RIP, OSPF, AND EIGRP

Yogaraj Govindarajalu Prabagaran

# Table of Contents

[Table of Contents 2](#_Toc150118818)

[Lab 3 – Dynamic Routing 3](#_Toc150118819)

[Parts 3](#_Toc150118820)

[Description 3](#_Toc150118821)

[Observations 3](#_Toc150118822)

[Preparation 4](#_Toc150118823)

[Screenshots 4](#_Toc150118824)

[Reflection 46](#_Toc150118825)

[Lab 4 – EIGRP 47](#_Toc150118826)

[Parts 47](#_Toc150118827)

[Description 47](#_Toc150118828)

[Preparation 47](#_Toc150118829)

[Observations 48](#_Toc150118830)

[Screenshots 50](#_Toc150118831)

[Reflection 103](#_Toc150118832)

[References 104](#_Toc150118833)

# Lab 3 – Dynamic Routing

# Parts

## Description

In this lab, I embarked on a hands-on journey into the realm of dynamic routing, exploring the intricacies of the RIP and OSPF routing protocols. Building upon my experiences from previous labs and armed with a Cisco 2960 Switch, three Cisco 2811 Routers, and other essential devices, the initial setup promised exciting challenges. After thoroughly understanding the lab objectives and plan, I meticulously built and configured the network topology, adhering to the provided schematic. This included integrating devices like two workstations, web servers, and a switch. The primary goal was to ensure that all IP configurations were precise, creating a solid foundation for dynamic routing.

The lab was divided into three distinct sections. First, I constructed the topology and ensured connectivity. Subsequently, I delved into RIP routing, enabling RIP version 2, specifying network addresses, and configuring passive interfaces. I verified RIP configurations, examined routing databases, and tested the routing by confirming access to websites and pinging between network nodes. The transition to OSPF routing marked the next phase, involving disabling RIP on all routers and configuring OSPF with network addresses, passive interfaces, and even MD5 authentication for added security. This transition was meticulously tested, and throughout the lab, I diligently recorded observations and provided reflections on the routing protocols and network behavior. This lab was a testament to the importance of selecting the suitable routing protocol for a network's scale and security needs, with dynamic routing proving to be a dynamic and versatile tool in network management.

## Observations

Throughout the lab, I maintained a keen eye on the network's performance and behavior, and I am pleased to report that the entire process unfolded without a hitch. The assigned IP addresses and naming conventions were applied to the devices as specified in the lab document. The initial setup of the network topology proceeded seamlessly, with no significant challenges or issues encountered. As I transitioned to testing RIP routing, I was delighted to observe the successful execution of routing protocols, the flawless connectivity between network nodes, and the unfaltering access to web services. The meticulous configuration of RIP brought forth results that aligned with expectations, and I recorded this smooth performance in my observations.

In the subsequent lab phase, when transitioning to OSPF routing, I used a different Packet Tracer (pkt) file to ensure a clear demarcation between RIP and OSPF configurations. This change in file management allowed for a structured approach to testing the OSPF routing protocol. I meticulously documented the results and observed that OSPF routing was as seamless as RIP, showcasing the network's resilience. These observations will serve as valuable reference points for future network management decisions and troubleshooting, showcasing the adaptability of dynamic routing protocols like RIP and OSPF to ensure a smoothly functioning network.

## Preparation

For the successful execution of this lab, I took a methodical approach to preparation. The equipment list I needed was relatively straightforward: a Cisco 2960 Switch, three Cisco 2811 Routers, two PC Packet Tracer (PT) Objects, two PT Server Objects with web services enabled, and one PT Laptop. I ensured that all device passwords were set uniformly to "Secret55" for consistency. Equally important was utilizing the network assignments specified in the Subnet file provided within the assessment portal. This lab demanded a degree of continuity from previous exercises, so I tried to review configurations from Labs 1 and 2, which could be potentially migrated for efficiency. An essential aspect emphasized throughout the lab preparation was connecting to network devices – exclusively through SSH or local console interfaces, avoiding using GUI for configuration and maintenance. This disciplined approach to preparation paved the way for a smoother and more focused execution of the lab objectives.

