing) divides a channel into multiple intervals of time, or time slots. WDM (wavelength division multiplexing) carries multiple light signals simultaneously by dividing a light beam into different wavelengths, or colors, on a single fiber. CWDM (coarse wavelength division multiplexing) lowers cost by spacing frequency bands wider apart to allow for cheaper transceiver equipment.

4. Which cable is best suited for ultra-high-speed connections between a router and a switch on the same rack?

    a. RG-6 coaxial cable

    b. Cat 5e twisted-pair cable

    c. Cat 6 twisted-pair cable

    d. Passive twinaxial cable

    Answer: d. Passive twinaxial cable

    Explanation: Twinax an inexpensive option for short, high-speed connections, such as when connecting switches to routers or servers in a data center; **passive twinax** is sufficient for the shortest distances of less than about 5 or 7 meters. RG-6 coaxial cables is used to deliver broadband cable Internet service and cable TV, particularly in the last stretch to the consumer's location. Cat 5e and cat 6 twisted-pair cable have more limited available throughput than twinax.

5. Which of these categories of twisted-pair cable can support Gigabit Ethernet?

    a. Cat 5, cat 6, cat 7

    b. Cat 5e, cat 6, cat 3

    c. Cat 5e, cat 6a, cat 7

    d. Cat 6, cat 7a, cat 5

    Answer: c. Cat 5e, cat 6a, cat 7

    Explanation: **Cat 5e** is the minimum category of twisted-pair cable that supports Gigabit Ethernet. **Cat 6a** and **cat 7** also support Gigabit speeds or higher.

6. Suppose you're creating patch cables to be used in a government office. What color wire goes in the first pin?

    a. White/orange

    b. White/green

    c. Brown

    d. Blue

Answer: b. White/green

Explanation: The federal government requires T568A on all federal contracts for backward-compatibility. Pin 1 in the T568A pinout takes the **white and green striped** wire.

7. What is the earliest twisted-pair cabling standard that meets the minimum requirements for 10GBASE-T transmissions at 100 meters?

    a. Cat 5e

    b. Cat 6

    c. Cat 6a

    d. Cat 7

    Answer: c. Cat 6a

    Explanation: While cat 6 cable can support 10 Gbps speeds at shorter distances, **cat 6a** is the first category of cable rated for 10 Gbps at 100 meters.

8. What type of fiber-cable problem is caused when pairing a 50-micron core cable with a 62.5-micron core cable?

    a. Dirty connectors

    b. Wavelength mismatch

    c. Fiber type mismatch

    d. TX/RX reverse

    Answer: c. Fiber type mismatch

    Explanation: Same-mode cables can be mismatched if the cores have different widths; a cable with a 50-micron core should not be connected to a cable with a 62.5-micron core, even though they're both MMF, as this results in a **fiber type mismatch**. Signal loss and other errors can be caused by dirty connectors. A wavelength mismatch occurs when transmissions are optimized for one type of cable but sent over a different type of cable. A TX/RX (transmission/receive) reverse occurs when the TX and RX wires are crossed in a twisted-pair cable.

9. Which part of a toner and probe kit emits an audible tone when it detects electrical activity on a wire pair?

    a. TDR

    b. Tone generator

c. Tone locator

d. Toner

Answer: c. Tone locator

Explanation: A **tone locator**, or probe, emits an audible tone when it detects electrical activity on a wire. A tone generator, or toner, issues a signal on a wire that is then detected by the tone locator. A TDR (time domain reflectometer) issues a signal on a cable and then measures the way the signal bounces back (or reflects) to the TDR.

10. Which fiber connector contains two strands of fiber in each ferrule?

    a. MT-RJ

    b. SC

    c. ST

    d. LC

    Answer: a. MT-RJ

    Explanation: The **MT-RJ** connector is unique from SC, ST, and LC connectors 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.

11. How is latency measured, and in what unit?

    Answer: Latency is measured by calculating a packet's RTT, 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.

12. What is a twist ratio, and why is it important?

    Answer: Twist ratio is the number of twists per meter or foot. The more twists per foot in a pair of wires, the more resistant the pair will be to crosstalk or noise.

