VLAN, STP, AND Packet Filtering Firewall

Yogaraj Govindarajalu Prabagaran

# Table of Contents

[Table of Contents 2](#_Toc152286731)

[Lab 5 – VLAN and STP 3](#_Toc152286732)

[Parts 3](#_Toc152286733)

[Description 3](#_Toc152286734)

[Observations 3](#_Toc152286735)

[Preparation 4](#_Toc152286736)

[Screenshots 4](#_Toc152286737)

[Reflection 15](#_Toc152286738)

[Lab 6 – Packet Filtering Firewall 16](#_Toc152286739)

[Parts 16](#_Toc152286740)

[Description 16](#_Toc152286741)

[Preparation 16](#_Toc152286742)

[Observations 16](#_Toc152286743)

[Screenshots 17](#_Toc152286744)

[Reflection 49](#_Toc152286745)

[References 50](#_Toc152286746)

# Lab 5 – VLAN and STP

# Parts

## Description

In Lab 5, I am tasked with practically implementing Virtual Local Area Networks (VLANs), InterVLAN Routing (IVR), and Spanning Tree Protocol (STP) in a network topology featuring a headquarters site and a branch office site. I aim to enhance my skills in configuring VLANs, IVR, STP, and EIGRP using Variable Length Subnet Masks (VLSM). I must build and configure the topology, conduct initial tests, and thoroughly document my progress. The lab is divided into two parts: the first involves setting up the initial topology with EIGRP, and the second focuses on configuring and testing VLANs, IVR, and STP. I will provide screenshots, running-configs, and packet tracer files to prove my completion. Additionally, I am required to reflect on the advantages and scenarios for implementing VLANs, IVR, and STP.

## Observations

Throughout the execution of Lab 5, several observations were made regarding the configuration and testing processes. Initial configurations were conducted smoothly, including the setup of VLANs, inter-VLAN routing, and Spanning Tree Protocol (STP). Notably, establishing EIGRP routing demonstrated successful communication between routers and the accurate advertisement of network addresses.

During the testing phase, it was observed that workstations could efficiently ping all interfaces on their respective routers, ensuring robust intra-LAN connectivity. Additionally, successful pinging between workstations and their associated switches reflected the effectiveness of the VLAN and trunking configurations. SSH connectivity to switches and routers was also validated, indicating secure remote access.

In the VLAN, InterVLAN Routing, and STP configuration stage, the implementation of PVST on switches SW1, SW2, and SW3 proceeded without significant issues. The assignment of root bridges for specific VLANs was accomplished, contributing to optimized network performance. Observations during testing included the verification of VLAN and STP configurations using relevant commands, ensuring the network's stability.

Despite the generally smooth execution, a notable observation was the importance of meticulous configuration verification. When ping tests or SSH connectivity did not align with expectations, careful examination and rectification of configurations proved essential. These observations underscore the significance of thorough testing and verification in achieving a robust and reliable network configuration.

## Preparation

To adequately prepare for Lab 5, I ensured I had the essential equipment ready for seamless execution. This included 5 Cisco 2960 Switches for VLAN management, 2 Cisco 2811 Routers for inter-VLAN communication and EIGRP routing, 8 PC PT Objects representing workstations, 1 PC Server Object simulating a server, and 1 PT Laptop for additional networking scenarios. I set a uniform password; in this case, all devices were configured with "Secret55" for consistent access. Moreover, I assigned IP addresses based on the networks specified in the Portfolio 3 subnets file to maintain coherence across devices. These configurations laid the groundwork for the lab exercises, ensuring a standardized environment, and it was imperative to verify these settings to prevent complications during the lab session.

## Screenshots

A diagram of a computer network

Description automatically generated

Figure 1: Initial Configuration

This screenshot showcases the initial configuration of the network topology as per the lab schematic. All devices, including routers, switches, and workstations, are appropriately connected, and IP addressing is visible on the routers and switches. The use of classless VLSM for WAN and LAN interfaces is evident in the IP configurations.

A screenshot of a computer

Description automatically generated

Figure 2: VLAN Configuration on Switches

This screenshot provides a detailed view of the VLAN configuration on switch SW1.

A screenshot of a computer

Description automatically generated

Figure 2.1: VLAN Configuration on Switches

This screenshot provides a detailed view of the VLAN configuration on switch SW2.