## Screenshots

A diagram of a network

Description automatically generated

Figure 1-1: Dynamic Routing Topology.

This screenshot provides an overview of the network topology, highlighting the configuration of network devices, including routers, switches, workstations, and servers.

A screenshot of a computer

Description automatically generated

Figure 1-2: Enabling RIP and Network Addresses for the Waterloo Router.

I am configuring RIP routing on one of the routers in this screenshot. It shows the steps to enable RIP, set the version to RIP Version 2, specify the network addresses for RIP advertisement, and disable auto-summary.

A screenshot of a computer

Description automatically generated

Figure 1-2.1: Enabling RIP and Network Addresses for the Kitchener Router.

I am configuring RIP routing on one of the routers in this screenshot. It shows the steps to enable RIP, set the version to RIP Version 2, specify the network addresses for RIP advertisement, and disable auto-summary.

A screenshot of a computer

Description automatically generated

Figure 1-2.2: Enabling RIP and Network Addresses for the Stratford Router.

I am configuring RIP routing on one of the routers in this screenshot. It shows the steps to enable RIP, set the version to RIP Version 2, specify the network addresses for RIP advertisement, and disable auto-summary.

A screenshot of a computer

Description automatically generated

Figure 1-3: Verifying RIP Configuration for the Waterloo Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3.1: Verifying RIP Configuration for the Waterloo Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure 1-2: Verifying RIP Configuration for the Kitchener Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3.3: Verifying RIP Configuration for the Kitchener Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3.4: Verifying RIP Configuration for the Stratford Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure 1-3.5: Verifying RIP Configuration for the Stratford Router.

This screenshot displays the output of various commands used to verify the RIP configuration. It includes a list of routing protocols, the routing database, RIP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure 1-4: Testing RIP Routing on the Kitchener Server.

In this screenshot, I am conducting tests to ensure the functionality of RIP routing. It illustrates the successful access to the websites on the Kitchener Server and the Stratford Webserver from Waterloo\_PC1.

A screenshot of a computer

Description automatically generated

Figure 1-4.1: Testing RIP Routing on the Stratford Webserver.

In this screenshot, I am conducting tests to ensure the functionality of RIP routing. It illustrates the successful access to the websites on the Kitchener Server and the Stratford Webserver from Waterloo\_PC1.

A screenshot of a computer

Description automatically generated

Figure1-5: Testing RIP Routing Continued

Continuing from the previous screenshot, this demonstrates the successful pinging of the Stratford Server and Waterloo\_PC2 from the Kitchener Server, validating the RIP routing configuration.

A screenshot of a computer

Description automatically generated

Figure 1-6: Shows RIP events using debug mode for the Waterloo Router.

A screenshot of a computer

Description automatically generated

Figure 1-6.1: Shows RIP events using debug mode for Kitchener.

A screenshot of a computer

Description automatically generated

Figure 1-6.2: Shows RIP events using debug mode for Stratford.

Ospf:

A diagram of a network

Description automatically generated

Figure1-1: Dynamic Routing Topology

This screenshot provides an overview of the network topology, highlighting the configuration of network devices, including routers, switches, workstations, and servers. It serves as a visual representation of the lab's network setup.

A screenshot of a computer

Description automatically generated

Figure1-2: Enabling OSPF and Network Addresses for the Waterloo Router

In this screenshot, I am configuring OSPF routing on the Waterloo Router. It shows the steps to enable OSPF, specify the network addresses for OSPF advertisement, and configure passive interfaces. This is a critical step in setting up OSPF routing.

A screenshot of a computer

Description automatically generated

Figure1-2.1: Enabling OSPF and Network Addresses for the Kitchener Router

Similar to the previous screenshot, this one demonstrates the configuration of OSPF routing, but this time on the Kitchener Router. The steps include enabling OSPF, specifying network addresses, and configuring passive interfaces to ensure proper OSPF functionality.