13. What fiber is used in fiber-optic cabling to protect the inner core and prevent the cable from stretching?

    Answer: To prevent the cable from stretching, and to protect the inner core further, strands of Kevlar (a polymeric fiber) surround the plastic buffer.

14. What characteristic of optical transmission is primarily responsible for the distance limitations of fiber-optic cabling?

    Answer: Optical loss

15. Why is SMF more efficient over long distances than MMF?

    Answer: The core of SMF is much narrower than that of MMF and reflects very little. The light does not disperse as much along the fiber.

16. Why do APC ferrules create less back reflection than UPC ferrules?

    Answer: The end faces are placed at an angle to each other, and the reflection is sent back in a different direction than the source of the signal.

17. Which fiber transceiver is the same size as SFP transceivers, but can support network speeds over 10 Gbps?

    Answer: SFP+ transceivers are the same module size as SFP; theoretical maximum transmission speed is 16 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?

    Answer: SMF

19. What is the difference between short circuits and open circuits?

    Answer: A short circuit is one where connections exist in places they shouldn't, while an open circuit is one where needed connections are missing.

20. What kind of tool can measure the distance to the location of damage in a cable?

    Answer: Answers may include cable performance tester, line tester, certifier, or network tester.

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.

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, 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** 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?

   Answer: Answers may vary. For group members on the same LAN, usually one hop is sufficient. For group members working from different networks, the number of hops will be higher.

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:

sudo apt-get install traceroute

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** (Tokyo International University). What

command did you use?

Answer: Answers may vary and should include a tracert or traceroute command targeting a website across one ocean from the student's geographical location.

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.

   Answer: Answers may vary and should be significantly above 100 percent.

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: 129/27 × 100% = 478%. 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?

   Answer: Answers may vary and should include a tracert or traceroute to a location more than one ocean away from the student's geographical location.

   Answer: Answers may vary and should include a relatively low number of hops, such as 8, 10, or 12.

   Answer: There may or may not be noticeable anomalies at this point. Examples might include the direction of travel for the trace's messages (such as going east instead of west), the point at which the trace crossed each ocean, or other countries the route traversed.

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?

   Answer: Answers may vary and should include a tracert or traceroute to a location directly opposite the global position of the student's geographical location.

   Answer: Answers may vary and should include a relatively high number of hops, such as 20 or 30, which is the default maximum for tracert and traceroute.

Answer: Answers may vary. You can tell which direction the trace went by examining the locations of routers along the way.

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** in your browser. Enter the final hop's IP address to determine that router's location.

   Answer: Answers may vary and should list a router's location in or near New Zealand, which is where the web server is located.

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.

   Answer: Answers may vary and should list a target website, its location, and locations of routers along the way.

   Answer: Screenshot should show a trace to a website in an interesting location or that is reached through an interesting route (such as going through African routers located in sparsely populated areas, attempting to find a route that crosses Paris, or finding a route that traverses extreme northern Russia).

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

   Answer: Both ping and tracert use ICMP messages, which are very low priority and are often blocked by firewalls. The tracert utility, however, sends multiple echo request messages with incremental TTL increases. Even though the final message might be turned away by the destination's firewall, the shorter lifespan messages earlier in the process still trigger responses from routers along the route to the destination. Tracert relies on these router responses to build its output, not necessarily on a response from the destination's server. However, ping depends only on the destination's server responding.

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, or Newegg.com.

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?

   Answer: Answers may vary and could include any one of the following: green and green-striped pair, blue and blue-striped pair, orange and orange-striped pair, or brown and brown-striped pair.

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. **Take a photo of your loopback plug**; submit this visual with your answers to this project's questions.

   Answer: Photo should show one wire pair looped into a single RJ-45 connector, similar to the one shown in Figure 5-54.

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?

   Answer: Answers will vary widely. Students often struggle with lining up the pins correctly, inserting the wires deeply enough into the connector, and applying enough force with the crimper to adequately penetrate the wires inside the connector. In contrast, it can be informative and rewarding to open up a cable to see what's inside, to finally get the wires lined up correctly inside the connector, and to see the loopback plug successfully activate a network port.

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, or Newegg.com.

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?

   Answer: Answers may vary and could include any one of the following: green and green-striped pair, blue and blue-striped pair, orange and orange-striped pair, or brown and brown-striped pair.

