Instructor Guide

Computer Networking Fundamentals

LESSON: VLANs and ACLs

Before you Begin

Module 10 brings together concepts from module 7 (switching) and module 8 (routing). You may find that reviewing OSI layers 2 and 3 may be helpful. In this module, consider focusing on how VLANs create logical boundaries within the physical switch and how inter-VLAN routing is needed when these data packets target a remote network. It is a great opportunity to also re-introduce the ARP protocol in your discussion to build on the concepts previously covered. By the end of this lesson, learners should be able to have a high-level fundamental understanding on how data packets move through a network. 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 Virtual Local Area Networks (VLANs) and how they enhance network performance, security, and organization. They will discover the two operational modes of switch ports, Access and Trunk, and their roles in facilitating communication within and between VLANs. The lesson covers trunking protocols like IEEE 802.1Q and DTP, as well as the router-on-a-stick technique for inter-VLAN communication. Learners will study Access Control Lists (ACLs) and their types, including stateless and stateful ACLs, to secure and control network traffic. The concept of wildcard masks, named and numbered ACLs, and extended ACLs will be explained. By the end of the lesson, learners will have a solid understanding of VLANs, trunking protocols, inter-VLAN communication, and ACLs, empowering them to optimize network performance and security.

Objectives

- Describe VLANs.
- Explain the benefits of VLANs.
- Differentiate between Access and Trunk switch interface modes.
- Describe the purpose of the Trunk mode.
- Identify the different trunking protocols used in computer networking.
- Explain the concept of inter-VLAN routing.
- Describe the router-on-a-stick method.
- Compare and contrast the router-on-a-stick method with other methods of inter-VLAN routing.
- Explain the principles of Access Control List (ACL) and how it can be used to improve network security and resource management.
- Differentiate between the various applications of ACLs and identify scenarios in which each type of ACL may be appropriate.
- Evaluate the benefits and limitations of using ACLs as a tool for network compartmentalization and access control.
- Differentiate between standard and extended ACLs and identify when to use each type in the configuration process.
- Describe the purpose of standard ACL and its limitations.
- Explain the process of configuring and verifying standard ACL on a router.
- Describe the process of configuring extended ACLs, including specifying the source and destination addresses, protocols, and port numbers.
- Explain the importance of testing and verifying extended ACL configurations to ensure proper functioning and troubleshoot any issues that arise.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Lesson Opener:** VLANS and ACLs	● Introduce learners to the importance of understanding VLANs and ACLs as the basis for computer networking.
5 min	**Real World Scenario:** VLANS and ACLs	● 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:** VLANs Overview	● Define VLAN as a Layer 2 feature that allows virtual network segmentation. ● Explain how VLANs divide a physical network into separate logical networks where each network operates as a separate broadcast domain. ● Discuss the advantages of VLANS: improved security by controlling traffic, enhanced performance by reducing the scope of the broadcast domain, and simplified management by better organizing users. ● Explain the need for unique VLAN IDs to identify and separate traffic in different VLANs. ● Review the valid range for VLAN IDs for Cisco devices (1 to 1005) and the extended range (1006 to 4094). ● Discuss VLANs 1 and 1002-1005 as reserved and automatically added during device installation and also describe VLANs 2-1001 commonly used for data exchanges and data traffic tagging. ● Highlight Interface VLAN 1 as the management VLAN used for SVI and basic network functions. ● Native VLAN: Describe VLAN 1 as the default native VLAN for forwarding untagged traffic among switches. ● Clarify that access ports carry traffic for a specific VLAN and are assigned to end devices like PCs. ● Discuss and demonstrate some of the common IOS commands related to VLANS: show vlan brief, vlan <id>, name <word>, switchport mode access, switchport access vlan <id>, switchport voice vlan <id>. ● Explain how trunk ports carry traffic for multiple VLANs using identifier tags (802.1Q or ISL). ● Provide instructions for setting up Voice VLANs to manage VoIP traffic efficiently. ● 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:** Trunk Protocols	● Define trunk mode as a method to transmit multiple VLAN traffic sessions over the same physical connection to a remote device (switch or router). ● Explain how frames are tagged with the source VLAN to maintain VLAN isolation when forwarding frames to another switch. ● Describe ISL as a proprietary protocol developed by Cisco for VLAN information encapsulation in Ethernet frames. ● Introduce IEEE 802.1Q as an industry-standard trunk protocol allowing trunk link creation between switches of various vendors and how 802.1Q encapsulates VLAN information within the frame. ● Discuss the “switchport mode trunk” command and “show interfaces trunk” command. ● Explain DTP as a Cisco protocol automating trunk link creation and selecting the trunk protocol on both sides. ● Describe the dynamic auto mode, which passively waits for requests, and dynamic desirable mode, which actively attempts to establish a trunk link. ● Demonstrate examples of using the following commands: switchport mode dynamic <mode> and switchport nonegotiate. Explain how to display the interface mode for each. ● Explain port configuration options by discussing the results of each mode combination. ● Define native VLAN as the VLAN processing untagged frames on trunk ports and that VLAN 1 is the default native VLAN. ● Explain that native VLANs are essential for protocol updates among interconnected switches (CDP, VTP, DTP, STP) since trunk ports drop untagged frames. ● Recommend best practices, such as reassigning native VLANs to non-default VLANs (e.g., VLAN 200) for security purposes. ● Emphasize the need for the same native VLAN on both ends of the trunk link to ensure correct delivery of untagged frames and avoid warning messages. ● Provide an example of changing the default native VLAN on interconnected switches. ● Show how to display the Native VLAN settings using the “show interfaces trunk” command.