A screenshot of a computer

Description automatically generated

Figure 2.2: VLAN Configuration on Switches

This screenshot provides a detailed view of the VLAN configuration on switch SW3.

A screenshot of a computer

Description automatically generated

Figure 3: Spanning tree on Switch 1

This screenshot provides a detailed view of the Spanning tree on Switch 1 and displays VLAN 5 as the root bridge.

A screenshot of a computer

Description automatically generated

Figure 3.1: Spanning tree on Switch 1

This screenshot provides a detailed view of the Spanning tree on Switch 1 and displays VLAN 5 as the root bridge.

A screenshot of a computer

Description automatically generated

Figure 3.2: Spanning tree on Switch 2

This screenshot provides a detailed view of the Spanning tree on Switch 2 and displays VLAN 10 as the root bridge.

A screenshot of a computer

Description automatically generated

Figure 3.2: Spanning tree on Switch 2

This screenshot provides a detailed view of the Spanning tree on Switch 2 and displays VLAN 10 as the root bridge.

A screenshot of a computer

Description automatically generated

Figure 3.3: Spanning tree on Switch 3

This screenshot provides a detailed view of the Spanning tree on Switch 3 and displays VLAN 15 as the root bridge.

A screenshot of a computer

Description automatically generated

Figure 3.3: Spanning tree on Switch 3

This screenshot provides a detailed view of the Spanning tree on Switch 3 and displays VLAN 15 as the root bridge.

A screenshot of a computer program

Description automatically generated

Figure 4: Pings from the Office PC.

This screenshot shows the Office 1 PC successfully pinging other PCs on the other two VLANs.

## Reflection

In deploying VLANs, I appreciate their role in enhancing network security and performance through segmentation, isolating broadcast domains, and simplifying management. The ability to logically group devices based on function streamlines administration, while broadcast control and improved security add further value. Inter-VLAN Routing (IVR) proves indispensable for enabling communication between VLANs, optimizing resource utilization, and ensuring scalability. As for Spanning Tree Protocol (STP) 's contribution lies in loop prevention, guaranteeing network stability by blocking redundant paths and facilitating automatic path selection for high availability. These technologies offer a comprehensive solution for building efficient, secure, resilient networks, particularly in large and dynamic environments.

In retrospect, Lab 5 provided valuable insights into the practical implementation of VLANs, InterVLAN Routing (IVR), and Spanning Tree Protocol (STP). Configuring these network features deepened my understanding of their functionalities and highlighted their significance in optimizing network performance and scalability.

The deployment of EIGRP for dynamic routing demonstrated its effectiveness in automatically adapting to changes in the network topology, facilitating efficient communication between routers. This experience emphasized the importance of dynamic routing protocols in real-world networking scenarios.

Introducing VLANs and InterVLAN Routing added a layer of flexibility to network design. Segregating broadcast domains enhanced network security and allowed for efficient resource utilization. Configuring STP, especially in the context of PVST, showcased the importance of redundancy elimination and loop prevention in a network, contributing to stability and reliability.

One notable aspect was the assignment of root bridges for specific VLANs, a crucial element in STP configuration. This exercise emphasized the strategic placement of root bridges to optimize traffic paths, minimizing the risk of network disruptions.

Reflecting on the challenges encountered, meticulous verification of configurations emerged as a key takeaway. Careful examination and troubleshooting were essential for resolving discrepancies when connectivity issues arose. This underscores the critical role of troubleshooting skills in maintaining a robust, error-free network infrastructure.

In practical terms, implementing VLANs, IVR, and STP showcased their relevance in designing scalable and resilient networks. The ability to navigate through potential challenges and configure a network that meets specific requirements is a valuable skill set that this lab has contributed to developing.

# Lab 6 – Packet Filtering Firewall

# Parts

## Description

Lab 6 focuses on hands-on experience with stateless packet filtering firewalls, building on concepts from previous labs. Divided into three parts, the initial configuration involves securing the network devices, followed by configuring standard access lists to control communication between spoke networks. The final part extends the complexity by implementing extended access control lists for precise traffic control between LANs and specific ports on HUBs. The lab emphasizes individual effort and thorough documentation, including screenshots, observations, and reflections on each configuration step. Practical tests are conducted to ensure the effectiveness of access control rules, providing a comprehensive understanding of network security principles and reinforcing skills in ACL configuration using Packet Tracer.