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. 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.

   Answer: Photo should show two wires inserted into the pins on the loopback jack. Exact wiring will vary depending on jack design. The pinout should show one wire connecting the green/white labeled pin to the orange/white labeled pin and the other wire connecting the orange labeled pin to the green labeled pin.

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), giving you a handy two-in-one tool for your toolkit.

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
- 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.

- Internet access

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**. 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:

    a. What network media connects your computer to your network?

Answer: Answers may vary and should identify either a wired or wireless connection.

    b. 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?

Answer: Answers may vary. For a wired connection, answer should include the cable's category rating and maximum supported throughput according to Table 5-3 earlier in the module.

    c. What network media connects the target computer to your network?

Answer: Answers may vary and should identify either a wired or wireless connection.

    d. If this is a wired connection, what is the cable's category? Based on this information, what is the maximum throughput the cable supports?

Answer: Answers may vary. For a wired connection, answer should include the cable's category rating and maximum supported throughput according to Table 5-3 earlier in the module.

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. Select the folder as the target and click **Start Test**.

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

    a. How do your test results for upload and download speeds compare with the maximum supported throughput for your cables?

Answer: Answers may vary. Reported speeds should be less than the theoretical throughput given in Step 4 above.

b. If your test results differ from the standards you were expecting, how do you explain these results?

Answer: Answers may vary and might include concerns related to the router or switch on the LAN, capabilities of the computers used, or quality of the cables used.

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:

8. Go to **tamos.com** 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.

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

   a. On the server device, click **Start** and, in the Start menu, click **Run Server**. If necessary, click **Yes** in the UAC dialog box.

   b. 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.

10. 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.

11. On the device acting as the client, enter the server's IP address, then click **Connect**. Figure 5-58 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.

    Answer: Screenshot should show TamoSoft Throughput Test Client console with a test in progress.

12. 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.

a. On the Throughput chart, what was the highest reading obtained, and what kind of traffic was it?

Answer: Answers may vary, and the traffic type could be TCP Upstream, TCP Downstream, UDP Upstream, or UDP Downstream.

b. 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?

Answer: Answers may vary and could include UDP Upstream Loss or UDP Downstream Loss. Theories and solutions might address concerns regarding the computers' NICs, connectivity devices, or cabling.

c. 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?

Answer: Answers may vary. Spikes might have corresponded somewhat to low throughput or high losses.

Document both these application installations in your wikidot website.

Capstone Projects

Note 5-17

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.

Capstone Project 5-1: Decode a TCP Segment in a Wireshark Capture

Estimated time: 45 minutes

Objective: Given a scenario, use the appropriate network software tools and commands. (Obj. 5.3)

Resources:

- Windows 10 computer with administrative access and Wireshark installed
- Internet access

Context:

In Module 2, you installed Wireshark and examined several messages in your capture. In Module 4, you dissected sample headers captured by Wireshark to interpret the fields included in each header. In this project, you'll pull these concepts together and use Wireshark to capture your own DNS messages, examine TCP headers in a TCP stream, and practice interpreting the information that you find. Complete the following steps:

1. Open Wireshark and snap the window to one side of your screen. Open a browser and snap that window to the other side of your screen so you can see both windows.

Note 5-18

In Windows, you can quickly snap the active window to one side of your screen by pressing the Win key with the left or right arrow key. Alternatively, you can drag a window to one edge of your screen until it snaps into position.

2. Before starting your capture, clear your browser's DNS cache so you can capture a DNS query. To do this, you need to access the net-internals page for the browser. For example, in Edge's address bar, enter **edge://net-internals/#dns** and then click **Clear host cache**. Similarly, in Chrome, enter **chrome://net-internals/#dns** and click **Clear host cache**. For other browsers, do some research online to find more specific instructions to clear the browser's DNS cache.

3. You'll also need to clear your computer's DNS cache. In a PowerShell or Command Prompt window, enter **ipconfig /flushdns**.

4. Start the Wireshark capture on your active network connection. In the browser, navigate to either **nasa.gov/nasalive** or **explore.org/livecams**—if you've visited one of these sites recently, choose the other one. Once the page loads, stop the Wireshark capture. You'll have fewer messages to sort through if you can do this entire process fairly quickly.