A screenshot of a computer

Description automatically generated

Figure1-2.2: Enabling OSPF and Network Addresses for the Stratford Router

Continuing with OSPF configurations, this screenshot showcases the setup on the Stratford Router. It involves enabling OSPF, specifying network addresses, and configuring passive interfaces, aligning with the lab's OSPF routing objectives.

A screenshot of a computer

Description automatically generated

Figure1-3: Verifying OSPF Configuration for the Waterloo Router

This screenshot displays the output of various commands to verify the Waterloo Router's OSPF configuration. It includes routing protocols, the routing database, OSPF routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3-0.5: Verifying OSPF Configuration for the Waterloo Router

This screenshot displays the output of various commands to verify the Waterloo Router's OSPF configuration. It includes routing protocols, the routing database, OSPF routing information, and events captured in debug mode.

A screenshot of a computer screen

Description automatically generated

Figure1-3.1: Verifying OSPF Configuration for the Kitchener Router

Similar to the previous screenshot, this one focuses on verifying the OSPF configuration, but this time for the Kitchener Router. It provides insights into routing protocols, routing databases, and OSPF events in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3.1.5: Verifying OSPF Configuration for the Kitchener Router

Similar to the previous screenshot, this one focuses on verifying the OSPF configuration, but this time for the Kitchener Router. It provides insights into routing protocols, routing databases, and OSPF events in debug mode.

A screenshot of a computer

Description automatically generated

Figure1-3.3: Verifying OSPF Configuration for the Stratford Router

This screenshot examines the OSPF configuration on the Stratford Router, ensuring that the routing protocols, databases, and OSPF events align with the desired configurations.

A screenshot of a computer

Description automatically generated

Figure1-3.4: Verifying OSPF Configuration for the Stratford Router

Similar to the previous screenshot, this one continues to verify the OSPF configuration for the Stratford Router. It provides essential insights into OSPF routing behavior and debugging information.

A screenshot of a computer

Description automatically generated

Figure1-4: Testing OSPF Routing on the Kitchener Server

In this screenshot, I conduct tests to ensure the functionality of OSPF routing. It showcases the successful access to the websites on the Kitchener Server and the Stratford Webserver from Waterloo\_PC1.

A screenshot of a computer

Description automatically generated

Figure1-4.1: Testing OSPF Routing on the Stratford Webserver

Similar to the previous screenshot, this one highlights the successful testing of OSPF routing. It confirms access to the websites on the Kitchener Server and the Stratford Webserver from Waterloo\_PC1.

A computer screen shot of a computer program

Description automatically generated

Figure1-5: Testing OSPF Routing Continued

Continuing from the previous screenshot, this demonstrates the successful pinging of the Stratford Server and Waterloo\_PC2 from the Kitchener Server, validating the OSPF routing configuration.

A screenshot of a computer

Description automatically generated

Figure1-6: Shows OSPF events using debug mode for the Waterloo Router

This screenshot captures OSPF events using debug mode for the Waterloo Router, providing a detailed view of the OSPF routing behavior and any events or issues encountered during the testing process.

A screenshot of a computer

Description automatically generated

Figure1-6.1: Shows OSPF events using debug mode for Kitchener

Continuing with OSPF event capture, this screenshot focuses on the Kitchener Router, shedding light on the OSPF events and routing behavior during testing.

A screenshot of a computer

Description automatically generated

Figure1-6.2: Shows OSPF events using debug mode for Stratford

This screenshot highlights the OSPF events captured using debug mode for the Stratford Router, offering insights into the OSPF routing protocol's behavior and performance during the lab testing phase.

A screenshot of a computer

Description automatically generated

Figure 1-7: Configuring OSPF Authentication with MD5 on Kitchener Router

Like the previous screenshots, this one focuses on the Kitchener Router. It showcases the configuration of OSPF authentication using MD5 encryption within the OSPF router process, enhancing the network's security.

