Solution and Answer Guide

Jill West, CompTIA Network+ Guide to Networks, 9th Edition, ISBN: 9780357508138; Module 4: Protocols

Table of Contents

Text

Applying Concepts

Applying Concepts 4-1: Examine a Sample TCP Header

This is a step-by-step activity. It does not require any solutions.

In Project 2-4, you captured and filtered to a TCP stream using Wireshark. Now that you know the function of each TCP segment field, you can interpret a segment's header contents. Let's practice with an example. Figure 4-5 shows a sample TCP header.

Suppose the segment in Figure 4-5 was sent from computer B to computer A. Table 4-2 interprets the rows shown in Figure 4-5, beginning with the row labeled "Source port."

Table 4-2 Translation of TCP field data

Field name	TCP header data
Source port	The segment was issued from computer B's port 80, the port assigned to HTTP by default.
Destination port	The segment is addressed to port 1958 on computer A.
Sequence number	The segment is identified by sequence number 3043958669.
Acknowledgment number	By containing a value other than zero, this field informs computer A that its last communication was received. Computer B is indicating that the next segment it receives from computer A should have the sequence number of 937013559, which is the same as this segment's acknowledgment number.
Header length	The TCP header is 24 bytes long—4 bytes larger than its minimum size, which means that some of the available options were specified or the padding space was used.
Flags: Congestion Window Reduced (CWR) and ECN-Echo	These optional flags can be used to help TCP react to and reduce traffic congestion. They are only available when TCP is establishing a connection. However, in this segment, they are not activated.

Flags: Acknowledgment and Syn	Of all the possible flags in the Figure 4-5 segment, only the ACK and SYN flags are set. This means that computer B is acknowledging the last segment it received from computer A, and it's also negotiating a synchronization scheme for sequencing.
Window size	The window size is 5840, meaning that computer B can accept 5840 bytes of data from computer A before computer A should expect an acknowledgment.
Checksum	The valid outcome of the error-checking algorithm used to verify the segment's header is 0x206a. When computer A receives this segment, it will perform the same calculation, and if the result matches, it will know the TCP header arrived without damage.
Maximum segment size	The maximum TCP segment size for this session is 1460 bytes.

Note 4-3

A computer doesn't "see" the TCP segment as it's organized and formatted in Figure 4-5. The information in Figure 4-5 was generated by a <KTRM>**protocol analyzer**</KTRM> (in this case, Wireshark), which is an application that collects and examines network messages. Wireshark translates each message into a user-friendly format. From the computer's standpoint, the TCP segment arrives as a series of bits: 0s and 1s. The computer relies on TCP standards to determine how to interpret each bit in the segment based on its location and value. You'll use the Wireshark protocol analyzer again in a later module.

Applying Concepts 4-2: Examine a Sample IPv4 Header

This is a step-by-step activity. It does not require any solutions.

Let's examine the IPv4 header shown in the Wireshark capture in Figure 4-8. The fields are explained in Table 4-4, beginning with the Version field.

Table 4-4 Explanation of IPv4 header fields listed in Figure 4-8

Field name	IPv4 header data
Version	The transmission relies on version 4 of the Internet Protocol.
Header length	The packet has a header length of 20 bytes. Because this is the minimum size for an IP header, you can deduce that the packet contains no options or padding.

Differentiated Services Field	No options for priority handling are set, which is not unusual in routine data exchanges such as requesting a web page.
Total Length	The total length of the packet is 44 bytes. This makes sense when you consider that its header is 20 bytes and the TCP segment that it encapsulates is 24 bytes. Considering that the maximum size of an IP packet is 65,535 bytes, this is a very small packet.
Identification	This field uniquely identifies the packet. This packet, the first one issued from computer B to computer A in the TCP connection exchange, is identified in hexadecimal notation as 0x0000 or simply 0.
Flag: Don't fragment and Fragment offset	The Don't fragment option is set to 1, indicating this packet is not fragmented. And because it's not fragmented, the Fragment offset field does not apply and is set to 0.
Time to live	This packet's TTL is set to 64. If the packet were to keep traversing networks, it would be allowed 64 more hops before it was discarded.
Protocol	This field indicates that a TCP segment is encapsulated within the packet. TCP is always indicated by the hexadecimal string of 0x06.
Header checksum	This field provides the correct header checksum answer, which is used by the recipient of this packet to determine whether the header was damaged in transit.
Source and Destination	These last two fields show the IPv4 addresses for the packet's source and destination, respectively.

Applying Concepts 4-3: Examine a Sample IPv6 Header

This is a step-by-step activity. It does not require any solutions.

Figure 4-10 shows the contents of an IPv6 packet header captured by Wireshark, and Table 4-6 breaks down what it all means. This packet formed part of a message issued by ping.

Table 4-6 Explanation of IPv6 header fields listed in Figure 4-10

Field name	IPv6 header data
Version	Version 6 of the Internet Protocol is used, expressed in binary format as 0110.
Traffic class and Flowlabel	Both these fields are set to 0x00000000, which means neither field has a specified value. Routers receiving a packet that lacks Traffic class or Flow label

	information will not prioritize the packet or make any guarantees that it will reach its destination at the same time as any other packets. For many types of traffic, this is perfectly acceptable.
Payload length	This packet carries 64 bits of data. Considering that IPv6 packets can carry payloads as large as 64 KB, this is a very small packet.
Next header	The data in this packet's payload belongs to an ICMPv6 transmission.
Hop limit	This packet can be forwarded by routers up to 64 times before it is discarded.
Source and Destination	These last two fields show the IPv6 addresses for the packet's source and destination hosts, respectively.

Applying Concepts 4-4: Browser Security

You can change the settings in your browser to make sure you're using the latest version of TLS. On a Windows machine, changes you make to one browser for these settings will affect other browsers installed on your computer. Complete the following steps:

1. In the Settings app, search for **Internet options**, and then click **Internet Options** in the search results.
2. On the **Advanced** tab, scroll down to the Security section. Which SSL/TLS options are currently enabled?

