Solution and Answer Guide

Jill West, CompTIA Network+ Guide to Networks, 9th Edition, ISBN: 9780357508138; Module 3: Addressing

Table of Contents

Text

Applying Concepts

Applying Concepts 3-1: Identify a NIC Manufacturer

Most network packets include the MAC address of the sender, the receiver, or both. When collecting network data on Wireshark using the default settings, some OUIs are automatically resolved, telling you the manufacturer of each device. In Figure 3-2, you can see where Wireshark has identified the manufacturers—TP-Link and ASUS—of two NICs on this network.

Sometimes, however, you might be working with physical addresses provided by a command output, or you might need a little more information than what is provided by a Wireshark capture. For these situations, use an online MAC address lookup table such as Wireshark's OUI Lookup Tool. Complete the following steps:

1. In your browser, go to **wireshark.org/tools/oui-lookup**.
2. Notice earlier in Figure 3-2 that the MAC addresses of the Source and Destination devices are listed in the Ethernet frame. The first three bytes of the Destination device's MAC address, 40:16:7e, make up the OUI of the device's manufacturer. Type those numbers into Wireshark's OUI Lookup Tool and click **Find**. What results did you get?

   Answer: 40:16:7E ASUSTek COMPUTER INC.

Note 3-5
If you are pulling OUIs from your own Wireshark capture or command-line output, you can copy and paste one or more OUIs into the website search box.

You can perform the same lookup using output from a PowerShell or Command Prompt window:

3. Open a PowerShell or Command Prompt window and enter **ipconfig /all** to identify your NIC's MAC address.
4. From your command output, select the first three bytes of the physical address for the active network connection and press **Ctrl**+**C**. *Note:* You might need to first press **Ctrl**+**M** to enable marking.
5. Click in the search box on Wireshark's website, press **Ctrl**+**V** to paste the information into the Wireshark Lookup Tool, and click **Find**. Who is the manufacturer of your NIC?

   Answer: Answers will vary and should identify a network device manufacturer, such as ASUS, TP-Link, Cisco, Aruba, Dell, Huawei, Samsung, Arista, Apple, Netgear, Intel, or many others.

Applying Concepts 3-2: Windows TCP/IP Settings

Let's begin with a look at IP addresses and related TCP/IP settings on a Windows 10 computer. Take note that, if you're using a computer with Hyper-V enabled, you might see a few interesting variations as you click through the screens in this module. For example, a computer not running Hyper-V will likely show a direct connection to your LAN, as shown in Figure 3-5a. A computer that is running Hyper-V will likely show a connection to your virtual switch that you created in Module 1, as shown in Figure 3-5b. You'll learn more about why this is the case in a later module when you study virtualization technologies more closely.

To check TCP/IP settings on your Windows computer, complete the following steps:

1. Click **Start** and then click the **Settings** gear icon. Click **Network & Internet**. Alternatively, you can right-click the active network connection icon on the right side of your taskbar near the date and time (see Figure 3-6) and then click **Open Network & Internet settings**.

2. Click **Change connection properties** and scroll down to the IP settings and Properties sections. Figure 3-7 shows the TCP/IP settings, including IP assignment source (Automatic from DHCP), IPv6 and IPv4 addresses, DNS servers, and Physical address (MAC).

3. You probably have the Automatic (DHCP) option enabled, which dynamically assigns an IP address from a DHCP server. The Properties section shows your IP address, MAC address, and DNS (Domain Name Service) servers. DNS servers are responsible for tracking computer names and their IP addresses. Later in the module, you'll learn more about the various types of DNS servers and how they work together.

You can find similar information and more using the **ipconfig** utility, which you first used in Project 2-3 while working with Nmap. You'll learn more about this utility later in this module. Network technicians need to be comfortable with the CLI (command line interface) because it is quicker and often more powerful and flexible than a GUI (graphical user interface). To see the additional information ipconfig reports, complete the following steps:

4. Open a PowerShell or Command Prompt window and enter **ipconfig**. What are your IPv4 address, subnet mask, and default gateway settings for your active network connection?

   Answer: Answers may vary and should include a private IPv4 address, subnet mask, and default gateway address.

Note 3-6

Notice that ipconfig by itself does not output the MAC address. You must use the /all parameter to see the MAC address, which you did earlier in Applying Concepts 3-1.

Here's a brief explanation of the subnet mask and default gateway settings:

- A s**ubnet mask**, also called a netmask, is a 32-bit number that helps one computer find another. The 32 bits are used to indicate what part of an IP address's bits are the network portion, called the **network ID** or network address, and which bits consist of the host portion, called the **host ID** or **node ID**. Using this information, a computer can determine if another computer with a given IP address is on its own or a different network.

- A **gateway** is a computer, router, firewall, or other device that a host uses to access another network. The **default gateway** is the routing device that nodes on the network turn to for access to the outside world. In the *On the Job* story at the beginning of this module, you read about a problem that appeared to be a DNS issue but was, in fact, a missing default route that prevented network nodes from reaching DNS servers outside the local network. The default gateway provides a connection to all resources outside the local network when static routes aren't available (which is most of the time).

Note 3-7

Technically, there is a subtle distinction between the meanings of the terms *subnet mask* and *netmask*. A **subnet** is a smaller network within a larger network. A netmask indicates the bits of an IP address that identify the larger network, while the subnet mask indicates the bits of an IP address that identify a smaller subnet within the larger network. Most of the time, however, these two terms are used interchangeably. You'll learn more about subnets in a later module.