Somewhere in your capture, a DNS message will show the original request to resolve the name *nasa.gov* or *explore.org* to its IP address. A series of TCP messages after that will show the three-way handshake, along with the rest of the data transmission. Because your transmission has to do with DNS and then requesting a secure web page using HTTPS, you need to filter first to DNS and then to TCP port 443. Complete the following steps:

5. Apply the following filter to your capture to expose the messages involved with your DNS request: **dns**

6. The correct DNS messages show DNS in the Protocol field and something to the effect of "Standard query" and "**www.nasa.gov**" or "explore.org" in the Info field, as shown in Figure 5-59. Notice that in this capture, the local computer made a DNS query to its primary (1.1.1.1) DNS server to resolve the domain name.

7. Once you've located the message querying the DNS server, click on it and examine the details of the message in the second pane. Answer the following questions:

    a. What is the OUI of the source's NIC?

    Answer: Answers may vary and should list a six-character number from the beginning of a MAC address, such as 7C:DD:90.

    b. Which IP version was used?

    Answer: In most cases, the IP version is 4, although some responses might list IP version 6.

    c. If the message used IPv4, what was the TTL? If IPv6, what was the hop limit?

    Answer: Answers may vary. The default TTL or hop limit for Windows is 128; therefore, most answers will give 128.

    d. Did the message use TCP or UDP?

    Answer: Most DNS requests will use UDP.

    e. What is the source port? The destination port?

    Answer: The source port will vary widely and will likely be a random 5-digit number, such as 53,562. The DNS destination port is almost always 53.

    f. What DNS record type is requested?

    Answer: In most cases, an A record is requested.

8. With the DNS message selected, update your filter to **dns or tcp.port eq 443**.
9. Check your filter results for the first [SYN] message after the selected DNS request. Open the TCP segment header in the second pane. Make sure the Sequence Number (relative sequence number) is 0, as shown in Figure 5-60. If it's not, try the next SYN message. When you find the first SYN message after the DNS message and with a Sequence Number (relative sequence number) of 0, check the TCP flags. Which flags are set in the TCP segment?

    Answer: In most cases, the only flag set will be SYN.

Wireshark shows relative sequence numbers and also the raw numbers used in the segments themselves. Relative numbers are easier for humans to keep up with, but they provide no security in that they're very predictable. Random numbers, on the other hand, are more difficult to fake.

10. Apply another filter layer to show only the messages for this TCP conversation. To do this, right-click the **[SYN]** message you selected earlier, point to **Follow**, and click **TCP**

Stream. Close the Follow TCP Stream dialog box that opens, as you will be examining data in the actual capture.

11. Immediately after that initial [SYN] message, locate the [SYN, ACK] message and answer the following questions:

    a. What is the source IP address? The destination IP address?

    Answer: The source IP address should be a public IP address, and the destination IP address should be a private IP address.

    b. In the TCP header, what is the relative sequence number? The relative acknowledgment number?

    Answer: The relative sequence number is 0, and the relative acknowledgment number is 1.

    c. Which TCP Flags are set?

    Answer: In most cases, the set flags will be Syn and Acknowledgment.

12. Locate the third message in this three-way handshake, the [ACK] message, and answer the following questions:

    a. What is the source IP address? The destination IP address?

    Answer: The source IP address should be a private IP address, and the destination IP address should be a public IP address.

    b. In the TCP header, what is the relative sequence number?The relative acknowledgment number?

    Answer: The relative sequence number is 1, and the relative acknowledgment number is 1.

    c. Which flags are set in the TCP segment?

    Answer: In most cases, the only flag set will be Acknowledgment.

13. The three-way handshake establishes the session, but the conversation continues as the web server begins to respond to your browser's request for the web page. First, the web server redirects the conversation to a secure website using HTTP over SSL/TLS. Look for a series of messages listing TLS in the Protocol field. Locate the Client Hello and Server Hello messages, as shown in Figure 5-61. A few lines below that, locate the Certificate and Server Key Exchange message where the server completes its Hello process or the Change Cipher Spec message where a new set of encryption keys is requested. **Take a screenshot** of your capture showing these messages; submit this visual with your answers to this project's questions.