A screenshot of a computer

Description automatically generated

Figure 1-8: Setting MD5 Authentication on Kitchener Router Interfaces

This screenshot continues the process of OSPF authentication with MD5 on the Kitchener Router. It highlights the critical step of configuring MD5 authentication on each interface that will receive OSPF updates, reinforcing the network's authentication security.

A screenshot of a computer

Description automatically generated

Figure 1-9: Configuring OSPF Authentication with MD5 on Stratford Router

In this screenshot, the focus shifts to the Stratford Router. It demonstrates the configuration of OSPF authentication with MD5 encryption within the OSPF router process on the Stratford Router, a vital step in securing OSPF communications. The router is a vital step in securing OSPF communications.

A screenshot of a computer

Description automatically generated

Figure 1-10: Setting MD5 Authentication on Stratford Router Interfaces

Continuing with the Stratford Router, this screenshot illustrates the process of setting MD5 authentication on the interfaces of the Stratford Router that will receive OSPF updates. This measure enhances the overall network security by ensuring that OSPF updates are authenticated.

A screenshot of a computer

Description automatically generated

Figure 1-11: This screenshot displays OSPF debug events in the Waterloo Router.

A screenshot of a computer

Description automatically generated

Figure 1-12: This screenshot displays OSPF debug events in the Kitchener Router.

A screenshot of a computer

Description automatically generated

Figure 1-13: This screenshot displays OSPF debug events in the Stratford Router.

A screenshot of a computer

Description automatically generated

Figure 1-14: Testing OSPF Routing with MD5 Authentication from Waterloo\_PC1

With the MD5 authentication in place, this screenshot depicts the testing phase. From Waterloo\_PC1, I verify the network's functionality, ensuring successful access to the websites on the Kitchener and Stratford servers. This demonstrates the network's robustness even with enhanced security measures.

A screenshot of a computer

Description automatically generated

Figure 1-14.1: Testing OSPF Routing with MD5 Authentication from Waterloo\_PC1

With the MD5 authentication in place, this screenshot depicts the testing phase. From Waterloo\_PC1, I verify the network's functionality, ensuring successful access to the websites on the Kitchener and Stratford servers. This demonstrates the network's robustness even with enhanced security measures.

A computer screen shot of a computer program

Description automatically generated

Figure 1-15: Testing OSPF Routing with MD5 Authentication from Kitchener Server

Similar to the previous test, this screenshot focuses on the Kitchener Server. It demonstrates the successful pinging of the Stratford Server and Waterloo\_PC2, confirming that OSPF routing with MD5 authentication functions as expected, reinforcing the network's security.

## Reflection

In completing this lab on dynamic routing, I embarked on an individual journey to set up a network infrastructure using RIP and OSPF routing protocols, along with Variable Length Subnet Masks (VLSM) and a single IP address for all required networks. The lab, which builds upon the knowledge gained in previous exercises, required a comprehensive understanding of the objectives and careful planning. It involved configuring a network of Cisco routers, switches, workstations, and web servers.

The initial phase of building and configuring the topology was a critical starting point. It involved configuring network devices with assigned IPs and verifying connectivity. This setup process aimed to establish a foundation for dynamic routing and ensured that all components could communicate effectively. The subsequent transition to configuring RIP routing was a significant step, enabling me to explore the intricacies of this protocol. The lab provided opportunities to test and verify RIP functionality, including checking access to websites, pinging servers, and capturing events using debug mode.

A pivotal moment in the lab came when transitioning from RIP to OSPF routing. Disabling RIP and enabling OSPF required careful attention, and configuring OSPF authentication using MD5 further enhanced security. The OSPF routing and authentication tests were conducted meticulously, ensuring that routing updates and communication were not compromised.

In reflecting on this lab, I found comparing the benefits of RIP and OSPF routing intriguing. With its simplicity, RIP might be suitable for smaller networks, while OSPF offers more advanced features and scalability, making it preferable for more extensive, complex infrastructures. Understanding the routing path from the Guelph router to the Stratford router and the timing of routing update transfer were enlightening aspects of this exercise.

