Instructor Guide

Computer Networking Fundamentals

LESSON: Infrastructure Services & Troubleshooting

Before you Begin

Module 11 is the final module in the synchronous portion of this course. The focus of this module is to introduce and discuss common networking services that learners may come across as they continue to explore the fundamentals of any typical network. Topics include protocols and services such as DHCP, NAT, syslog and troubleshooting activities. By the end of this lesson, learners should be able to have a high-level understanding of the importance of these services for a network to function properly. 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 DHCPv6 for IPv6 address assignment and various allocation methods. They will delve into Network Address Translation (NAT) techniques, troubleshooting network connectivity using commands like Traceroute and Extended Ping, and syslog configuration. The lesson also covers NTP and OSI troubleshooting methods. By the end, learners will have a comprehensive understanding of networking concepts and protocols, empowering them to effectively manage and troubleshoot network devices.

Objectives

- Explain the purpose of DHCP.
- Describe the process of DHCP in assigning IP addresses to devices in a network.
- Differentiate between dynamic and static IP address allocation.
- Define NAT.
- Differentiate between the various types of NAT.
- Describe the process of how NAT works.
- Apply the troubleshooting process to diagnose basic network issues.
- Analyze more complex network problems and apply appropriate troubleshooting techniques to resolve them.
- Explain the importance of the Syslog standard in monitoring computer, network, and security systems, and differentiate its use in comparison to other monitoring tools.
- Describe the implementation of the Syslog standard in Cisco IOS, including the configuration of logging and the usage of log messages to identify and troubleshoot network issues.
- Identify the significance of utilizing the Syslog standard in computer network and system monitoring and troubleshooting, and analyze how its use can enhance network performance and security.
- Explain the key features of NTP, including its purpose, the role of time servers, and synchronization processes.
- Describe the importance of time zones and stratum in NTP and explain how they are used in time synchronization across networks.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Lesson Opener:** Infrastructure Services &	● Introduce learners to the importance of understanding Infrastructure Services & Troubleshooting as the basis for computer networking.

	Troubleshooting	
5 min	**Real World Scenario:** Infrastructure Services & Troubleshooting	● 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:** DHCP Overview	● Explain the need for unique IP addresses on a network and the challenges of manual IP address assignment. ● Introduce DHCP as an automated IP address management solution that dynamically allocates addresses to devices on the network. ● Discuss how DHCP also provides additional network information like DNS server addresses and default gateway addresses. ● Present DHCP's location in the OSI and TCP/IP models and its use of UDP ports 67 and 68. ● Mention that DHCP supports both IPv4 (DHCPv4) and IPv6 (DHCPv6). ● Introduce dynamic allocation, automatic allocation, and reservation address methods for IP address management. ● Explain the concepts of leasing IP addresses and how each method differs in lease expiration and address allocation. ● Break down the DHCP process into four steps: Discover, Offer, Request, and Acknowledgment (DORA). ● Detail the role of the client and the DHCP server in each step and explain how DHCP packets encapsulate information. ● Describe Stateless Address Autoconfiguration (SLAAC), Stateless DHCPv6, and Stateful DHCPv6. ● 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.
30 min	**Cyber Uncovered:** NAT Overview	● Explain the significance of NAT as a protocol that converts private addresses to public addresses and enables internet access for local networks. ● Mention that NAT is commonly enabled on firewall or router devices at the edge of the network.

		● Discuss the need for private and public addresses due to the depletion of available IPv4 addresses. ● Explain that private addresses identify devices within a network, while public addresses identify devices outside the network. ● Introduce the transparent operation of NAT and its function to hide the internal network from the internet, adding a layer of security. ● Describe the three NAT methods: Static, Dynamic, and Port Address Translation (PAT). ● Present the special table in NAT-enabled devices that store evidence of its operation. ● Outline the benefits of NAT, such as preventing IPv4 address depletion, providing flexibility in network design, and adding an extra security layer. ● Mention the disadvantages, including potential difficulties in accessing internal resources and network performance reduction. ● Define and explain the Inside Local, Outside Local, Inside Global, and Outside Global addresses used in NAT. ● Describe One-to-One NAT as a permanent mapping of private to public addresses, not meant for address conservation but for access to internal resources. ● Explain Many-to-Many NAT, a dynamic mapping of multiple private addresses to a pool of public addresses. ● Detail Many-to-One NAT (PAT), the most common method used for address conservation by converting multiple private addresses to a single public address with the use of source port numbers. ● Introduce NAT64 as a technology facilitating communication between IPv6-only and IPv4-only hosts and networks. ● Explain how NAT64 helps accelerate IPv6 adoption while handling IPv4 address depletion for enterprises and ISPs. ● 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.
15 min	**Lab:** Nat Configuration	● 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.