   Answer: Answers may vary and might include any combination of the following: Use SSL 3.0, Use TLS 1.0, Use TLS 1.1, Use TLS 1.2, Use TLS 1.3 (experimental)
3. Disable **SSL 3.0**, **TLS 1.0**, and **TLS 1.1**. Make sure **TLS 1.2** and **TLS 1.3** are enabled. While TLS 1.3 might be labeled experimental, it was finalized in 2018 and provides better security at faster speeds and is already widely used by websites. Also, if you regularly use an unsecured wireless network like at a coffee shop or a restaurant, also select **Warn if changing between secure and not secure mode** so you'll be notified when interacting with an unsecured website. See Figure 4-16. Click **OK**.

Some browsers will prevent navigation to unsecured websites when the warning option is checked as previously instructed. This is a good thing if you're using a questionable network. But if you have trouble navigating to unsecured sites you feel comfortable with, you'll need to go back and uncheck this option in Internet options.

Caution

When visiting secure websites, it's important to notice if you have a secure connection with a trusted website before entering personal information on that site. Edge, for example, shows a padlock icon when the site's certificate has been identified and confirmed. This visual is still no guarantee, however, as scammers are now figuring out how to impersonate HTTPS websites' credentials.

4. In your browser, navigate to **paypal.com**. What is the exact address shown in the address box after the page loads in the browser?

   Answer: **https://www.paypal.com/us/home**

5. Click the padlock icon and then click the certificate listed. What CA verified the legitimacy of the website?

   Answer: DigiCert</NL>

Applying Concepts 4-5: Trace the Route to Google.com

You can perform a trace using an IP address or a host name. On a UNIX or Linux system, the command syntax would be the following:

traceroute 8.8.8.8 or **traceroute google.com**

Because tracert is installed by default on Windows, use a Windows machine for this exercise instead:

1. On a Windows system, perform a trace on one of Google's public DNS servers with the command **tracert 8.8.8.8**. How many hops were traced? What is the IP address of the final hop?

   Answer: Answers will vary and should include a number of hops (as low as 2 or possibly much higher) and an IPv4 address for the final node, which most likely will be 8.8.8.8.

2. Use tracert to perform a trace on Google's web server with the command **tracert google.com**. How many hops were traced this time? What is the IP address of the final hop? Why is this IP address different than the IP address of the final hop in the previous step?

   Answer: Answers will vary and should include a number of hops and an IPv4 address for the final node (such as 172.217.13.78).

   Answer: The IP address for Google's web server is different than the IP address of Google's DNS server.

Applying Concepts 4-6: Change a MAC address

This is a step-by-step activity. It does not require any solutions.

It only takes a few, short steps to change a Windows computer's MAC address. Complete the following steps:

1. Open Network and Sharing Center, and click Change adapter settings.
2. Right-click any wired network adapter and click Properties. Then click Configure.
3. On the Advanced tab, click Network Address (on a VM, this field is called Locally Administered Address). Select the Value radio button, and then enter a 12-digit value with no hyphens or colons, and click OK. Close all windows and restart the computer.
4. Run ipconfig /all to confirm the new MAC address is active.
5. To return to the default MAC address, repeat the earlier steps but select Not Present on the Advanced tab.

Review Questions

1. Which protocol's header would a layer 4 device read and process?

    a. IP

    b. TCP

    c. ARP

    d. HTTP

    Answer: b. TCP

    Explanation: Each device is known by the innermost OSI layer header it reads and processes; **TCP (Transmission Control Protocol)** operates in the transport layer of the OSI model. IP (Internet Protocol) belongs to the network layer of the OSI model. ARP (Address Resolution Protocol) is a layer 2 protocol that works with IPv4 in layer 3. HTTP (Hypertext Transfer Protocol) is an application layer protocol.

2. What field in a TCP segment is used to determine if an arriving data unit exactly matches the data unit sent by the source?

    a. Source port

    b. Acknowledgment number

    c. DiffServ

d. Checksum

Answer: d. Checksum

Explanation: TCP sends a character string called a **checksum**; TCP on the destination host then generates a similar string. If the two checksums fail to match, the destination host asks the source to retransmit the data. The Source port field indicates the port at the source host. The Acknowledgment number field confirms receipt of data via a return message to the sender. The DiffServ field in an IPv4 header informs routers the level of precedence they should apply when processing the incoming packet.

3. At which OSI layer does IP operate?

   a. Application layer

   b. Transport layer

   c. Network layer

   d. Data link layer

   Answer: c. Network layer

   Explanation: IP (Internet Protocol) belongs to the **network layer** of the OSI model. It allows data to traverse more than one LAN segment and more than one type of network through a router, which is a network layer device. Data and instructions, known as the payload, are generated by an application running on the source host, and the application layer describes the interface between two applications, each on separate computers. A transport layer protocol, usually either TCP or UDP, adds a header in front of the payload; this header includes a port to identify the receiving application on the destination host. The data link layer encapsulates data in a frame that includes a physical address used to find a node on the local network; common data link layer protocols are Ethernet and Wi-Fi.

4. What is the Internet standard MTU?

   a. 65,535 bytes

   b. 1,522 bytes

   c. 1,500 bytes

   d. 9,198 bytes

   Answer: c. 1,500 bytes

   Explanation: For Ethernet, the default MTU is **1,500 bytes**, a value that is generally considered the Internet standard. The maximum size of a network layer packet is 65,535 bytes. Ethernet frames on a VLAN (virtual LAN) can have an extra 4-byte field and a

maximum frame size of 1,522 bytes. Some special-purpose networks use a proprietary version of Ethernet that allows for a jumbo frame, in which the MTU can be set above 9,000 bytes.

