Instructor Guide

Computer Networking Fundamentals

LESSON: Network Addressing

Before you Begin

This is the start of the second week for these learners in the extended program. Many of them may feel somewhat overwhelmed. You will find that some are doing very well. Keep in mind that module 4 goes much deeper into layer 2 and layer 3 addressing and introduces technical concepts that may be difficult to grasp for these learners so early in the extended program. For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed:

- Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
- Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
- Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them if needed.
- For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
- Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
- At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.

Summary

In this lesson, learners will explore the structure and limitations of IPv4 addresses, consisting of four sets of numbers separated by periods, representing 8-bit octets. They will understand the

advantages of IPv6, which expands address space, enhances security, and supports modern network technologies. The lesson will introduce MAC addresses, explaining their 48-bit hexadecimal structure and their role as unique identifiers for network interface cards. Learners will also learn about the ARP protocol, used to resolve IP addresses to MAC addresses, and how to display the host ARP table. Additionally, the lesson will cover Wireshark, a network protocol analyzer, teaching learners how to capture and analyze network traffic, filter packets, and follow traffic flow. By mastering these concepts, learners will be able to gain insights into network behavior, troubleshoot issues, and improve network security using Wireshark.

Objectives

- Analyze the structure of an IPv4 address.
- Evaluate the limitations of the IPv4 protocol.
- Describe the key characteristics of the IPv6 protocol.
- Compare the IPv4 and IPv6 protocols.
- Explain the structure of IPv6 addresses.
- Explain the purpose and function of MAC addresses in computer networking.
- Analyze the structure and format of MAC addresses.
- Describe the key characteristics and operation of the ARP protocol.
- Identify the parameters and commands used in ARP tables.
- Describe the importance of using Wireshark as a troubleshooting tool in computer networks.
- Analyze network traffic using Wireshark.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Lesson Opener:** Network Addressing	● Introduce learners to the importance of network addressing.
5 min	**Real World Scenario:** Network Addressing	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
20 min	**Cyber Uncovered:** IPv4	● Define Internet Protocol (IP) as a numerical label assigned to network devices for identification and communication. ● Explain that IP addresses are managed by IANA and divided into regional internet registries (RIRs).

		● Discuss the structure of an IP address. Introduce the concept of a binary digit. Show how IPv4 addresses are divided into four octets. ● Discuss the binary representation of IP addresses using the example: 192.168.1.1 = 11000000.10101000.00000001.00000001. ● Explain the concept of network and host parts in an IPv4 address defined by the subnet mask. ● Explain how the subnet mask is used to identify the network and host address. Discuss an example demonstrating that all hosts on the same network segment all share the same network address but each host has its unique host address. ● Introduce the three main types (classes) of networks: class A, class B, and class C. ● Explain that unicast is one-to-one communication, multicast is one-to-many, and broadcast is one-to-all. ● Explain link-local addresses (APIPA) reserved for communication within the network broadcast domain and how those addresses are generated by the host. ● Define private IP addresses and their purpose in creating non-internet-facing networks. ● Highlight the three ranges reserved for private IPs and their non-uniqueness across separate networks. ● Explain public IP addresses used for internet communication, requiring uniqueness and purchase from service providers. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class to network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
30 min	**Lab:** My First Network	● **Important**: This lab introduces the learner to Cisco Packet Tracer for the first time. Instructors should provide a basic overview of the emulation environment and where to find common objects such as PCs, switches, routers, and cabling. Explain how this emulation environment works and the benefits of using this type of learning tool. Because of this first experience, this lab requires additional time when compared to other similar labs. ● Demonstrate the lab, encourage the learners to participate and ask them to practice this lab and seek assistance as needed during office hours.
5 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.

20 min	**Cyber Uncovered:** IPv6	● Introduce IPv6 as the solution to address the depletion of the IPv4 space as well as the limitations of IPv4 and provide additional enhancements. ● Highlight the larger 128-bit address space in IPv6, offering 340*10^36 available addresses compared to IPv4 using only 32 bits. ● Discuss the long and complex format of IPv6 addresses, consisting of eight blocks with four hexadecimal digits and how rules exist to simplify IPv6 addresses, such as omitting leading zeros, consecutive zero blocks, and zero blocks. ● Provide an example and demonstrate the step-by-step simplification process for an IPv6 address. ● Demonstrate the configuration of IPv6 on a router interface using the ipv6 address command. ● Define unicast communication as representing one-to-one communication, multicast as one-to-many, and anycast allows for the use of the same address on multiple devices to allow packets to be routed to the nearest device using that address. ● Describe global unicast addresses similar to IPv4 public addresses, uniquely routable on the internet; Discuss link-local addresses for communication within the same local link (LAN); Discuss unique-local addresses, similar to IPv4 private addresses, not routable in the global IPv6. ● Explain the role of the prefix in IPv6, representing the network portion of the address. ● Define the concept of dual stack, where devices simultaneously run both IPv4 and IPv6 protocols. ● Explain tunneling as a method to encapsulate IPv6 packets within IPv4 packets for transmission. ● Discuss translation techniques that allow IPv6 and IPv4-enabled devices to communicate. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class to network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** MAC Address	● Define MAC Address as a unique 48-bit hardware identifier embedded in a network card during manufacturing. ● Explain that MAC Addresses are also known as Physical Addresses or Hardware Addresses.