## Preparation

In preparation for Lab 6 on stateless packet filtering firewalls, I ensured I had the required tools and software. I confirmed that I had the latest version of Packet Tracer installed on my system to align with lab requirements and access the latest features. I retrieved the Packet Tracer file from Lab 4 and set up my working environment based on previous network configurations. The devices included six 2960 Switches, four 2811 Spoke, two hubs, and six PCs. I used the IP addresses assigned in the Subnet file from the assessment portal. All network devices were configured with the password "Secret55" to ensure security and consistency. Adhering to the lab's password guidelines, I standardized all passwords, particularly the privileged mode password, to "Secret55. This comprehensive preparation ensured a smooth and focused execution of the lab tasks, minimizing potential issues during the configuration process.

## Observations

Throughout Lab 6, a series of observations unfolded, revealing valuable insights into the intricacies of network configurations. In the initial topology configuration, while tasks like setting up the privileged mode password and enforcing login proceeded smoothly, a misconfiguration in routing became apparent during testing, highlighting the necessity for meticulous checks before advancing. Moving on to standard access list configuration, the straightforward creation and application of access lists on Spoke-1 and Spoke-2 contrasted with the challenges uncovered during testing. An oversight in the ACE sequence initially led to unintended communication between spokes, emphasizing the pivotal role of the ACE order. As the lab progressed to extended access control lists, careful rule definition for EIGRP, ping, telnet, and SSH traffic was crucial. Testing revealed connectivity issues, emphasizing the iterative nature of refining configurations for complex scenarios. These observations collectively underscored the iterative and interconnected nature of network configurations, emphasizing the importance of systematic testing and troubleshooting for each step in the process.

## Screenshots

A diagram of a network

Description automatically generated

Figure 1: Initial Configuration Screenshots

This figure encompasses screenshots capturing the initial configuration of the lab topology.

Part 2:

Lab Description:

This lab aims to implement standard access lists for packet filtering in a network topology with multiple spokes. The specific objective is to allow communication between hosts on spoke one and spoke 2 and hosts on other spokes while preventing communication between spoke 1 and 2. The process involves creating standard access lists on Spoke-1 and Spoke-2, denying traffic from specific LAN networks, and allowing traffic from any other network. These access lists are then applied inbound on the external interfaces of the respective spokes. Testing ensures communication between other PCs on different spokes while restricting communication between Spoke-1, Spoke-2, and Spoke-4.

Observations:

Screenshots are taken to document the ACL configuration on each spoke, including ACL names, ACEs, and any filtering effects. Additionally, interface assignments for the access lists are captured. Testing involves confirming communication between specific PCs and observing the expected restrictions between Spoke-1, Spoke-2, and Spoke-4.

Screenshots:

A screenshot of a computer program

Description automatically generated

Figure 2: PC1 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4.

This figure encompasses screenshots capturing the PC's ability to communicate with all others demonstrated, showcasing the successful implementation of the initial setup.

A screenshot of a computer program

Description automatically generated

Figure 2.1: PC2 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4.

This figure encompasses screenshots capturing the PC's ability to communicate with all others demonstrated, showcasing the successful implementation of the initial setup.

A computer screen shot of a computer program

Description automatically generated

Figure 2.2: PC4 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4.

This figure encompasses screenshots capturing the PC's ability to communicate with all others demonstrated, showcasing the successful implementation of the initial setup.

A computer screen shot of a black and white screen

Description automatically generated

Figure 3: PC1 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4 after the “no permit any” command.

This figure encompasses screenshots capturing the PC's disability to communicate with all others demonstrated.

A computer screen shot of a program

Description automatically generated

Figure 3.1: PC2 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4 after the “no permit any” command.

This figure encompasses screenshots capturing the PC's disability to communicate with all others demonstrated.

A computer screen shot of a black screen

Description automatically generated

Figure 3.2: PC4 pinging the PCs on Spoke-1, Spoke-2, and Spoke-4 after the “no permit any” command.

This figure encompasses screenshots capturing the PC's disability to communicate with all others demonstrated.

A screenshot of a computer

Description automatically generated

Figure 4: Access Lists Configuration

This figure includes screenshots depicting the access lists on Spoke-1.