5. Which two protocols manage neighbor discovery processes on IPv4 networks?

    a. ICMP and ARP

    b. IPv4 and IPv6

    c. TCP and UDP

    d. NDP and Ethernet

    Answer: a. ICMP and ARP

    Explanation: On IPv4 networks, neighbor discovery is managed by **ARP (Address Resolution Protocol)** with help from **ICMP (Internet Control Message Protocol)**. IP (Internet Protocol) versions 4 and 6 specify where data should be delivered and enable TCP/IP to internetwork. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) include a physical address used to find a node on the local network. NDP (Neighbor Discovery Protocol) eliminates the need for ARP and some ICMP functions in IPv6 networks. Ethernet uses physical addresses to find nodes on the local network.

6. You're getting a duplicate IP address error on your computer and need to figure out what other device on your network is using the IP address 192.168.1.56. What command will show you which MAC address is mapped to that IP address?

    a. telnet 192.168.1.56

    b. tracert 192.168.1.56

    c. arp -a

    d. netstat -n

    Answer: c. arp -a

    Explanation: The database of IP-to-MAC address mappings is called an ARP table; to view a workstation's ARP table, enter the command arp -a. The command telnet 192.168.1.56 will attempt to connect to a device on the network at the IP address listed. The command tracert 192.168.1.56 will trace a path from the local node to the node at the listed IP address. The netstat -n command lists current connections on the local device, including IP addresses and ports.

7. What is one advantage offered by VDI over RDS and VNC?

    a. Offers access to multiple OSs in VMs

b. Supports remote access to mobile devices

c. Allows multiple users to sign in at once

d. Provides open source flexibility

Answer: a. Offers access to multiple OSs in VMs

Explanation: VDI (Virtual Desktop Infrastructure) **offers access to VMs running many different OSs**. VNC (Virtual Network Computing) is open source so other companies can develop their own software, and it supports remote access to computers, tablets, and smartphones. RDS (Remote Desktop Services) allows multiple users to access the same virtual or physical Windows Server at one time.

8. Which encryption protocol does GRE use to increase the security of its transmissions?

a. SSL

b. SFTP

c. IPsec

d. SSH

Answer: c. IPsec

Explanation: GRE (Generic Routing Encapsulation) is a versatile tunneling protocol and, like many tunneling protocols, it's used in conjunction with **IPsec (IP Security)** to increase the security of its transmissions. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are both methods of encrypting TCP/IP transmissions, such as HTTP, SMTP, LDAP, IMAP, and POP3. SFTP (Secure FTP) is a file-transfer version of SSH (Secure Shell), which is a collection of protocols that performs both authentication and encryption for a remote access session.

9. Which encryption benchmark ensures data is not modified after it's transmitted and before it's received?

a. Confidentiality

b. Integrity

c. Availability

d. Symmetric

Answer: b. Integrity

Explanation: **Integrity** ensures data is not modified in the time after the sender transmits it and before the receiver picks it up. Confidentiality ensures data can only be viewed by its intended recipient or at its intended destination. Availability ensures data is available and

accessible to the intended recipient when needed. Symmetric key encryption uses the same key during both the encryption and decryption of the data.

10. Which remote file access protocol is an extension of SSH?

    a. SFTP

    b. TFTP

    c. FTPS

    d. HTTPS

    Answer: a. SFTP

    Explanation: **SFTP (Secure FTP)** is a file-transfer version of SSH that includes encryption and authentication, and it's sometimes inaccurately called FTP over SSH or SSH FTP. TFTP (Trivial FTP) is a simple protocol similar to FTP except that it includes no authentication or security for transferring files. FTPS (FTP Secure or FTP over SSL) provides an added layer of protection for FTP using SSL/TLS that can encrypt both the control and data channels. HTTPS (HTTP Secure) uses SSL/TLS encryption and TCP port 443 rather than port 80.

11. What three characteristics about TCP distinguish it from UDP?

    Answer: TCP is connection-oriented, uses sequencing and checksums, and provides flow control.

12. What process is used to establish a TCP connection?

    Answer: Three-way handshake

13. What is the difference between dynamic ARP table entries and static ARP table entries?

    Answer: Dynamic ARP table entries are created when a client makes an ARP request, whereas static ARP table entries are entered manually using the ARP utility.

14. Which two fields in an Ethernet frame help synchronize device communications but are not counted toward the frame's size?

    Answer: Preamble and SFD

15. Explain the key difference between how symmetric encryption works and how asymmetric encryption works.

    Answer: Symmetric encryption uses the same key during both the encryption and decryption of the data. Asymmetric encryption requires the use of two different keys, one to encrypt and the other to decrypt.

16. Which secured tunneling protocol might be able to cross firewalls where IPsec is blocked?

Answer: OpenVPN

17. When surfing online, you get some strange data on an apparently secure website, and you realize you need to check the legitimacy of the site. What kind of organization issues digital certificates for websites?

    Answer: CA (Certificate Authority)

18. What tcpdump command will capture data on the eth0 interface and redirect output to a text file named checkme.txt for further analysis?

    Answer: tcpdump -i eth0 -w checkme.txt

19. Which terminal emulation protocol is similar to RDP but is open source?

    Answer: VNC (Virtual Network Connection)

20. Which port must be open for RDP traffic to cross a firewall?

    Answer: 3389

Hands-On Projects

Note 4-12

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 4-1: Install and Use WSL (Windows Subsystem for Linux)

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
- Internet access

Context:

WSL (Windows Subsystem for Linux) is a Linux shell for Windows that allows users to interact with underlying Windows functions and system files. It's not a VM, and it's not a fully separate operating system. It runs on any 64-bit Windows 10 system with the Anniversary Update (version 1607) or later. To use it, you must first turn on Developer Mode, and then enable the Windows Subsystem for Linux feature. To enable Windows Subsystem for Linux and install an Ubuntu Terminal on a Windows 10 system, complete the following steps:

1. First, turn on Developer Mode.

    a. Open the **Settings** app and click **Update & Security**. In the left pane, scroll down and click **For developers**.

    b. Select **Developer mode**, as shown in Figure 4-29. Click **Yes** to turn on Developer Mode and close the Settings app.