		● Discuss the 12-digit hexadecimal format of MAC Addresses showing the common representation of MAC Addresses using Colon-Hexadecimal notation. ● Explain that the first six digits of a MAC Address identifies the manufacturer through the OUI and how vendors must register with the IEEE Registration Authority ● Emphasize that MAC Addresses are used in LAN environments to identify devices and enable communication between them. ● Highlight that MAC Addresses play a crucial role in local network traffic routing. Emphasize that without MAC addresses, local delivery of data packets would not be possible. ● Explain the use of MAC Addresses in conjunction with ARP to resolve IP addresses to MAC addresses on a LAN. ● Discuss how ARP operates to map IP addresses to MAC addresses for efficient communication. ● Clarify that MAC Addresses are burned into the hardware of a Network Interface Card and cannot be changed but mention that through specific software tools, modification of the MAC address is possible. ● Provide instructions and demonstrate if possible on how to view the MAC Address of a network adapter in popular operating systems like Windows and Linux. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class to network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Pulse Check**	● After the poll is concluded, review the results with the learners. Encourage those in the red zone to attend office hours and/or to reach out to the instructors for assistance.
5 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** Address Resolution Protocol	● Explain that Address Resolution Protocol (ARP) is used to resolve a logical address (IP) to a physical address (MAC) for communication on the same LAN. ● Emphasize the importance of ARP in encapsulating MAC addresses to enable successful communication between devices and that without ARP, local delivery of data packets would not be possible in an IPv4 network. ● Discuss how ARP operates in both Layer 2 (Data Link Layer) and Layer 3 (Network Layer) of the OSI model.

		• Highlight that every Layer 3 device uses ARP to resolve IP addresses to MAC addresses. • Present a scenario where Host A wants to communicate with Host B but does not know Host B's MAC address. Explain that the ARP cache or table is stored in the RAM of a device. • Introduce commands to display and manage the ARP cache, such as "arp -a" (display), "arp -g" (display on some platforms), "show arp" (Cisco devices), "arp -d" (delete entry), and "arp -s" (add static entry). • Explain that hosts generally learn about the MAC addresses of other hosts dynamically using ARP but that static ARP entries can be performed. • Discuss the benefits of static ARP in reducing the risk of ARP spoofing attacks and enhancing network security. • Provide demonstrations and examples of using ARP commands to display, delete, and add entries to the ARP table. • Explain the syntax and parameters of commands like "arp -s" to add static entries, "arp inet_addr" to define an IP address, and "arp eth_addr" to define a MAC address. • Be prepared to discuss the implication of the real world scenario presented at the beginning of class to network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Break**	• Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** Introduction to Wireshark	• Explain that Wireshark is a free application used to capture and view data on a network and that this tool is used by many different roles within the cybersecurity field. • Highlight its ability to read packet contents and apply filters for troubleshooting and software development. • Demonstrate how to start Wireshark and navigate the initial screen with available network interfaces. • Explain the process of selecting an interface to begin capturing network traffic and how all traffic passing through the selected interface will be captured. • Discuss the ability of Wireshark to open traffic captured by other tools, such as TCP dump and that various file formats (.pcap or .pcapng) of captured data can be exported. • Explain how a security professional can use the information found in the Packet List view, Packet Details section, and Bytes section in the analysis of captured data.

		● Explain the use of filters and the use of logical conditions in Wireshark to efficiently view specific packets or protocols of interest. ● Introduce the concept of streams, which are collections of packets from the same conversation and how to perform stream inspection by selecting a packet and using the Follow Stream option. ● Discuss the limitations of Wireshark in analyzing encrypted traffic, which appears as non-meaningful characters. ● Summarize the key points covered in the lesson, emphasizing the usefulness of Wireshark in network analysis. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class to network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
30 min	**Lab:** Analyzing with Wireshark	● This is the first use of Wireshark in the extended program and learners may not be familiar with the use of this tool. Spend a few minutes introducing the tool and various options to filter, view, import and export date. ● Demonstrate the lab with the learners and encourage them to participate in discussion. ● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab in order to properly assess their knowledge and determine where they might need additional assistance.
15 min	**Lesson Closure**	● Spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as the structure of an IP address as well as the MAC address. Ensure learners understand the importance and role of ARP on a network and how without this protocol, delivery of data packets on a local network would not be possible. In addition, stress the importance of becoming more familiar with tools such as Wireshark so that network capture and analysis is possible. ● You will be able to use the data collected in the pulse check to help with the lesson closure. Remind those learners that reported being in the “red zone” to take advantage of office-hours.

		● Recommend that the learners ensure they submit all of the assignments on-time to ensure the appropriate credit is provided to them. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation

Share Your Experience

Cybersecurity is a challenging field and learners need to stay motivated and engaged. To learners, you are not only a subject matter expert but also a role model and an inspiration. Consider sharing your personal experience in these areas:

- Can you recall a specific challenge or problem you encountered while working with network addressing? How did you approach and overcome it? What lessons did you learn from that experience?
- Have you ever been involved in a network addressing project or implementation that required creative problem-solving or out-of-the-box thinking? How did you navigate the complexities and find a solution?
- As a network professional, have you ever faced a situation where a network addressing issue directly impacted the security or performance of a system? How did you address the issue and mitigate any potential risks?