A screenshot of a computer

Description automatically generated

Figure 5: Access Lists Configuration

This figure includes screenshots depicting the access lists on Spoke-1.

A screenshot of a computer

Description automatically generated

Figure 6: Spoke1’s fE 0/0

I spoke 1 using the command “show IP interface” to show the ACL name.

A screenshot of a computer

Description automatically generated

Figure 6.1: Spoke 1’s fE 0/1

I spoke 1 using the command “show IP interface” to show the ACL name.

A screenshot of a computer

Description automatically generated

Figure 6.2: Spoke2’s fE 0/0

Spoke 2 using the command- “show IP interface” to show the ACL name.

A screenshot of a computer

Description automatically generated

Figure 6.3: Spoke2’s fE 0/1

Spoke 2 using the command- “show IP interface” to show the ACL name.

Reflection:

This lab offered valuable insights into the intricacies of packet filtering and access control list (ACL) configuration. The path of ping traffic between spokes was meticulously controlled through the implemented ACLs. When testing communication between spokes, it was observed that the traffic paths adhered to the defined rules. Specifically, communication between PCs on different spokes was successful, while attempts between Spoke-1 and Spoke-2 were appropriately restricted, as intended by the ACL rules denying such traffic.

Removing the Access Control Entry (ACE), allowing traffic from any source, resulted in expected restrictions. The ACE was initially configured to permit communication from any network, and its removal consequently blocked traffic from all sources not explicitly allowed by the ACL rules. This underscores ACLs' critical role in dictating network traffic flow and enforcing security policies.

Considering the modification of packet filtering configuration to achieve the same effect on Spoke-4 as on Spoke-1 and Spoke-2, careful adaptation of ACL rules is necessary. The configuration should be tailored to Spoke-4's specific role and communication requirements. By mirroring the rules applied to Spoke-1 and Spoke-2 but adjusting them for Spoke-4's unique network relationships, it is possible to create a similar restrictive environment. This process involves identifying the relevant LAN networks to deny and allowing communication to other networks.

In summary, this lab provided hands-on experience with ACL configuration and packet filtering, emphasizing the significance of thoughtful design and precise rule implementation. Understanding the traffic paths, knowing where communication stops, and discerning the implications of ACE modifications contribute to a comprehensive grasp of network security concepts and practical troubleshooting skills in real-world scenarios.

Part-3:

Lab Description:

In Part 3 of the lab, more advanced packet filtering is introduced by configuring Extended Access Control Lists (ACLs). The goal is to enable specific communication patterns within the network topology. Users on LANs connected to HUB A and HUB B are expected to access hosts in all other LANs with restricted access based on defined protocols. Telnet traffic is allowed only from PCs on Spokes 1-3 to the LAN interface on HUB A, while SSH traffic is permitted from PCs on Spokes 4-6 to the LAN interface on HUB B. EIGRP and Ping traffic is allowed from specified sources, and all other traffic is denied.

Observations:

Screenshots are taken to document the ACL configuration on each HUB, including ACL names, ACEs, and any filtering effects. Interface assignments for the access lists are also captured. Testing involves confirming that only PCs on the defined LANs can initiate specific communication with the PCs on HUB A and HUB B.

Screenshots:

A screenshot of a computer

Description automatically generated

Figure 7: The above Screenshot displays the access list for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 7.1: The above Screenshot displays the access list for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 8: The above Screenshot displays the ACL name for each interface for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 8.1: The above screenshot displays the ACL name for each HUB-A interface.

A screenshot of a computer

Description automatically generated

Figure 8.2: The above Screenshot displays the ACL name for each interface for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 8.3: The above Screenshot displays the ACL name for each interface for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 8.4: The above Screenshot displays the ACL name for each interface for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 9: The above Screenshot displays the ACL name for each interface for HUB-B.

A screenshot of a computer

Description automatically generated

Figure 9.1: The above Screenshot displays the ACL name for each interface for HUB-B.

A screenshot of a computer

Description automatically generated

Figure 9.2: The above Screenshot displays the ACL name for each interface for HUB-B.

A screenshot of a computer

Description automatically generated

Figure 9.3: The above Screenshot displays the ACL name for each interface for HUB-B.