2. Enable Windows Subsystem for Linux.<SAL>

    a. Open **Control Panel** and click **Programs and Features**. In the left pane, click **Turn Windows features on or off**.

    b. Scroll down and click **Windows Subsystem for Linux**, as shown in Figure 4-30. Click **OK**.

Note 4-13

To open Turn Windows features on or off directly, you can also click Start, begin typing **turn Windows**, then click **Turn Windows features on or off**.

    c. Restart the computer when the changes are complete to finish enabling Windows Subsystem for Linux.</SAL>

Now that you have enabled Windows Subsystem for Linux, you can install a distribution of Linux designed to run on Windows. To install and run Ubuntu on Windows, do the following:

3. Open the **Microsoft Store** app and search for **Ubuntu**. Install the latest, free Ubuntu on Windows app, as shown in Figure 4-31.

4. After the installation is complete, launch the app. Enter a new UNIX username at the prompt. This username can be different from your Windows username.

5. Enter a password at the next prompt. The cursor will not move as you type the password. Re-enter the password at the next prompt. Add this information as a Secure Note in your LastPass vault.

6. After the installation is complete, you'll see the Ubuntu Terminal, as shown in Figure 4-32. What is the Ubuntu prompt on your computer? Include all symbols in your answer. **</EOCNL>**

    Answer: Answers may vary. One example is jwest@LAB-OWL:$

At this point, many of the Linux commands you have become familiar with will work as usual at the Ubuntu shell prompt. The commands interact with the underlying Windows system files, and changes to those files can be monitored through other Windows tools. **<EOCNL>**

7. Enter the commend **pwd** to show your current working directory (recall the Linux calls

folders *directories*). What is the current directory?

Answer: /home/*username*

8. To open a File Explorer window showing this directory, enter the command **explorer.exe .** (Notice the extra space and period after the explorer.exe portion.) Figure 4-33 shows the command entered in the Ubuntu Terminal window and the File Explorer window showing Ubuntu's home directory.

9. To create a new directory, enter the command **mkdir mydir**. Refresh the File Explorer window. Do you see your new directory listed?

   Answer: Yes

10. To navigate to that directory in Ubuntu, enter the command **cd mydir**. To create a new file in that directory, enter the command **touch myfile.txt**. In File Explorer, open the **mydir** folder. What items do you see listed here?

    Answer: The file myfile.txt

11. Choose three other Linux commands and practice using them. For each one, **take a screenshot** of the Ubuntu Terminal window showing the command and its output. Submit this visual with your answers to this project's questions.

    Answer: One or more screenshots should show three Linux commands entered in the Ubuntu Terminal window and output from those commands.

12. In your wiki, add a new page titled **Applications:WSL-Ubuntu**. Indicate the module and project number for this installation, the computer you used for this project, a brief description of what you learned, and any other information you might find helpful when using Ubuntu on Windows later.

Project 4-2: Use Remote Desktop

Estimated time: 45 minutes

Objective: Compare and contrast remote access methods and security implications. (Obj. 4.4)

Group work: This project can be completed by an individual working alone or, if desired, in cooperation with a team of two or three classmates. In some cases, working as a group could provide beneficial insights when troubleshooting challenging steps and brainstorming solutions. Check with your instructor for details specific to your class.

Resources:

- Two Windows computers (with administrative access) on the same network<SBL>

- These two computers can be both physical, both virtual, or one of each.
- One of these systems must have Windows 10 Professional, Education, or Enterprise installed, and the other can have any edition of Windows 7, 8, 8.1, or 10.
- If you're using a VM as one computer and the VM's physical host as the second computer, the VM must serve as the RDP host and must have Windows 10 Professional, Education, or Enterprise installed. You might need to create a new Windows VM to meet these requirements if you previously installed Windows 10 Home on your VM. If you do create a new VM, be sure to record credentials in your LastPass vault. The physical computer will be the RDP client.
- If you're using a VirtualBox VM as one computer and a physical machine as the second computer, the VM's network adapter must be configured in the bridged mode. Before starting the VM, open the VM's **Settings** window, click **Network**, and change the *Attached to* field to **Bridged Adapter**. Click **OK**. You can now start the VM.</SBL>

- Internet access or a Windows ISO file if a new VM is needed

Context:

The host or server computer is the remote computer that serves up Remote Desktop to your local client computer. Note that a Windows Home computer cannot serve as an RDP host, although it can connect as a client to another RDP host. To prepare your host computer, you need to get its name and configure the Remote Desktop service. Complete the following steps on a Windows 10 (Professional, Education, or Enterprise) machine:

1. Right-click the **Start** button and click **System**. Under Device specifications, find the device's name and copy it to a text file using Notepad for future reference in this project. What is the RDP host's device name?

   Answer: Answers will vary widely. One example is DESKTOP-B7HE79M.

2. To enable the Remote Desktop service on the host computer, in the left pane of the Settings window, scroll down and click **Remote Desktop**. Click the slider to **Enable Remote Desktop**. In the warning box, click **Confirm**.

3. Make sure you know the sign-in credentials for a user on this system. Users who have administrative privileges are allowed to use Remote Desktop by default, but other users need to be added. If you need to add a user, click **Select users that can remotely access this PC** and follow the directions on-screen.

4. Verify that Windows Firewall is set to allow Remote Desktop activity to this computer. To do this, in the Settings app, search for **firewall**, click **Firewall & network protection** and then click **Allow an app through firewall**.

5. The Allowed apps window appears. Scroll down to Remote Desktop. If the changes don't match the settings in Figure 4-34, click **Change settings** and make any needed adjustments. Click **OK** to apply any changes. Close the Windows Defender Firewall and Settings windows.