Answer: Screenshot should show a Wireshark capture with the tcp.stream filter applied, the Client Hello Server Hello messages, and either the Certificate and Server Key Exchange message or the Change Cipher Spec message.

14. Soon after this key exchange, you'll see several messages using the TLS protocol that are labeled Application Data. Look at the Length field for these messages. What is the size of the longest message listed?

    Answer: Answers may vary. In most cases, the longest message will be 1484, 1504, or 1514.

15. Click on one of the longest messages and answer the following questions:

    a. List the types of headers included in this message, in order.

    Answer: In most cases, the layers will be Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security.

    b. What is the source IP address? The destination IP address?

    Answer: The source IP address should be a public IP address, and the destination IP address should be a private IP address.

    c. In the TCP header, which flags are set in the TCP segment?

    Answer: In most cases, the only flag set will be Acknowledgment.

Capstone Project 5-2: Build a Packet Tracer Network

Estimated time: 1 hour

Objective: Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. (Obj. 1.1)

Resources:

- Computer with Cisco Packet Tracer installed
- Storage space for Packet Tracer network file to be accessed in later modules

Context:

In Capstone Project 2-2 in Module 2, you installed Packet Tracer and completed several modules in the Introduction to Packet Tracer course. In Module 3, you worked with MAC address tables in Packet Tracer. And in Module 4, you set up a TFTP server in Packet Tracer. Look back at your notes on your Wikidot website if you need help remembering details about what you learned in these earlier projects. In this project, you will begin to build a more extensive network, and you'll continue building on this network in future modules. Make sure you're working on a computer where you'll be able to save your Packet Tracer network file for later use, either by working on the same computer every time or by saving your file in the cloud where you can get to it later. The Packet Tracer network you begin building in this project is the starting point for many additions to this network in later modules. To begin building your more extensive Packet Tracer network, complete the following steps:

1. Open **Packet Tracer** and, if necessary, sign in with your Networking Academy account.
2. Add one **PT-Router** to the workspace.
3. Add two **2960 switches** to the workspace.
4. Add two **PCs** to the workspace.
5. Arrange these devices in a pyramid shape, with the workstations at the bottom, the switches in the middle, and the router at the top. See Figure 5-62 to get an idea of the correct layout. Use the **Copper Straight-Through** connection to connect each of these devices as described next:

    a. On each workstation, connect the Ethernet cable to the **FastEthernet0** interface.

    b. On each switch, connect the Ethernet cable from the workstation to the **FastEthernet0/1** interface. Connect the Ethernet cable to the router to the **FastEthernet0/2** interface.

    c. On the router, connect Switch0 to the **FastEthernet0/0** interface, and connect Switch1 to the **FastEthernet1/0** interface.

    d. Wait a few minutes for the workstation-to-switch connections to turn to green triangles on both ends of each connection.

The router and the switch must be configured for the connections to come up:

6. Click **Router0** to open its configuration window. Click the **Config** tab. As you make changes, notice the commands that show up in the Equivalent IOS Commands pane at the bottom of the window.
7. Click the **FastEthernet0/0** interface. Make the following changes to the interface's configuration:

    IP Address: **192.168.0.1**

    Subnet Mask: **255.255.255.0**

    Port Status: **On**

8. Click the **FastEthernet1/0** interface. Make the following changes to the interface's configuration:

IP Address: **172.16.0.1**

Subnet Mask: **255.255.0.0**

Port Status: **On**

9. Close the **Router0** window and wait a few minutes for the switch-to-router connections to turn to green triangles on both ends of each connection.
10. Click **PC0** to open its configuration window. Click the **Desktop** tab and then click **IP Configuration**. Make the following changes to the workstation's configuration:

    IP Configuration: **Static**

    IP Address: **192.168.0.100**

    Subnet Mask: **255.255.255.0**

    Default Gateway: **192.168.0.1**

11. Close the IP Configuration window by clicking the small, blue **X** near the upper right corner. Then click **Command Prompt**. Enter **ipconfig** to confirm the network configuration is correct.
12. Close **Command Prompt** and close the **PC0** configuration window.
13. Click **PC1** to open its configuration window. Click the **Desktop** tab and then click **IP Configuration**. Make the following changes to the workstation's configuration:

    IP Configuration: **Static**

    IP Address: **172.16.0.100**

    Subnet Mask: **255.255.0.0**

    Default Gateway: **172.16.0.1**

14. Close the IP Configuration window by clicking the small, blue **X** near the upper right corner. Then click **Command Prompt**. Enter **ipconfig** to confirm the network configuration is correct.
15. Enter the command **ping 192.168.0.100**. Was the ping successful? If so, then you have successfully begun building your Packet Tracer network. If not, troubleshoot your network to determine where the problem is and fix it. What problems did you have to fix, if any?