Applying Concepts 3-3: Configure a DHCP Server

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

While each type of DHCP server software is configured differently, they offer many options in common. Generally, you define a range of IP addresses, called a **DHCP scope** or DHCP pool, to be assigned to clients when they request an address. For example, Figure 3-9 shows a screen provided by the firmware utility for a home router, which is also a DHCP server.

Using this screen, you set the starting IP address (192.168.2.100 in the figure) and the ending IP address (192.168.2.199 in the figure) of the DHCP scope. The scope includes the following additional information, called **scope options**:

A time limit, called a **lease time**, which restricts the amount of time a network host can keep the IP address before it must request a renewal. When the lease time expires without renewal, the DHCP server returns the IP address to the available address pool.

- The default gateway's IP address, which each client must know to send messages to hosts on other networks. The default gateway is typically a router or firewall.

- The primary and secondary DNS server addresses, which clients use to match computer names with IP addresses. DNS servers might be internal to the local network or external and

accessed through the default gateway, like you saw in the *On the Job* story at the beginning of this module.

When other nodes on the network frequently need to know the IP address of a particular client, you can have DHCP offer that client the same IP address every time it requests one. The DHCP server recognizes this client based on its MAC address, so this reserved IP address is called a variety of names: **MAC reservation**, **IP reservation**, or **DHCP reservation**. For example, a network printer should consistently use the same IP address so that computers on the network can always find it. In Figure 3-10, which shows the management interface for a TP-Link SOHO router, an OKI Data network printer has a reserved IP address of 192.168.2.200.

Note 3-8

A reserved IP address is not quite the same thing as a static IP address. A reserved IP address is offered to the client by DHCP when the client requests an IP address. A static IP address is configured on the client itself so that the client never requests an IP address from DHCP in the first place. If you have one or more clients on the network with static IP addresses, you need to configure an IP **exclusion range** on the DHCP server. This excludes one or more IP addresses from the IP address pool so the server doesn't offer those IP addresses to other clients.

In Linux systems, you configure the DHCP software by editing a configuration file in a text editor. For example, the configuration file for one Linux distro's DHCP server is dhcpd.conf (notice the .conf file extension), which is stored in the /etc/dhcp directory. Figure 3-11 shows the configuration file as it appears in vim, which is a Linux text editor. A hash symbol (#) at the beginning of a line identifies the line as a comment line (a line that is not executed). The range of IP addresses that will be assigned to clients in Figure 3-11 is 10.254.239.10 to 10.254.239.20, which consists of 11 IP addresses.

Applying Concepts 3-4: Configure Address Translation Using

For simple default gateways such as a home router, configuring address translation means making sure NAT is turned on. That's about all you can do. However, for more advanced gateways, such as an industrial-grade Cisco router or Linux server, you configure the NAT software by editing NAT translation tables stored on the device. For example, suppose your network supports a web server available to the Internet, as shown in Figure 3-14.

On the web, the website is known by the public IP address 69.32.208.74. Figure 3-15 shows the sample text file required to set up the translation tables for DNAT to direct traffic to the web server at private IP address 192.168.10.7. Note that any line beginning with an exclamation mark (!) is a comment.

The first section of code defines the router's outside interface, which connects with the outside network and is called the serial interface. The second section defines the router's inside Ethernet interface. The last line that is not a comment line says that, when clients from the Internet send a request to IP address 69.32.208.74, the request is translated to the IP address 192.168.10.7.

At the end of this module, you'll create your own NAT translation table entry using this example as a template. To help you better understand where the IP addresses in a translation table entry come from, answer the following questions about the information in Figures 3-14 and 3-15:

1. What is the router's outside interface IP address?

   Answer: 69.32.208.100

2. What is the router's inside interface IP address?

   Answer: 192.168.50.1

3. What is the website's public IP address?

   Answer: 69.32.208.74

4. What is the private IP address of the active web server?

   Answer: 192.168.10.7

Applying Concepts 3-5: Change DNS Servers

In Applying Concepts 3-2, you practiced finding TCP/IP settings on a Windows 10 computer using the Settings app and the CLI. You might have noticed that, in the Settings app, you could only change the DNS settings if you turned off DHCP. While it's possible to set preferred DNS servers without disabling DHCP, you must do so in Control Panel. It's a bit of a challenge to find Control Panel in Windows 10. Here are a few options:

- In the Search box, start typing **control** and press **Enter** when the Control Panel app appears.
- Press **Win+R**, type **control**, and press **Enter**.
- Click **Start**, scroll down and click **Windows System**, and then click **Control Panel**.

You can pin Control Panel to the Start menu or to your taskbar at the bottom of your screen to make it more accessible in the future. With Control Panel open, right-click its icon in the taskbar, and click **Pin to taskbar**.

When Control Panel is used for projects in this course, steps are written for the Large icons view unless stated otherwise. This generally makes the most important items to technicians easier to access. To change the view in Control Panel, click the **View by** drop-down menu in the top right corner of the window. Windows will usually remember the last view you used the next time you open Control Panel.