You will learn more about Windows Defender Firewall later. </EOCNL>

You are now ready to test Remote Desktop by accessing the host computer (physical or virtual) from another computer (physical or virtual) on your local network. Note that any edition of Windows 7, 8.1, or 10 can serve as a client computer (the computer viewing the host computer's desktop) for a Remote Desktop connection. The following steps are written specifically for Windows 10.

Follow these steps on the client computer (any edition of Windows 7, 8, 8.1, or 10) to create a Remote Desktop connection to the host computer: **<EOCNL>**

6. First, confirm the two computers can communicate on the network. In a PowerShell or Command Prompt window, ping the RDP host computer from the RDP client computer. If the ping works, continue to Step 7. If it does not work, you'll need to do some troubleshooting. Here are some possible solutions:

    a. Make sure both computers are connected to the same network and subnet. In most cases, the first three octets of each computer's IP address should be identical to each other.

    b. Make sure both computers can communicate successfully with other resources on the network. For example, try pinging the default gateway.

    c. Make sure both computers are connected to the network in Private mode. To check this, click the network connection's icon on the right side of the taskbar near the clock, and then click **Network & Internet settings**. The connection should be labeled "Private network" on both computers. If it is not, click **Change connection properties** and choose the **Private** option. Note that if you're working on a physical machine connected to a Hyper-V virtual switch, the network status will show *vEthernet* and you will not have the option to change between Public and Private network modes because the computer should already be in Private network mode.

    d. If the ping still won't work, enabling File and Printer Sharing on Windows Defender Firewall sometimes solves the problem. To do this, open Network and Sharing Center and click **Change advanced sharing settings**. Select **Turn on file and printer sharing** for private networks on both computers.</SAL>

7. Press **Win**+**R**, type **mstsc** in the search box, and press **Enter**. This is easier to remember if you know that Remote Desktop Services was formerly called Microsoft Terminal Services; mstsc (Microsoft Terminal Services Client) is the client portion. Alternately, you can click **Start**, scroll down and click **Windows Accessories**, and then click **Remote Desktop Connection**.

8. Enter the host name of the computer to which you want to connect. To be able to transfer files from one computer to the other, click **Show Options** and then click the **Local Resources** tab, as shown in the left side of Figure 4-35. Under *Local devices and resources*,

click **More**. The dialog box on the right side of Figure 4-35 appears.

9. Check **Drives**, click **OK**, and then click **Connect** to make the connection. If a warning box appears, check the box for *Don't ask me again for connections to this computer* and then click **Connect** again.

10. Enter a password for the remote computer. If you need to sign in with a different account than the one you're using on the client computer, click **More choices**, click **Use a different account**, and enter the account credentials. If you're using a client computer that you own, you can check the box for *Remember me*, and then click **OK**. If a warning box appears saying the identity of the remote computer cannot be verified, you can check the box for *Don't ask me again for connections to this computer*. Click **Yes** to continue with the connection.

Note 4-14

Even though Windows normally allows more than one user to be logged on at the same time, Remote Desktop does not. When a Remote Desktop session is opened, all local users on the host computer are logged off.

11. The desktop of the remote computer appears in a maximized window that covers your entire screen. Float your cursor at the top of your screen to find the RDP controls. From here, you can reduce the size of the RDP window so you can see both your local computer's desktop and the remote computer's desktop, as shown in Figure 4-36. When you click inside the RDP window, you can work with the remote computer just as if you were sitting in front of it, except the response time will be slower. To move files back and forth between computers, use File Explorer on the remote computer. Files on your local computer and on the remote computer will appear in File Explorer on the remote computer's screen in the This PC group.

12. Position File Explorer on the remote computer's desktop so that you can see both the server's and the client's hard drives listed in the left pane. **Take a screenshot**; submit this visual with your answers to this project's questions.

    Answer: Screenshot should show the local hard drive and the RDP client's hard drive listed in File Explorer's navigation pane.

13. To close the connection to the remote computer, shut down or sign out of the remote computer or close the Remote Desktop Connection window.

14. In your wiki, add a new page titled **Applications:RDP**. Indicate the module and project number for this activity, the computers you used for this project, a brief description of what you learned, and any other information you might find helpful when using RDP later.

15. If you created a new VM for this project, add the new VM's information to your VMclients page in your wiki. Include the module number, hypervisor used, VM computer name, and VM

operating system. Also note any additional information that you might find helpful when you return to this VM in the future.

Project 4-3: Redirect Command Output to a Text File

Estimated time: 15 minutes

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

Resources:

- Internet access

Context:

Sometimes when you're using a command such as tcpdump, the sheer volume of output can be daunting to work with. There's no way to search through the output for specific information, and you can only expand the PowerShell or Command Prompt window so far. One solution to this problem is to redirect the command output to a text file where you can search the text, copy and paste text, and save the output for future reference. To accomplish this feat, you'll need to add a redirection operator to the command whose output you want to export to a text file. Complete the following steps:

1. First, try this simple command in PowerShell or Command Prompt:

   ipconfig > ipconfigtest.txt

   This runs the ipconfig command and redirects the output to a text file named ipconfigtest.txt. By default, the file is saved to the current default folder, for example, C:\Users\JillWest. Use File Explorer to find the file. **Take a screenshot** showing the file and its file path; submit this visual with your answers to this project's questions.

   Answer: Screenshot should show the file ipconfigtest.txt in File Explorer.

2. To specify the location of the file when you create it, add the path to the file in the command line. For example, to save the file to the desktop, use the following command (substitute the correct file path to your desktop). What command and file path did you enter?

   ipconfig > C:\Users*Username*\Desktop\ipconfigtest.txt

   Answer: Answers may vary and should show the ipconfig command with output redirected to a file in a complete file path.

Note 4-15

If you're not sure what the file path is to your Desktop, you can find it in File Explorer. In the navigation pane on the left, right-click the **Desktop** link and click **Properties**. The file path is shown in the Location field. Note that your desktop might be showing your OneDrive Desktop, which would be located at the following path:

C:\Users*Username*\OneDrive\Desktop

In this case, you might not be able to send command output to your OneDrive desktop. Save your files for this project to a folder on your hard drive instead.