		● 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.
20 min	**Lab:** Configuring VLANs and Trunks	● 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:** Inter-VLAN Routing	● Explain that although VLANs are logical segments, they still operate within the framework of a network and are broadcast domains. ● Emphasize that switches at Layer 2 cannot move traffic across different VLANs and that a Layer 3 device is needed for routing data between VLANs. ● Explain how the router uses the process of encapsulation and decapsulation of data packets to enable data transfer between VLANs. ● Introduce Router-on-a-Stick as the most common technique for Inter-VLAN Routing. ● Highlight its effectiveness in using a single physical connection between the switch and router, minimizing costs. ● Explain that a router's single physical interface is segmented into multiple logical subinterfaces to accommodate multiple IP addresses and that each sub-interface represents a default gateway for a specific VLAN. ● Instruct how to set the local interface connected to the router to trunk mode for VLAN tagging. ● Explain how to use the show ip interface brief command to display interface settings and mode on the router. ● Mention that additional details, such as the interface and its VLAN ID, can be viewed using the show running-config command. ● Provide a practical example of configuring Router-on-a-Stick for two interconnected VLANs on a switch and router. ● Walk through the configuration process step-by-step, demonstrating the commands and their impact on the network. ● 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.
20 min	**Lab:** Initialize Router on a Stick	● 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:** ACLs Overview	● Define ACL as a rule-based feature that enables network administrators to configure basic traffic filtering. ● Explain that ACLs use packet header information to determine whether to drop or forward a packet. ● Describe the various areas where ACLs are commonly used, including computer networks (firewalls, switches, and routers), computer file systems, web portals, and cloud configurations. ● Explain the role of ACLs in firewalls, where stateless and stateful firewalls apply different filtering techniques based on source, destination, and connection details. ● Discuss how ACLs can improve network performance by allowing only relevant services to communicate, reducing unnecessary traffic. ● Emphasize the role of ACLs in restricting user access to sensitive services, enhancing network security. ● Highlight the ability of ACLs to restrict specific protocol types and packets, such as routing protocol advertisements and ICMP traffic. ● Describe how standard ACLs examine only the source IP address when implementing restrictions, with Cisco recommending placement close to the destination device. ● Explain how extended ACLs filter packets based on various parameters like protocol type, source/destination IP addresses, and source/destination port numbers, with Cisco recommending placement close to the source. ● Explain that when configuring ACLs on an interface, the traffic direction (inbound or outbound) must be specified for the router to implement proper restrictions. ● Describe how inbound ACLs examine incoming traffic to the interface. ● Explain how outbound ACLs examine outgoing traffic from the interface.