As for DNS servers, in most cases, your computer is probably using the DNS servers your ISP provides. For various reasons (such as performance improvements, filter options, or outage problems), you might want to change your DNS servers to third-party options such as Google Public DNS, OpenDNS, Cloudflare, or Verisign DNS. You can search online for these DNS servers' IP

addresses. Then complete the following steps to configure your Windows 10 computer to refer to one of these DNS providers instead:

1. In Control Panel, click **Network and Sharing Center**. In the left pane, click **Change adapter settings**.
2. Right-click the active network connection and click **Properties**. In the connection's properties dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**. See Figure 3-23.
3. Select *Use the following DNS server addresses* to manually assign DNS server addresses. For example, if you want to use Cloudflare's DNS servers, you would enter 1.1.1.1 as the Preferred DNS server and 1.0.0.1 as the Alternate DNS server. Then click **OK**. Which DNS servers did you decide to use?

   Answer: Answers may vary and should state that the student either decided to stick with the ISP's default DNS servers or should list the DNS provider selected.

Review Questions

1. Which part of a MAC address is unique to each manufacturer?

   a. The network identifier

   b. The OUI

   c. The device identifier

   d. The physical address

   Answer: b. The OUI

   Explanation: The first 24 bits of a MAC (Media Access Control) address are known as the **OUI (Organizationally Unique Identifier)**, which identifies the NIC's manufacturer. The last 24 bits make up the extension identifier or device ID and identify the device itself. The entire MAC address is also called a physical address. The first part of an IP address identifies the network.

2. What type of device does a computer turn to when attempting to connect with a host with a known IP address on another network?

   a. Default gateway

   b. DNS server

   c. Root server

   d. DHCP server

Answer: a. Default gateway

Explanation: The **default gateway** is the routing device that nodes on the network turn to for access to the outside world. A DNS (Domain Name Service) server helps to find the IP address when that information is not known. A root server is a type of DNS server. A DHCP (Dynamic Host Configuration Protocol) server manages the dynamic distribution of IP addresses to devices on a network.

3. What decimal number corresponds to the binary number 11111111?

    a. 255

    b. 256

    c. 127

    d. 11,111,111

Answer: a. 255

Explanation: The largest possible 8-bit number is 11111111, which is equal to **255** in decimal. When counting 00000000, there are 256 possible 8-bit values for each octet in an IPv4 address. An IPv4 loopback address can fall anywhere in the range of 127.0.0.1 through 127.255.255.254. The decimal number 11,111,111 is equal to 101010011000101011000111 in binary.

4. Suppose you send data to the 11111111 11111111 11111111 11111111 IP address on an IPv4 network. To which device(s) are you transmitting?

    a. All devices on the Internet

    b. All devices on your local network

    c. The one device that is configured with this IP address

    d. No devices

Answer: b. All devices on your local network

Explanation: The largest possible IP address in decimal is 255.255.255.255. In binary, this number is written 11111111.11111111.11111111.11111111. The address 255.255.255.255 is used for broadcast messages by TCP/IP background processes, and a broadcast message is read by **all devices on your local network**.

5. When your computer first joins an IPv6 LAN, what is the prefix of the IPv6 address the computer first configures for itself?

    a. FF00::/8

b. ::1/128

c. 2000::/3

d. FE80::/64

Answer: d. FE80::/64

Explanation: During IPv6 autoconfiguration, the computer creates its IPv6 address and uses **FE80::/64** as the first 64 bits. FF00::/8 is the prefix for multicast addresses. Global unicast addresses begin with 2000::/3. The address ::1/128 is the loopback address and is used to test that an interface and supporting protocol stack is functioning properly.

6. If you are connected to a network that uses DHCP, and you need to terminate your Windows workstation's DHCP lease, which command would you use?

   a. ipconfig /release

   b. ipconfig /renew

   c. ifconfig /release

   d. ifconfig /renew

   Answer: a. ipconfig /release

   Explanation: The command **ipconfig /release** releases the IP address when dynamic IP addressing is being used. The command ipconfig /renew leases a new IP address from a DHCP server. The ifconfig command is a Linux command. While you can use ifconfig to release an IP address, you don't accomplish this with the /release parameter.

7. Which of these commands has no parameters in Windows?

   a. ping

   b. ipconfig

   c. hostname

   d. nslookup

   Answer: c. hostname

   Explanation: The **hostname** command displays a device's host name, either in Windows, UNIX, or Linux systems. In Windows, hostname has no additional parameters. The ping, ipconfig, and nslookup commands offer many parameters and options in Windows.

8. Which DNS server offers the most current resolution to a DNS query?

   a. Primary DNS server

b. Root DNS server

c. Caching DNS server

d. TLD DNS server

Answer: a. Primary DNS server

Explanation: A **primary DNS server** is the authoritative name server for the organization, which is the authority on computer names and their IP addresses for computers in their domains and always holds the most current records. All other DNS servers, such as caching DNS servers and forwarding DNS servers, can only offer aged information held in their caches. Thirteen clusters of root DNS servers hold information used to locate the TLD (top-level domain) servers. These TLD servers hold information about how to find the authoritative name servers owned by various organizations.