3. If you already have a file on the desktop by that name, the file will be overwritten with the new data. What if you would rather append data to an existing file? In this case, use the >> operator. Enter this command (substitute the correct file path to your desktop):

   ipconfig >> C:\Users*Username*\Desktop\ipconfigtest.txt

   Now the new output will appear at the end of the existing file, and all the data is preserved within this single file. This option is useful when collecting data from repeated tests or from multiple computers, where you want all the data to converge into a single file for future analysis.

Note 4-16

When reusing an earlier command or portions of an earlier command, you can press the up arrow on your keyboard to recall earlier commands. Then use the side arrows to place your cursor to make edits.

4. Where do command parameters fit when redirecting output? Let's use the netstat command to show the IP address and port of each TCP and UDP connection on the computer. In the following command, substitute the correct file path to your desktop to output the data to a new file. Notice that any parameters you want to use should be inserted after the command itself and before the redirection operator.

   netstat –an > C:\Users*Username*\Desktop\connections.txt

   Open the file you just created. How many TCP ports are in the ESTABLISHED state?

   Answer: Answers may vary and should list the number of ports in the ESTABLISHED state, such as 1 or 2.

5. Open your browser and visit two or three websites in different tabs. With your browser still open, run the netstat command again and append the new data to your existing file. What command did you run? How many TCP ports are in the ESTABLISHED state now?

   Answer: The exact file path may vary. Otherwise, the command is netstat –an >> C:\Users*Username*\Desktop\connections.txt

Answer: Answers may vary and will likely list a much larger number of ports in the ESTABLISHED state.

6. You can include a space in the filename by putting quotation marks around the entire filename *and* location. Enter the following command:

   ping 8.8.8.8 > "C:\Users*Username*\Desktop\find google.txt"

7. **Take a screenshot** of your File Explorer window showing the files you created in this project from Step 2 through Step 6; submit this visual with your answers to this project's questions.

   Answer: Screenshot should show the File Explorer window with at least three files listed: *ipconfigtest.txt*, *connections.txt*, and *find google.txt*. **</EOCNL>**

Project 4-4: Repair a Duplicate IP Address

Estimated time: 15 minutes (+5 minutes for group work, if assigned)

Objective: Given a scenario, troubleshoot general networking issues. (Obj. 5.5)

Group work: This project includes enhancements when assigned as a group project.

Resources:

- Windows 10 computer with administrative access

Context:

ARP can be a valuable troubleshooting tool for discovering the identity of a machine whose IP address you know, or for identifying two machines assigned the same IP address. Let's see what happens when two devices on the network are assigned the same IP address. First you change the IP address of a local Windows machine to match an IP address of another device—in other words, you "break" the computer. Then you see how the arp command helps you diagnose the problem. Complete the following steps:

1. Open a PowerShell or Command Prompt window and enter the command **arp –a**. Your device's IP address is listed as the Interface address at the top of the list. Write down this IP address and the address of another device on the network.

2. Open the Network and Sharing Center, click **Change adapter settings**, right-click the active network connection, and click **Properties**. If necessary, enter an administrator password in the UAC box and click **Yes**.

3. Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**. Set the IP address to match the other device's IP address that you wrote down in Step 1. The system automatically assigns the Subnet mask, as shown in Figure 4-37. Also assign the

Cloudflare public DNS servers: 1.1.1.1 and 1.0.0.1. Click **OK** and then click **Close**.

4. Back at the CLI, enter **ipconfig /all**.
5. Find the appropriate network connection and identify your computer's current IPv4 address. Answer the following questions:

    a. Has your computer identified the duplicate IP address problem yet? How do you know?

    Answer: Most likely, the computer has identified the duplicate IP address problem and labels the IP address as a duplicate.

    b. Your computer might also have autoconfigured another IP address. If so, what address did your computer resort to?

    Answer: The computer has probably autoconfigured an APIPA address in the range of 169.254.0.1-169.254.255.254.

    c. **Take a screenshot** of your TCP/IP configuration information; submit this visual with your answers to this project's questions.</SAL>

    Answer: Screenshot should show output for ipconfig /all with configuration information for the active network interface, including a Duplicate IP address warning and an auto-configured APIPA IP address.

6. In the window on the left side of Figure 4-38, you can see a warning that the IP address is a duplicate. The system also shows a preferred IPv4 address of 169.254.143.79, which is an APIPA address. How can you tell this is an APIPA address?

    Answer: Any IP address in the range of 169.254.0.1-169.254.255.254 is an APIPA address.

7. To confirm the duplication of IP addresses, enter the command **arp –a**. You can see in Figure 4-38 that the local computer's IPv4 address listed on the left matches another IP address in the ARP table on the right, and again you see the APIPA address assigned to the local interface. What are two ways to solve this problem?

    Answer: Answers may vary. One way is to change the static IP address of one or both devices. Another way is to configure the local device to use DHCP.

8. **For group assignments:** Run the **arp -a** command in your CLI window and answer the following questions:

    a. How many other APIPA addresses appear in the output?

    Answer: Answers may vary and should include the number of other APIPA addresses listed.

b. Which ones belong to your group members?

Answer: Answers may vary and should identify which APIPA addresses belong to other group members.

c. How many digits in these APIPA addresses are the same for all group members?

Answer: The first two octets are the same for all APIPA addresses: 169.254. In some cases, some additional digits might also be the same.

9. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box again and select the options **Obtain an IP address automatically** and **Obtain DNS server address automatically** and then click **OK.** Close all active windows except your CLI.

10. Run the **ipconfig** command or the **arp –a** command to confirm that a unique IP address has been assigned to your local device's active network interface. What is the new IP address?

    Answer: Answers may vary and should include a private IPv4 address.