    Answer: Answers may vary. If the preceding steps were followed correctly, the ping should work. Otherwise, the student might need to check earlier instructions and fix typos or missed steps.

16. In the main Packet Tracer window, open the **Simulation Panel** (click the **Simulation** button in the lower right corner, or press **Shift**+**S**). In the PC1 configuration window, run the ping again. Move or minimize the PC1 configuration window so you can see the devices in the workspace. In the Simulation Panel, click the **Play** button and watch what happens.

17. When you're ready, click any ICMP message on the network to examine its details and to see an explanation of each step in the process. Click through the various layers and read their explanations. Click the Inbound PDU Details and Outbound PDU Details tabs to examine the headers of each ICMP message. Explore at least three different ICMP messages and answer the following questions for each of the three messages:

    a. Which two devices are exchanging each message (sender and receiver)?

    Answer: Answers may vary. For each of the three ICMP messages, answer should include any two devices from this list: PC0, Switch0, Router0, Switch1, and PC1.

    b. Which OSI layers added headers to each message?

    Answer: ICMP messages add headers to OSI layers 1, 2, and 3.

18. When you've explored the ICMP messages, in the Simulation Panel, click the **Reset Simulation** button to stop the simulation. Close the **Simulation Panel**, close **Command Prompt**, and close the **PC1** window.

19. Add a **Note** to each connection that lists its IP address, subnet mask, and default gateway if relevant. Figure 5-63 shows an example for the router, which has two interfaces with IP addresses. After adding all your documentation, **take a screenshot of your Packet Tracer network**; submit this visual with your answers to this project's questions.

    Answer: Screenshot should show Packet Tracer network with one router, two switches, and one PC connected to each switch, along with sufficient documentation of IP addresses and subnet masks on the router and PCs, and default gateways on the PCs.

20. Click **File** and **Save**. Give the file an informative name (such as NetPlusPTnetwork), and save your Packet Tracer file in a safe place for future projects. What is the name of your Packet Tracer file?

    Answer: Answers may vary and should list a descriptive network name for easy identification later.

21. Add the Packet Tracer network file's name and location to the Packet Tracer page on your Wikidot website, along with any notes you think might be helpful to you for the next Packet Tracer project. When you're finished, close Packet Tracer.

MindTap

Reflection Discussion 5: Cabling Upgrade

Knowing when to upgrade cabling and what to upgrade it to is an art that requires you to consider many factors, such as existing cabling, current network needs, anticipated future needs, costs of cabling and installation, and business concerns like existing budget and other demands on that budget. You can get some practice all these needs by looking at your own network or at your school's network. Get ready to do some sleuthing! And then respond to the following questions:

- Either on your home network or in your school's computer lab, look at the stamp on the cable connecting your home router to your ISP's device (such as a modem), or connecting your computer to a switch or router. What is the category of this cable? What is the maximum bandwidth supported by this category of cable?
- Research online to find how much cabling of higher categories would cost. Choose a higher category that offers better throughput for reasonable costs. Consider whether you would be able to use existing connectors on devices or if devices would need adapters or replacement. What target cable category did you choose? How much does this cabling cost, on average, per meter?
- Measure the length of cabling you would need for your network if you were to upgrade your network's cabling to this new category. Consider all the relevant cabling for your home network or for the computers within your lab (you don't need to consider cabling outside the lab). Multiply the average price of the cable by the number of meters you'll need. How much will the new cabling cost?
- Write a short paragraph describing the benefits this cabling upgrade would offer for your network. Consider that purchasing the cabling is not the only expense—you might also have installation costs (depending on much cabling is involved and whether it runs through walls or ceilings). Do you think the expense of the upgrade would be worth it for the benefits that would be gained? Why or why not?