9. You have just brought online a new secondary DNS server and notice your network-monitoring software reports a significant increase in network traffic. Which two hosts on your network are likely to be causing the increased traffic and why?

    a. The caching and primary DNS servers because the caching server is requesting zone transfers from the primary server

    b. The secondary and primary DNS servers because the secondary server is requesting zone transfers from the primary server

    c. The root and primary DNS servers because the primary server is requesting zone transfers from the root server

    d. The web server and primary DNS server because the web server is requesting zone transfers from the primary DNS server

    Answer: b. The secondary and primary DNS servers because the secondary server is requesting zone transfers from the primary server

    Explanation: When a secondary DNS server needs to update its database or when it comes online for the first time, it makes the request to the primary server for the information. **The secondary and primary DNS servers then perform a zone transfer from the primary server to the secondary server**. A caching server adds information to its cache only as it encounters that information will resolving DNS queries. A root DNS server holds information used to locate the TLD (top-level domain) servers. A web server does not perform a zone transfer.

10. Which type of DNS record identifies an email server?

    a. AAAA record

b. CNAME record

c. MX record

d. PTR record

Answer: c. MX record

Explanation: An **MX (mail exchanger)** record identifies an email server and is used for email traffic. AAAA (address) records (called a "quad-A record") hold the name-to-address mapping for IPv6 addresses. CNAME (canonical name) records hold alternative names for a host. A PTR (pointer) record is used for a reverse lookup, also called rDNS (reverse DNS), which provides a host name when you know its IP address.

11. What is the range of addresses that might be assigned by APIPA?

    Answer: 169.254.0.1 through 169.254.255.254

12. You are the network manager for a computer training center that allows students to bring their own laptops to class for learning and taking notes. Students need access to the Internet, so you have configured your network's DHCP server to issue IP addresses automatically. Which DHCP option should you modify to make sure you are not wasting addresses used by students who have left for the day?

    Answer: Lease time

13. You have decided to use SNAT and PAT on your small office network. At minimum, how many IP addresses must you obtain from your ISP for all five clients in your office to be able to access servers on the Internet?

    Answer: 1

14. Explain how the bits of an IPv6 address are organized and describe IPv6 shorthand notation.

    Answer: An IPv6 address has 128 bits that are written as eight blocks (also called quartets) of hexadecimal numbers separated by colons. Each block is 16 bits long. Leading zeroes in a four-character hex block can be eliminated. If blocks contain all zeroes, they can be eliminated and replaced by double colons (::). To avoid confusion, only one set of double colons is used in an IPv6 address.

15. FTP sometimes uses a random port for data transfer, but an FTP server always, unless programmed otherwise, listens to the same port for session requests from clients. What port does an FTP server listen on?

    Answer: 21

16. You issue a transmission from your workstation to the following socket on your LAN: 10.1.1.145:53. Assuming your network uses standard port designations, what application

layer protocol handles your transmission?

Answer: DNS (Domain Name Service)

17. Suppose you want to change the default port for RDP as a security precaution. What port does RDP use by default, and from what range of numbers should you select a private port number?

    Answer: 3389; 49152 through 65535

18. You have just set up a new wireless network at your house, and you want to determine whether your Linux laptop has connected to it and obtained a valid IP address. What command will give you the information you need?

    Answer: ip address show or ifconfig -a

19. While troubleshooting a network connection problem for a coworker, you discover the computer is querying a nonexistent DNS server. What command-line utility can you use to assign the correct DNS server IP address?

    Answer: nslookup (in interactive mode)

20. When running a scan on your computer, you find that a session has been established with a host at the address 208.85.40.44:443. Which application layer protocol is in use for this session? What command-line utility might you use to determine the domain name of the other computer?

    Answer: Port 443 indicates this an HTTPS session.

    Answer: nslookup can identify the domain name of the host at that IP address.

Hands-On Projects

Note 3-19

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 3-1: Create a NAT Translation Table Entry

Estimated time: 20 minutes

Objective: Given a scenario, configure a subnet and use appropriate IP addressing schemes. (Obj. 1.4)

Resources:

- No special resources required

Context:

Your corporation hosts a website at the static public IP address 92.110.30.123. A router directs this traffic to a web server at the private IP address 192.168.11.100. However, the web server needs a hardware upgrade and will be down for two days. Your network administrator has asked you to configure the router so that requests to the IP address 92.110.30.123 are redirected to the backup server for the website, which has the private IP address 192.168.11.110. The router's inside Ethernet interface uses IP address 192.168.11.254, and its outside interface uses the IP address 92.110.30.65. Answer the following questions about the new static route you'll be creating:

1. What is the router's outside interface IP address?

   Answer: 92.110.30.65

2. What is the router's inside interface IP address?

   Answer: 192.168.11.254

3. What is the website's public IP address?

   Answer: 92.110.30.123

4. What is the private IP address of the backup web server?

   Answer: 192.168.11.110

Use the example given in Figure 3-15 earlier in the module as a template to create the NAT translation table entries for the address translation. For the subnet masks, use the default subnet mask for a Class C IP address license. Include appropriate comment lines in your table. **Take a screenshot of your NAT translation table**; submit this visual with your answers to this project's questions.