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:** Troubleshooting Methods	● Emphasize that even advanced networks can experience issues and that troubleshooting is an essential skill for network administrators. ● Explain that this lesson covers effective ways to resolve network issues using efficient troubleshooting techniques and tools. ● Introduce the significance of discovery protocols in network troubleshooting and how they aid in identifying network devices and configurations. ● Stress the importance of continuous and detailed network documentation for quick and efficient troubleshooting to include physical and logical diagrams, configuration files, and addressing schemes. ● Present three troubleshooting methods: Bottom-Up, Top-Down, and Divide and Conquer. ● Explain how each approach targets different layers of the OSI model to diagnose and isolate network issues. ● Introduce Network Management Software (NMS) as an excellent tool for monitoring network activity and establishing baselines for reference. ● Present a list of essential command-line tools for network troubleshooting, such as show interfaces, show ip route, show ip interface brief, show running-config, and show startup-config. ● Describe the extended ping command, which performs advanced network connectivity checks and allows for source IP changes. ● Explain the purpose of the traceroute command in discovering the path of packets to a remote destination and identifying routing failures. ● 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.

25 min	**Cyber Uncovered:** Log Events & Syslog Server	● Explain that Syslog is a standard for logging messages, similar to keeping a diary of actions and events on network devices. ● Emphasize the importance of monitoring the network to ensure smooth functionality and efficient troubleshooting. ● Discuss the significance of system notification logging in increasing awareness of hardware or software malfunctions, service status, and security accountability. ● Highlight how log analysis can help troubleshoot the system and aid information security experts in investigating security breaches. ● Describe the various log storage methods, including logging buffer, console line, terminal line, and Syslog server. ● Explain the limitations of log storage due to buffer size and the importance of considering RAM erasure upon device power off. ● Define a Syslog server as a computer running Syslog software that centralizes logs from all network devices into one location. ● Discuss the benefits of using a Syslog server, such as easier log management, backup, and a user-friendly interface. ● Introduce the concept of severity levels in Syslog messages, ranging from 0 (emergencies) to 7 (system debugging). ● Explain how the severity levels represent critical malfunctions, system warnings, and various log message types. ● Describe the facility parameter, indicating the source that generated the log message, which can be a hardware component, protocol, or system service. ● Discuss the components of a Syslog message, including timestamp, facility, severity, mnemonic, and text description. ● Explain the significance of enabling the time information to ensure accurate log timestamps. ● Present the essential Syslog configuration commands, such as logging host, logging trap, service timestamps log datetime msec, logging console, terminal monitor, and login buffered. ● 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.
25 min	**Cyber Uncovered:** Network Time Protocol (NTP)	● Explain the purpose of Network Time Protocol (NTP) as the protocol responsible for synchronizing time and date across network devices. ● Highlight its widespread implementation as a simple client-server protocol for time synchronization. ● Compare the manual configuration method, where users set the time and date on each device, with the automatic configuration method using an NTP server. ● Emphasize the scalability benefits of automatic configuration and the time-saving advantages for large networks. ● Describe how Cisco routers and switches, along with various devices worldwide, use NTP to determine accurate time and date. ● Introduce the concept of Cisco devices acting as NTP servers. ● Explain the stratum levels, representing the hierarchy of devices connected to high-precision reference clocks. ● Define stratum 0 as the reference clock and how the hierarchy progresses with stratum 1, stratum 2, and so on. ● Discuss the critical role of accurate time settings for time-sensitive services and event logging. ● Emphasize the significance of timestamps in troubleshooting, network management, and network security. ● Address the drawbacks of manual clock setting, including devices becoming out of sync during shutdowns and the time-consuming process for large networks. ● Demonstrate how to make a Cisco device, like a router, set its clock with an external NTP server using the ntp server command and the server's IP 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.
35 min	**Lesson and Course Closure**	● For this lesson, spend a few minutes reminding the learners what the key ”take-aways'' were from the lesson. Important concepts to focus on are DHCP and the DORA process. Emphasize the importance of understanding the process a client goes through for obtaining an IP configuration through a DHCP lease. Review the most commonly used tools used when troubleshooting network issues. Finally, emphasize the

		importance of having synchronized time throughout the network devices. ● Since this is the last synchronous module in the course, spend a few minutes reviewing key concepts including how frames move between interfaces at layer 2 and how IP packets move across routers at layer 3. Emphasize to the learners that these concepts are critical for establishing a strong foundation in the field of cybersecurity. ● 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. ● Q&A
5 min	**End-of-Course Survey**	● Allocate 5 minutes to facilitate the completion of the End-of-Course Survey. ● Encourage learners to provide honest and constructive feedback about their learning experience.
	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 share an experience where the implementation of infrastructure services, such as firewalls or intrusion detection systems, played a crucial role in defending against a cyber attack or mitigating a security incident? How did these services contribute to the overall security of the network?
- Have you ever faced challenges in integrating infrastructure services, such as VPN or secure DNS, into a network environment? How did you overcome those challenges, and what impact did these services have on strengthening the network's security?
- Share an example where the use of infrastructure services, such as network monitoring and logging tools, helped in detecting and responding to a security incident. How did these services aid in incident investigation, threat analysis, and timely response?
- Can you recall a time when you encountered a complex network issue that required extensive troubleshooting? What steps did you take to identify the root cause of the

problem, and how did you ultimately resolve it? How did this experience enhance your troubleshooting skills and problem-solving abilities?

- Share an example of a network outage or disruption that you faced in your career. How did you approach the situation, and what troubleshooting techniques or methodologies did you employ to restore network connectivity and functionality? What lessons did you learn from this experience about the importance of thorough network documentation and preparation for handling unforeseen issues?