		● Explain why the order of statements in ACL is crucial. ● 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.
15 min	**Cyber Uncovered:** Standard ACL	● Define Standard ACLs as access control lists used for basic traffic filtering based on source IP addresses. ● Explain that the placement of Standard ACLs is crucial to avoid unintended restrictions on communication. ● Emphasize that Standard ACLs are placed as close to the destination as possible to avoid blocking communication with source networks. ● Introduce Standard Named ACLs, which allow unique names to be assigned to ACLs for easier identification and management. ● Describe Standard Numbered ACLs, which allow unique numeric values to be assigned to ACLs. ● Mention that the range for Standard Numbered ACLs includes 1-99 and 1300-1999. ● Explain the basic syntax for configuring a numbered ACL. ● Provide step-by-step instructions for creating a numbered ACL using the access-list command. ● Guide learners to choose the interface for ACL application using the interface command. ● Instruct learners to link the ACL to the appropriate interface in the outbound direction using the ip access-group command. ● Explain how to create a named ACL using the ip access-list standard command. ● Guide learners to create Deny and Permit ACE statements in ACL configuration mode. ● Instruct learners to apply the ACL on an interface using the ip access-group command, specifying the traffic direction (in or out). ● Instruct learners on how to use the show running-config and show access-list commands for ACL verification. ● 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.
15 min	**Cyber Uncovered:** Extended ACL	● Define Extended ACLs as access control lists used for filtering based on source/destination IP addresses, Layer 4 protocols (TCP and UDP), and protocol types. ● Explain the range of numbers used for Extended ACLs (100-199 and 2000-2699). ● Emphasize the importance of placing Extended ACLs as close to the source of the traffic being filtered to prevent unwanted traffic from traversing the network infrastructure. ● Explain the syntax for configuring numbered Extended ACLs ● Provide step-by-step instructions for creating a numbered ACL using the access-list command. ● Guide learners to choose the interface for ACL application using the interface command. ● Instruct learners to link the ACL to the appropriate interface in the inbound direction using the ip access-group command. ● Explain how to create a named ACL using the ip access-list standard command. ● Guide learners to create Deny and Permit ACE statements in ACL configuration mode. ● Instruct learners to apply the ACL on an interface using the ip access-group command, specifying the traffic direction (in or out). ● Instruct learners on how to use the show running-config and show access-list commands for ACL verification. ● 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.
20 min	**Lab:** Implementing Access Control Lists	● 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	**Lesson Closure**	● For this lesson, 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. Topics to focus on should include how VLANs can be used to improve and secure network communication, how routers

		are required to connect VLANs together, and how ACLs can be used to filter unwanted traffic on the network. ● 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:

- Have you encountered any real-world scenarios where VLAN implementation significantly improved network performance or enhanced security? How did VLANs play a role in addressing the challenges and achieving the desired outcomes?
- Can you recall a situation where Access Control Lists (ACLs) were instrumental in preventing a security breach or mitigating a network-related issue? How did the effective use of ACLs impact the overall network architecture and data protection?
- Share a memorable experience when troubleshooting VLAN or ACL configurations. What were the key lessons learned from that experience, and how did it shape your approach to managing and configuring VLANs and ACLs in subsequent projects?
- As a seasoned professional in the field of computer networking, how do you stay updated with the latest developments and best practices related to VLANs and ACLs? Are there any resources, certifications, or communities you find valuable for continuous learning and growth in these areas?