Answer: Comments may vary, otherwise the screenshot should show the following information:

interface serial 0/0

ip address 92.110.30.65 255.255.255.0

ip nat outside

!--- Defines the serial 0/0 interface as the router's NAT outside interface

!--- with an IP address of 92.110.30.65

```
interface ethernet 1/1
ip address 192.168.11.254 255.255.255.0
ip nat outside

!---Defines the Ethernet 1/1 interface as the router's NAT inside interface
!---with an IP address of 192.168.11.254

ip nat inside source static 192.168.11.110 92.110.30.123

!--- States that source information about the inside host will be translated
!--- so the host's private IP address (192.168.11.110) will appear as the
!--- public IP address (92.110.30.123). Both ingoing and outgoing traffic
!--- exchanged with the public IP address will be routed to the host at the
!--- private IP address.
```

Project 3-2: Change IPv6 Autoconfiguration Settings

Estimated time: 20 minutes (+15 minutes for group work, if assigned)

Objective: Given a scenario, configure a subnet and use appropriate IP addressing schemes. (Obj. 1.4)

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

Resources:

- Windows 10 computer with administrative access
- Internet access

Context:

By default, when configuring an IPv6 address, Windows 10 generates a random number to fill out the bits needed for the NIC portion of the IPv6 address. This security measure helps conceal your device's MAC address, and it further protects your privacy by generating a new number every so often. There may be times, however, when you need your system to maintain a static IPv6 address. To do this, you can disable IPv6 autoconfiguration using the netsh utility in an elevated PowerShell

or Command Prompt window. Forcing the computer to use SLAAC to generate its IPv6 address will result in the same IPv6 address every time. Complete the following steps:

1. In this project, you'll use the netsh utility. Do some research online about this tool and answer the following questions:

    a. What is netsh used for?

    Answer: Netsh is used to view or modify a computer's network configuration.

    b. What is the role of a netsh context?

    Answer: Each netsh context offers a specific set of features, commands, and subcontexts for interacting with a computer.

    c. What netsh command access the interface context for managing network connections?

    Answer: netsh interface or netsh int

2. Open an elevated PowerShell or Command Prompt window.

3. Enter **ipconfig /all** and find the TCP/IP information for the active network connection. **Take a screenshot** of this information; submit this visual with your answers to this project's questions. What is your computer's current IPv6 address and MAC address? Carefully compare the two addresses. Are they in any way numerically related?

    Answer: Screenshot should show the TCP/IP configuration information for the active network connection in response to the ipconfig /all command, including the MAC address and IPv6 address.

    Answer: IPv6 and MAC addresses will vary. The IPv6 address and the MAC address should not be numerically related.

4. To disable the random IP address generation feature, enter the command:

    netsh interface ipv6 set global randomizeidentifiers=disabled

5. To instruct Windows to use the EUI-64 standard instead of the default settings, enter the command:

    netsh interface ipv6 set privacy state=disabled

Figure 3-38 shows where both commands were entered and accepted.

6. Enter **ipconfig /all** again. What is your computer's new IPv6 address? How closely does this number resemble the MAC address? Notice after *FE80::* that the fixed value FF FE has been inserted halfway through the MAC address values. The host portion of the IPv6 address

might use a slightly different value than the OUI in the MAC address because the seventh bit of the MAC address is inverted.

Answer: IPv6 addresses may vary and should now be very similar to the MAC address.

7. **For group assignments:** Complete the following steps:

    a. Attempt to ping each other's devices using ping -6 and IPv6 addresses. What response did you get?

Answer: Answers may vary, including any of the following possibilities: a successful ping, request timed out, or a general failure.

    b. Attempt to ping Google's IPv6 DNS address on the Internet: 2001:4860:4860::8888. What response did you get?

Answer: Answers may vary, including any of the following possibilities: a successful ping, request timed out, or a general failure.

    c. There are many reasons why pinging an IPv6 address on your local network might not work even if the network and its devices are functioning properly. For example, your LAN might not support IPv6. In some cases, you might have successfully pinged an IPv6 address on your local network but not on the Internet. If one or both of your pings did not work, spend a few moments with your group doing some investigating and troubleshooting to see if you can determine where the IPv6 ping is failing and what you would need to do to fix it. What possibilities did you come up with?

Answer: Possible solutions might include needing to reset TCP/IP configurations, adjust anti-malware software, update device drivers, enabling IPv6 on LAN hardware, and switching to an ISP that supports IPv6.

8. Re-enable random IPv6 address generation with these two commands:

netsh interface ipv6 set global randomizeidentifiers=enabled

netsh interface ipv6 set privacy state=enabled

Project 3-3: Manage a DNS Cache

Estimated time: 10 minutes

Objective: Explain the use and purpose of network services. (Obj. 1.6)

Resources:

- Windows 10 computer with administrative access
- Internet access

Context:

You have learned that clients as well as name servers store DNS information to associate names with IP addresses. In this project, you view the contents of a local DNS cache, clear it, and view it again after performing some DNS lookups. Then you change DNS servers and view the DNS cache once again. Complete the following steps:

1. To view the DNS cache, open an elevated PowerShell or Command Prompt window and enter the following command: **ipconfig /displaydns**
2. If this computer has been used to resolve host names with IP addresses—for example, if it has been used to retrieve email or browse the web—a list of locally cached resource records appears. Read the file to see what kinds of records have been saved, using the scroll bar if necessary. What is the most common record type in this list?

   Answer: Answers may vary and will likely list A (Host) Records or possible CNAME Records or PTR Records.
3. Clear the DNS cache with this command: **ipconfig /flushdns**

   The operating system confirms that the DNS resolver cache has been flushed. One circumstance in which you might want to empty a client's DNS cache is if the client needs to reach a host whose IP address has changed (for example, a website whose server was moved to a different hosting company). If the DNS information is locally cached, the client will continue to look for the host at the old location. Clearing the cache allows the client to retrieve the new IP address for the host.
4. View the DNS cache again with the command: **ipconfig /displaydns**
5. Open a browser window and navigate to three websites you have not recently visited, such as **howstuffworks.com**, **nautil.us**, and **mapcrunch.com**.
6. Return to the PowerShell or Command Prompt window and view the DNS cache containing the new list of resource records. **Take a screenshot** of one of these records that was collected in response to your browser activity; submit this visual with your answers to this project's questions.