11. Close the PowerShell or Command Prompt window.

Capstone Projects

Capstone Project 4-1: Set Up and Use a TFTP Server in Packet Tracer

Estimated time: 30 minutes

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

Resources:

- Computer with Cisco Packet Tracer installed

Context:

In Capstone Project 2-2, you installed Packet Tracer, and you used it again in Capstone Project 3-2. Earlier in this module, you learned about TFTP servers that can be used to back up and configure network devices. In this Capstone Project, you configure a router, back up the router configuration on a TFTP server, and then create a replacement router from the backup file. Note that Cisco devices keep active configuration settings in a file called running-config. There are actually two files: The startup-config file provides initial settings when the device boots, and the running-config file maintains those settings in the device's memory while it is powered on. When you make changes to the running-config file, that does not change the startup-config file, which means your settings are lost on the device's next power cycle. You can copy the running-config file contents to the

startup-config file for later access. In this project, you'll focus on working with the running-config file. Complete the following steps:

1. Open Packet Tracer and, if necessary, sign in with your Networking Academy account.
2. In the Devices pane, click Network Devices category and then click Routers. Add a PT-Router to your workspace. Below the router's icon in the workspace, change the router's display name to RtrGiraffe. Add a note to indicate the router's IP address: 192.168.2.1/24
3. Click the router to open its configuration window. Click the Config tab. Change the hostname to RtrGiraffe. As you make this change, notice the commands scrolling in the Equivalent IOS Commands pane at the bottom of the window.
4. Under INTERFACE, click FastEthernet0/0. Set the router's IP address to 192.168.2.1. The subnet mask field should automatically populate with 255.255.255.0. Check the On box to activate the port.
5. In the Devices pane, click End Devices category. Add a Server to your workspace. Below the server's icon in the workspace, change the server's display name to TFTPserver. Add a note to indicate the server's IP address: 192.168.2.100/24
6. Click the server to open its configuration window. Click the Config tab and click FastEthernet0. Set the server's IP address to 192.168.2.100. The subnet mask field should automatically populate with 255.255.255.0.
7. In the Devices pane, click Connections category. Because you're connecting a server directly to a router, you need a crossover cable, which you'll learn more about later in this course. Click the straight, dashed line for the Copper Cross-Over cable and connect the FastEthernet0/0 interface on the router with the FastEthernet0 interface on the server.
8. In the server's configuration window, click the Desktop tab and click Command Prompt. Ping the router to confirm the connection works. What command did you use?

   Answer: ping 192.168.2.1

The server's TFTP service is on by default, so you're now ready to back up the router's running-config file to the server. You'll need to perform this task from the router's CLI. Complete the following steps:

9. In the router's configuration window, click the CLI tab. Click inside the IOS Command Line Interface pane and press Enter. The prompt should show RtrGiraffe (config-if)#. This prompt gives you some helpful information:
   a. The router's hostname is RtrGiraffe.
   b. The router's CLI is currently in the interface configuration mode, which is what

you used to configure the FastEthernet0/0 interface. To exit this mode, enter exit.

10. Your router is now in global configuration mode, indicated by the (config)# portion of the prompt. You need to step down one more mode level, so enter exit again and then press Enter.

11. Your router is now in privileged EXEC mode, which is what you need to copy the running-config file to the TFTP server. Enter the command copy running-config tftp, which instructs the router to copy its running-config file to the TFTP server. You'll need to provide a little more information:

    a. Enter the server's IP address: 192.168.2.100

    b. Enter the name of the file to be saved on the server: Giraffe

Now you're ready to check the logs on the TFTP server to confirm the file was copied successfully. Complete the following steps:

12. In the server's configuration window, click the Services tab and then click TFTP in the left pane. Take a screenshot of the logs, which should show the Giraffe entry at the top. Submit this visual with your answers to this project's questions.

    Answer: Screenshot should show TFTPserver's configuration window on the Services tab with TFTP logs indicating the Giraffe file was saved to TFTPserver.

Suppose your existing router fails, and you need to replace it with a new router. In the real world, you likely would have made many more configuration changes than simply the router's hostname and IP address. It would be time consuming and risky to attempt to copy this configuration manually to a new router. But you are prepared and have a backup configuration file! You're now ready to create a new router and copy the configuration file to this router. Complete the following steps:

13. From the Devices pane, add a new PT-Router to your workspace. Give this router the display name and hostname RtrZebra and set the FastEthernet0/0 interface to the same IP address as the first router: 192.168.2.1. Be sure to make these changes to the documentation in your workspace and to the router's configuration settings. The workspace documentation is for your benefit, but the router only knows about changes made within its configuration window.

14. Grab RtrGiraffe's end of the cable and drag it to RtrZebra, connecting the cable to the FastEthernet0/0 interface, as shown in Figure 4-39. From the server, ping the new router to confirm the connection works. What command did you use?

    Answer: ping 192.168.2.1

15. In RtrZebra's configuration window, click the CLI tab. Click inside the IOS Command Line Interface pane and press Enter. What is this router's hostname, as indicated by the prompt?

    Answer: RtrZebra

16. Enter the exit command twice and press Enter again to get to privileged EXEC mode.

17. To copy the old router's running-config file from the TFTP server to the new router, enter the command copy tftp running-config. Provide the TFTP server's IP address and the filename to be copied (Giraffe). Press Enter twice. What is the new router's hostname now, as indicated by the prompt? Why do you think this is?

    Answer: RtrGiraffe

    Answer: The old router was configured with the hostname RtrGiraffe. When its running-config file was copied onto the new router, the new router's hostname was changed to RtrGiraffe as well.

18. At this point, if you were to power cycle the new router, it would lose all these settings. To save the running-config data to the startup-config file so the changes persist, enter the command copy running-config startup-config

19. You do not need to save this Packet Tracer network for future projects. Before closing the network, take some notes in your Wikidot website about your work in this project, commands that you learned, and new insights you have about how Packet Tracer works.

Capstone Project 4-2: Use SSH in Ubuntu

Estimated time: 30 minutes (+5 minutes for group work, if assigned)

Objective: Compare and contrast remote access methods and security implications. (Obj. 4.4)

Group work: This project includes enhancements when assigned as a group project.