Go to the discussion forum in your school's LMS (learning management system). Write a post of at least 100 words discussing your thoughts about these questions. Then respond to two of your classmates' threads with posts of at least 50 words discussing their comments and ideas. Use complete sentences, and check your grammar and spelling. Try to ask open-ended questions that encourage discussion, and remember to respond to people who post on your thread.

Answer: Rubric provided for grading

Networking for Life Discussion 5: Networking Events

Many vendors and professional organizations offer educational events to help professionals keep their knowledge up-to-date and to encourage networking among IT professionals. For example, Cisco, VMware, AWS, Google, Microsoft, CompTIA, and many other organizations offer in-person or virtual conferences with keynotes from industry leaders and breakout sessions for more specific topics. You might also have access to regional or community organizations that host conferences in specialty areas such as networking, DevOps, programming, or cybersecurity. Many of these conferences are free to attend. While some of them do charge an admission fee, many offer scholarships for students.

Do some research to find an in-person conference in your area or a virtual conference scheduled soon. Look online and ask your instructors or other area professionals for recommendations. Then respond to the following questions:

- Which conference did you choose? What is the website for more information?
- When is the conference scheduled? How much does it cost to attend? If it's not free, are there scholarships available for students?
- What topics will be covered during the keynotes and breakout sessions that are interesting to you? How could this information help you in your career?

Go to the discussion forum in your school's LMS (learning management system). Write a post of at least 100 words discussing your thoughts about these questions. Then respond to two of your classmates' threads with posts of at least 50 words discussing their comments and ideas. Use complete sentences and check your grammar and spelling. Try to ask open-ended questions that encourage discussion. Remember to respond to people who post on your thread.

Answer: Rubric provided for grading

Rubric for Hands-on Projects and Capstone Projects

Criteria	Beginning	Developing	Proficient	Exemplary	Score
Responses to questions	All missing or incorrect **[0 points]**	Most missing or incorrect **[15 points]**	Little missing or incorrect **[20 points]**	All complete **[25 points]**	
Other deliverables	Missing **[0 points]**	Present but missing most or all the required information **[15 points]**	Present but missing some of the required information **[20 points]**	Present and contains all the required information **[25 points]**	
Critical thinking and engagement	Student shows little to no evidence of attempting to meet the	Student retains their existing understanding while	Student challenges their existing understanding and shows	Student challenges their existing understanding and displays	

	performance requirements of the assignment **[0 points]**	attempting to meet the performance requirements of the assignment **[15 points]**	evidence of new learning **[20 points]**	creative and original insights **[25 points]**	
Mechanics	Grammar, spelling, punctuation, and formatting make student's message difficult to understand **[0 points]**	Grammar, spelling, punctuation, and formatting detract from student's message **[15 points]**	Grammar, spelling, punctuation, and formatting support student's message **[20 points]**	Grammar, spelling, punctuation, and formatting enhance student's message **[25 points]**	
				Total	

Rubric for Discussion Assignments

Task	***Developing***	***Proficient***	***Exemplary***	***Score***
Initial post	Generalized statements **[30 points]**	Some specific statements with supporting evidence **[40 points]**	Self-reflective discussion with specific and thoughtful statements and supporting evidence **[50 points]**	
Initial post: Mechanics	· Length < 100 words · Several grammar and spelling errors **[5 points]**	· Length = 100 words · Occasional grammar and spelling errors **[7 points]**	· Length > 100 words · Appropriate grammar and spelling **[10 points]**	
Response 1	Brief response showing little	Detailed response with specific	Thoughtful response with specific	

	engagement or critical thinking **[5 points]**	contributions to the discussion **[10 points]**	examples or details and open-ended questions that invite deeper discussion of the topic **[15 points]**	
Response 2	Brief response showing little engagement or critical thinking **[5 points]**	Detailed response with specific contributions to the discussion **[10 points]**	Thoughtful response with specific examples or details and open-ended questions that invite deeper discussion of the topic **[15 points]**	
Both responses: Mechanics	· Length < 50 words each · Several grammar and spelling errors **[5 points]**	· Length = 50 words each · Occasional grammar and spelling errors **[7 points]**	· Length > 50 words each · Appropriate grammar and spelling **[10 points]**	
			Total	