   Answer: Screenshot should show one or more resource records related to the websites visited.

Project 3-4: Download and Use an IP Scanner

Estimated time: 20 minutes

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:

- Windows 10 computer with administrative access
- Internet access

Context:

You've already seen the kind of information you can detect about your network devices using Nmap. In this project, you will use a free, popular tool called Advanced IP Scanner to detect devices on your network and determine what additional information an IP scanner can collect. Complete the following steps:

1. Go to **advanced-ip-scanner.com**. Download and install the free application Advanced IP Scanner. When the installation is finished, run Advanced IP Scanner.
2. In the user interface, notice you have two options for the scan: Scan the local machine's subnet or scan a class C subnet. Depending on your network configuration, there might be no difference between these two options. If there is, choose the option that is most appropriate for your network. Also, if you are using the computer on which you installed your VMs from earlier Capstone Projects, the scan might target two IP ranges. What IP range(s) will you be scanning?

   Answer: Answers may vary and will likely include two class C ranges, such as 192.168.0.1-254 and 192.168.56.1-254.
3. When you're ready, click **Scan**. Give the scanner a few minutes to complete the scan.
4. When the scan is complete, **take a screenshot** of the results. Blur out any private information and submit this visual with your answers to this project's questions. Figure 3-39 shows the results of one network scan. Even some devices that do not have names were identifiable by manufacturer, such as the Roku device.

   Answer: Screenshot should show results of a network scan.
5. What surprises you about the results of your scan? Are there any devices you can't identify that you need to research further? Keep in mind that it's important to track which devices are connected to your network to ensure no one is using your network without permission and to ensure no devices are leaking sensitive information to the Internet or being maliciously controlled over the Internet.

   Answer: Answers may vary widely and should discuss the results of the scan and whether devices are connected to the network that shouldn't be.

6. Depending on the device, Advanced IP Scanner offers some remote-control options. For example, right-click one of the devices in your scan results and explore the options in the pop-up menu. Some of these tools require Radmin, which is a free remote access application. You can experiment with this tool if you want to. You also have some command-line tools in Advanced IP Scanner. Use the Ping tool to check the connection with one of the devices on your network. How does this ping function differently than the pings you've run in other projects? When you're ready, press **Ctrl+C** to stop the ping.

   Answer: The ping continues indefinitely.

7. **For group assignments:** One option for remotely accessing a computer through Advanced IP Scanner is RDP for Windows computers. Find another group member's computer in your scan results, right-click, point to **Tools**, and click **RDP**. The other person will need to enter their user account credentials. Alternatively, each group member can create a guest account and share those credentials with group members to use with RDP from Advanced IP Scanner.

8. In your wiki, add a new page titled **Applications:AdvancedIPScanner**. 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 Advanced IP Scanner later.

Capstone Projects

Capstone Project 3-1: Set Up an Ubuntu Server in a VM

Estimated time: 45 minutes

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

Resources:

- Access to the same computer used to complete Capstone Project 1-1 or Capstone Project 1-2
- Internet access
- If desired, instructor can provide Ubuntu Server image file

Context:

In the Module 1 Capstone Projects, you created a virtual machine using Oracle VirtualBox or Windows 10 Client Hyper-V. In Capstone Project 2-1, you added a second VM, this one running Ubuntu Desktop. In this Capstone Project, you create a third VM and install Ubuntu Server in the VM. You also learn how to use some Linux commands. Using the same computer that you used in

Capstone Project 1-1 or 1-2 (which should have Oracle VirtualBox or Client Hyper-V installed and activated), complete the following steps:

1. Go to **ubuntu.com/server** and download the Ubuntu Server OS to your hard drive using **Option 3: Manual install**. If you're given the choice of multiple versions, choose the latest version. The file that downloads is an ISO file.
2. Open the Oracle VM VirtualBox Manager or Hyper-V Manager. Refer back to the directions in the Module 1 Capstone Projects if needed, and give the VM an informative name. Note that if you're using Hyper-V Manager and you use the Quick Create option, click *Local installation source*, deselect *This virtual machine will run Windows (enables Windows Secure Boot)*, and then click *Change installation source*. In VirtualBox, mount the ISO file that contains the Ubuntu Server download to a virtual DVD in your VM.

Note 3-21

Ubuntu Server is only available as a 64-bit OS. To install a 64-bit guest OS in a VM, the host OS must also be 64-bit.

3. Start the VM and install Ubuntu Server, accepting all default settings. Be sure to record your Ubuntu hostname, username, and password in your LastPass vault. When given the option, decline to install any extra software bundled with the OS other than standard system utilities.
4. After you restart the VM, Ubuntu Server launches, which does not have a GUI interface. Enter your username and password to log in. You should now see the shell prompt, as shown in Figure 3-40.
5. Practice using Ubuntu Server by entering, in order, each of the commands listed in Table 3-13. As you do so, you'll examine the directory structure, create a new directory, and put a blank file in it.