A screenshot of a computer

Description automatically generated

Figure 9.4: The above Screenshot displays the ACL name for each interface for HUB-B.

A computer screen shot of a program

Description automatically generated

Figure 10: The above Screenshot ensures that the PC1 on the LAN defined in the access lists can ping the PC on the HUB B LAN.

A computer screen with white text and black background

Description automatically generated

Figure 10.1: The above Screenshot ensures that the PC4 on the LAN defined in the access lists can ping the PC on the HUB B LAN.

A computer screen shot of a black screen

Description automatically generated

Figure 10.2: The above Screenshot ensures that the PC3 on the LAN defined in the access lists can ping the PC on the HUB B LAN.

A computer screen with white text

Description automatically generated

Figure 11: The above Screenshot ensures that the PC2 on the LAN defined in the access lists can ping the PC on HUB A LAN.

A screenshot of a computer program

Description automatically generated

Figure 11.1: The above Screenshot ensures that the PC6 on the LAN defined in the access lists can ping the PC on HUB A LAN.

A screenshot of a computer

Description automatically generated

Figure 11.2: The above Screenshot ensures that the PC5 on the LAN defined in the access lists can ping the PC on HUB A LAN.

A screenshot of a computer

Description automatically generated

Figure 12: The above Screenshot ensures that only the PCs on Spokes 1 and 2 can telnet into the HUB A LAN interface.

A screenshot of a computer

Description automatically generated

Figure 12.1: The above Screenshot ensures that only the PCs on Spokes 1 and 2 can telnet into the HUB A LAN interface.

A computer screen shot of a black screen

Description automatically generated

Figure 13: The above Screenshot ensures that only the PCs on Spokes 3 and 4 can SSH into the HUB B LAN interface.

A computer screen shot of a black screen

Description automatically generated

Figure 13.1: The above Screenshot ensures that only the PCs on Spokes 3 and 4 can SSH into the HUB B LAN interface.

Lab 6 Part 3 Reflection:  
In configuring Extended Access Control Lists (ACLs) on HUB A and HUB B in this lab, each Access Control Entry (ACE) was meticulously crafted to regulate network traffic. EIGRP traffic was allowed from any network, ping traffic was controlled from specific sources, and telnet/SSH access was restricted to designated PCs and LAN interfaces. Attempting telnet from PC4 to HUB B or SSH from PC6 to HUB A would be denied, as the ACLs specified precise conditions for such access. The benefits of Extended ACLs over Standard ACLs were evident, offering granularity, protocol/port specification, specificity, and improved security policies. These ACLs exemplified the balance between facilitating necessary communication and enforcing stringent security, showcasing the robust capabilities of Extended ACLs in network security configurations.

## Reflection

Reflecting on Lab 6, the initial configuration phase highlighted the necessity of a thorough plan, preventing potential issues and emphasizing the intricate interconnectedness of network components. The routing configuration phase underscored the importance of meticulous attention to detail, as troubleshooting revealed the impact of even subtle misconfigurations. Moving to standard access list configuration, the significance of the access control entry (ACE) sequence became apparent during testing, reinforcing the need for a systematic approach to access list configurations. The iterative nature of testing and refining configurations emphasized the value of learning from mistakes to enhance overall proficiency in access control. Defining precise rules for specific traffic types proved complex when transitioning to extended access control lists. Connectivity issues during testing underscored the necessity of a deep understanding of the network's structure, while successful resolution highlighted the value of persistence and iterative refinement. In summary, Lab 6 provided hands-on experience and insights into the nuanced aspects of network security configurations, emphasizing the importance of planning, attention to detail, and iterative refinement for robust network security setups. These reflections will undoubtedly shape future network configuration endeavors.

# References

1. S. V. (2015, December 19). VLAN + VTP + TRUNK + STP Configuration SWITCH CISCO (CCNA) Packet Tracer. YouTube. <https://www.youtube.com/watch?v=MG1-E6rNar8>
2. *Basic Firewall Configuration in Cisco Packet Tracer*. (2022, June 30). GeeksforGeeks. <https://www.geeksforgeeks.org/basic-firewall-configuration-in-cisco-packet-tracer/>
3. *Firewalls and types*. (2019, March 9). <https://community.cisco.com/t5/security-knowledge-base/firewalls-and-types/ta-p/3145864>