Resources:

- Access to the same computer used to complete Capstone Project 1-1 or Capstone Project 1-2
- Internet access

Context:

In this project, you will learn to use SSH in Ubuntu. Using the Ubuntu VMs you created in Capstone Projects 2-1 and 3-1, follow these steps to create a SSH connection.

Note 4-18

If you're using VirtualBox, you first need to check the Network settings for this VM. Select the VM, click **Settings**, and click **Network**. If necessary, change the *Attached to* setting to **Bridged Adapter**. Click OK.

On the Ubuntu Server VM, do the following: **<EOCNL>**

1. Start the VM and log on. Refer to your LastPass vault if you don't remember your logon information.
2. SSH is included in Ubuntu Server but is not installed. Enter this command to install and start SSH: **sudo apt-get install ssh** (You'll have to enter your password, and you'll have to give permission to install the software.)
3. Enter the command **ip address show** and write down the IP address of the Ubuntu Server VM. Leave this VM running. **</EOCNL>**

On the Ubuntu Desktop VM, do the following: **<EOCNL>**

4. Start the VM and log on. Refer to your LastPass vault if you don't remember your logon information.
5. Open a shell prompt and enter the command **ip address show**. Note the IP address of the Ubuntu Desktop VM.
6. Enter the **ssh** command with the IP address of the Ubuntu Server VM. For example, if the server IP address is 192.168.1.147, enter this command:

   ssh 192.168.1.147

   If your username on the Ubuntu Server machine is not the same as your username on the Ubuntu Desktop machine, you'll need to add a bit more information to this command to remote into the server. Try this command instead:

   ssh *server_username@server_ipaddress*

   For example, if the server IP address is 192.168.1.147 and the server username is jillwest, you would enter this command:

   ssh **jillwest@192.168.1.147**
7. Enter your password on the server to log on to the server using SSH. You now have a SSH session established between the Ubuntu Desktop VM and the Ubuntu Server VM.
8. Enter the **dir** command. What directory is listed? Recall that you created this directory in Capstone Project 3-1.

   Answer: mydir

9. Enter the **ip address show** command. Which IP address is displayed in the command output: the Ubuntu Desktop VM's address or the Ubuntu Server VM's address?

   Answer: The Ubuntu Server VM's IP address

10. **Take a screenshot** of your Ubuntu Desktop VM's Terminal window showing your commands run on the SSH session with the Ubuntu Server VM; submit this visual with your answers to this project's questions.

    Answer: Screenshot should show the Ubuntu Desktop Terminal window with output from the commands dir and ip address show run on the Ubuntu Server's SSH connection.

11. When you're finished using the SSH session, enter the **exit** command to break the session.

12. **For group assignments:** Establish a SSH session with another group member's Ubuntu VM, either their Desktop VM or their Server VM. The VM's owner will need to enter their credentials to authenticate the connection. What command did you use to establish the connection? (Note that this should work from a Hyper-V VM to a VirtualBox VM but might not work in reverse.)

    Answer: ssh *vm_username@vm_ipaddress*

13. To shut down each VM, enter the **sudo poweroff** command in each VM.

14. Add some notes to your Wikidot website about the SSH installation on the Ubuntu Server VM.

MindTap

Reflection Discussion 4: Linux Distros

Because Linux is a free, open source operating system, many companies and individuals have developed their own version of Linux. Each of these is called a distribution, or distro for short. You've already worked with Ubuntu (pronounced *oo-boon-too*). Other popular Linux distros include MX Linux, Linux Mint, Debian, Elementary OS, Fedora, openSUSE (pronounced *soo-suh*), and Kali Linux. Note that while the Linux OS itself is free, some distros include other tools, trademarks, or support services, which incur a charge. One example of this is the robust Red Hat Enterprise Linux.

Do some research online about three of these Linux distros. Find videos that show demonstrations and basic tutorials for using them. Then respond to the following questions:

- Which three Linux distros did you research?
- What are strengths and weaknesses of each?
- Which one is your favorite and why?

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 4: RSS Feeds

So far in this course, you've explored CompTIA resources for continuing education, researched information about working in IT, and found some interesting podcasts to keep your networking knowledge up-to-date. Another great resource with regularly updated information in a consumer-friendly format is RSS feeds. These articles, blog posts, and even videos can be fed to your favorite RSS reader, such as Feedly, NewsBlur, or Winds. When you're waiting in line at the grocery store, hanging out a café, or riding on the bus, you can check your RSS reader for recent posts and refresh your knowledge with an investment of just a few minutes a day.

Respond to the following questions:

- Check out each of the RSS readers listed above—Feedly, NewsBlur, and Winds. Which one appeals to you the most? Add that app to your smartphone, tablet, or laptop.
- Find three RSS feeds related to networking that look interesting to you and follow them in your RSS reader. Some suggestions include: Reddit Networking (*reddit.com/r/networking/.rss*), Network World (*networkworld.com/index.rss*), Cisco Blog—Enterprise Networks (*blogs.cisco.com/eneterprise/feed*), and Network Computing (*networkcomputing.com/topic/networking*). Which three did you choose?
- Read at least one article from one of your RSS feeds. What's something you learned from the article?

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

Rubric for Hands-on Projects and Capstone Projects

Criteria	Beginning	Developing	Proficient	Exemplary	Score
Responses to questions	All missing or incorrect	Most missing or incorrect	Little missing or incorrect	All complete **[25 points]**	

	[0 points]	**[15 points]**	**[20 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 performance requirements of the assignment **[0 points]**	Student retains their existing understanding while attempting to meet the performance requirements of the assignment **[15 points]**	Student challenges their existing understanding and shows evidence of new learning **[20 points]**	Student challenges their existing understanding and displays 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	Self-reflective discussion with specific and	

		supporting evidence **[40 points]**	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 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]**	
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	