Step	Command	Description
1	**pwd**	Displays the full path to the current directory. When you first log in to a system, that directory is /home/*username.*
2	**mkdir mydir**	Creates a directory named mydir. The directory is created in the current directory. You must have permission to edit the current directory.
3	**dir**	Lists files and directories in the current directory. In Linux, a directory is treated more like a file than a Windows folder.

4	**cd mydir**	Goes to the directory you just created in the /home/*username* directory. What is your new shell prompt? Answer: *username*@*servername*:~/mydir$
5	**touch myfile**	Creates a blank file named myfile in the current directory
6	**ls**	Similar to dir, lists current directory contents
7	**cd ..**	Moves up one level in the directory tree. Take a screenshot of the commands you've entered so far and their output; submit this visual with your answers to this project's questions. Answer: Screenshot should show all commands entered so far and their output with evidence of a directory named mydir and a file within that directory named myfile.
8	**cd /etc**	Changes directory to the /etc directory, where text files are kept for configuring installed programs. What is your new shell prompt? Answer: *username*@*servername*:~/etc$
9	**ls**	Examines the contents of the /etc directory
10	**cd /home**	Changes directory to the /home directory
11	**ping 127.0.0.1**	Pings the loopback address. Pinging continues until you stop it by pressing CTRL+C.
12	**CTRL+C**	Breaks out of a command or process; use it to recover after entering a wrong command or to stop a command that requires you manually halt the output.
13	**ifconfig**	Displays basic TCP/IP information and network information, including the MAC address of the NIC
14	**ip address show**	Displays IP and MAC addresses. Notice the difference in output for ifconfig compared to ip address show. What is your VM's IPv4 address? Note that Linux calls this address inet. (Be careful you don't answer with the loopback address! Most likely, the active network connection is on the eth0 interface.) Answer: Answers may vary and should list a private IPv4 address.
15	**ip help**	Displays available objects and options for the ip command

16	**dig google.com**	Performs a DNS lookup on the google.com domain name
17	**df**	Displays the amount of free space on your hard drive. In this case, the VM is reporting on its virtual hard drive.
18	**exit**	Logs out; the login shell prompt appears, where you can log in again. Enter your username and password to log in again.
19	**sudo poweroff**	Elevates privilege to shut down the VM. You'll need to enter your password, and then the system shuts down.

6. Add the new VM's information to your VMclients page in your wiki. On the Virtualization:VMclients page, click **Edit** at the bottom of the page and add the new VM to your list. 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 such as how to view the Linux Manual or how to shut down the system. When you're finished, click **Save**.

7. **Take a screenshot** of the edited wiki page; submit this visual with your answers to this project's questions.

   Answer: Screenshot should show information for at least three VMs, one for each module so far. Information should include hypervisor, virtual resources created, VM name, and VM OS.

Capstone Project 3-2: Build a MAC Address Table in Packet Tracer

Estimated time: 45 minutes

Objective: Given a scenario, configure and deploy common Ethernet switching features. (Obj. 2.3)

Resources:

- Computer with Cisco Packet Tracer installed
- Internet access

Context:

In Capstone Project 2-2, you installed Packet Tracer and practiced interacting with the user interface. Earlier in this module, you learned about MAC address tables that switches use to track which device is connected to each of a switch's ports. In this Capstone Project, you build a small network in Packet Tracer and observe changes to a switch's MAC address table. 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 **Switches**. Add a **PT-Switch** to your workspace. Give the switch a moment to boot.

3. Click **Switch0** to open its configuration window. Click the **CLI** tab. This takes you to the CLI for this switch where you can enter commands to interact with the switch. While Packet Tracer offers some options for configuring devices through their GUIs, the tasks in this project can only be completed from the CLI.

4. Click at the bottom of the IOS Command Line Interface pane in the empty space below "Press RETURN to get started!" Press **Enter** to activate the CLI. By default, you begin in user EXEC command mode, which has the lowest level of privileges in a Cisco device. You can see what mode you're in by looking at the prompt—user EXEC mode shows the prompt *Switch*>. To enter privileged EXEC mode, enter **enable**. The prompt changes to *Switch#*.

5. Now that you're in privileged EXEC mode, you can check the switch's current MAC address table. Enter **show mac address-table**. What entries are listed?

   Answer: None—the table is empty.

6. From the **End Devices** group in the Devices pane, add two **PCs** to your workspace.

7. Click **PC0**. In PC0's configuration window, click the **Desktop** tab and then click **IP Configuration**. In this project and most Packet Tracer projects in this course, you'll set static IP addresses. Enter the following information and then close the configuration window (the information saves automatically):

   IP address: **192.168.0.2**

   Subnet mask: **255.255.255.0**

8. Repeat Step 7 for PC1 and enter the following information for PC1:

   IP address: **192.168.0.3**

   Subnet mask: **255.255.255.0**

9. It's important to get in the habit of keeping good documentation as you work. In the toolbar above your workspace, click the **Place Note (N)** tool. Click under each PC and document that device's IP address and subnet mask, as shown in Figure 3-41.

10. Now you're ready to connect your PCs to your switch. In the Devices pane, click **Connections** and then click the **Copper Straight-Through** cable, which is a thick, black line. Click **PC0** and select its **FastEthernet0** interface. Then click **Switch0** and select its **FastEthernet0/1** interface. Repeat this process for PC1, connecting PC1's **FastEthernet0** interface to Switch0's **FastEthernet1/1** interface. Wait for all indicator lights to turn into green triangles.

11. Access Switch0's CLI again. Click at the bottom of the CLI pane and press **Enter**. Check Switch0's MAC address table. What entries are listed?

    Answer: None—the table is empty.

Note to instructors: If students configure IP address information *after* connecting each PC to the switch, the PCs will start broadcasting their information on the network, and the switch might collect addressing information sooner rather than later. If students follow the steps exactly, the MAC address table should still be empty at this point.

Recall that the switch must see traffic crossing its interfaces to collect MAC addresses for connected devices. To generate traffic, run a ping from PC0 to PC1. Complete the following steps:

12. Click **PC0** and click the **Desktop** tab. Click **Command Prompt**. At the C:\> prompt, enter **ping 192.168.0.3** and wait for the ping to complete.

13. Return to Switch0's CLI and check its MAC address table again. **Take a screenshot** of the output; submit this visual with your answers to this project's questions.

    Answer: Screenshot should show output from the show mac address-table command with two devices listed in the MAC address table.

A switch can only see network traffic that crosses its interfaces. It's possible for traffic from multiple devices to enter a switch at a single switch port. In this case, the switch will record multiple MAC addresses for a single interface. Complete the following steps:

14. Add a second **PT-Switch** and a third **PC**.

15. Configure PC2 with the following information and create a note to document this configuration:

    IP address: **192.168.0.4**

    Subnet mask: **255.255.255.0**

16. In the **Connections** group, click the **Fiber** cable, which is the solid orange line. Click **Switch0** and select its **FastEthernet4/1** interface. Then click **Switch1** and select its **FastEthernet4/1** interface.

17. Use a **Copper Straight-Through** cable to connect PC2's **FastEthernet0** interface to Switch1's **FastEthernet0/1** interface. Wait for all indicator lights to turn into green triangles.

18. Check Switch0's MAC address table again. What entries are listed? Given this information, which connected device is Switch0 currently aware of?

    Answer: One entry for port Fa4/1 is listed. Switch0 is aware of Switch1.

19. Sending a ping between PC2 and PC0 will inform Switch0 of three devices' MAC addresses. Which devices do you expect Switch0 to know about after the ping?

    Answer: Students are asked to pose a theory and answers may vary. The correct answer is PC0, PC2, and Switch1; however, students might guess incorrectly at this point, and this is acceptable.

20. From PC2, ping PC0. Did the ping work?

    Answer: Yes

21. Return to Switch0's CLI and check its MAC address table again. **Take a screenshot** of the output; submit this visual with your answers to this project's questions.

    Answer: Screenshot should show output from the show mac address-table command with three devices listed in the MAC address table.

22. Examine the three devices listed in Switch0's MAC address table and answer the following questions:

    a. How many devices is Switch0 currently aware of?

    Answer: Three devices

    b. Which device is connected to Switch0's Fa0/1 interface? How can you confirm which device matches this MAC address?

    Answer: PC0. You can run ipconfig /all from PC0's Command Prompt window to match the listed MAC address.

    c. Which two devices communicated across Switch0's Fa4/1 interface?

    Answer: Switch1 and PC2

23. Currently, PC1 is not showing in Switch0's MAC address table. What can you do to make Switch0 aware of PC1?

    Answer: Answers may vary. Two options include pinging PC1 from either of the other two PCs, or pinging one of the other PCs from PC1.

24. You do not need to save this Packet Tracer network for future projects. However, 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.

MindTap

Reflection Discussion: CLI vs GUI

In this module, you started learning how to work from the command line to interact with computers and other devices on the network. You even created an Ubuntu Server VM, which doesn't offer a GUI (graphical user interface) at all. At first, working in a CLI (command-line interface) can feel intimidating and unfamiliar, especially if you've not used a CLI before. But it also might provide options to automate functions and to do tasks you can't do from a GUI. Think about your experiences during this module and in the past using both a GUI and a CLI, and do a little reading online to learn about other people's perspectives on this issue. Then respond to the following questions:

- What are some advantages of working with a GUI? Give an example of when a GUI is a better fit for the task.
- What are some advantages of working with a CLI? Give an example of when a CLI is a better fit for the task.
- Which of these user interface types do you prefer 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: Podcasts

Listening to podcasts is an easy and convenient way to continue building on your knowledge, keep up-to-date on networking technology, and develop a greater comfort level with the "lingo" used in networking. Many excellent podcasts are available in networking, cloud computing, cybersecurity, project management, DevOps, and many other areas. You can subscribe to these podcasts and listen to them as you're driving, doing chores, or eating lunch. Do some searching online for a podcast that interests you and schedule regular time in your daily or weekly schedule when you can listen to an episode or two. Some possible suggestions include Network Collective, Zigbits, The Network Insider, The Cloudcast, Software Gone Wild by ipSpace.net, and anything from Packet Pushers. Then respond to the following questions:

- What topic in IT are you most interested in regularly studying on your own time? Possible topics might include networking, cloud computing, cybersecurity, project management, or DevOps.

- What podcast did you find that you plan on listening to regularly?
- Listen to at least one episode. What was discussed in the episode?
- What do you think you can learn from this podcast going forward?

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 **[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 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	Grammar, spelling, punctuation, and	Grammar, spelling, punctuation, and formatting	Grammar, spelling, punctuation, and	

	formatting make student's message difficult to understand **[0 points]**	formatting detract from student's message **[15 points]**	support student's message **[20 points]**	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 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	