As I conclude this lab report, I emphasize the importance of saving and uploading packet tracer files and running configs, as they serve as valuable evidence of the completed work. This lab experience enhanced my understanding of dynamic routing and reinforced the significance of meticulous planning and documentation in network configuration and troubleshooting.

# Lab 4 – EIGRP

# Parts

## Description

Lab 4 – EIGRP aimed to design, configure, and test a hub-and-spoke network topology utilizing the Enhanced Interior Gateway Routing Protocol (EIGRP). This lab built upon the knowledge and skills acquired in previous labs (Labs 1, 2, and 3) and introduced EIGRP as the routing protocol of choice. EIGRP, being a Cisco-proprietary routing protocol, offers unique advantages in terms of efficiency, convergence, and security. The lab involved deploying EIGRP routing within a complex network, requiring meticulous routers, switches, and workstation configuration.

The network topology used in this lab was structured as a hub-and-spoke model, wherein a central router (hub) connected to multiple remote routers (spokes). The network infrastructure included six Cisco 2960 switches, six Cisco 2811 routers, six PC Packet Tracer (PT) objects, and one PT laptop. All devices were configured with the password "Secret55" for security purposes.

As I approached this lab, I meticulously followed the provided schematic, ensuring it reflected the assigned IP addresses and required naming conventions for the network topology. The lab consisted of two main parts: building and configuring the network topology and configuring and testing routing using EIGRP. This hands-on experience allowed me to delve into EIGRP routing, focusing on its configuration intricacies and understanding how it impacts network performance. I also set up MD5 authentication on each interface responsible for receiving EIGRP updates.

## Preparation

The lab required me to create a hub-and-spoke network topology using the Enhanced Interior Gateway Routing Protocol (EIGRP). The critical task was configuring the network devices and documenting the entire process. The guidelines underscored the importance of reading through the entire lab document to grasp the objectives fully. In order to execute this lab effectively, I needed the following resources:

Hardware Components:

6 Cisco 2960 Switches

6 Cisco 2811 Routers

6 PC Packet Tracer (PT) Objects

Passwords: All network devices were configured with the password "Secret55" to ensure security and consistency.

IP Addresses: I used the IP addresses assigned in the Subnet file from the assessment portal. This practice ensured conformity with the lab's specifications.

In line with the lab's guidelines, I used SSH or local console connections to interact with the network devices. Using graphical user interfaces (GUI) for device configuration was discouraged, highlighting the significance of mastering the command-line interface (CLI) for effective network management.

## Observations

Throughout Lab 4 – EIGRP, I meticulously documented my observations and experiences, aiming to comprehensively understand the lab's concepts and objectives. The observations were made at various lab stages, and I encountered both expected outcomes and some interesting issues. Here are my observations:

Part 1 - Building and Configuring the Topology:

Initial Configuration: As I progressed with building and configuring the network topology according to the lab schematic, I ensured that I precisely followed the steps outlined in Lab 2. The configuration process was smooth, with no significant hiccups.

IP Assignment: Assigning IP addresses to the workstation objects, routers, and switches based on the subnetted IP address was straightforward but also the most challenging part of this lab. The adherence to proper IP addressing conventions was crucial.

Please note that I had to distinguish between the LAN and WAN networks and assign IP to every device in the topology, which was straightforward but mentally draining.

Ping Tests: I conducted multiple ping tests to validate the connectivity of the workstations with the routers, switches, and switches with workstations. These tests were executed per the lab instructions, and I encountered no issues. All devices were successfully communicated.

SSH Configuration: I successfully configured SSH access for the workstations to connect to their respective switches and routers. This is a crucial step for secure network management.

Part 2 - Configure and Test Routing using EIGRP:

Loopback Interfaces: I configured loopback interfaces on the routers as instructed. This step is essential for network stability and redundancy.

EIGRP Configuration: Enabling EIGRP and configuring its parameters, such as network addresses and passive interfaces, was accomplished without complications.

Verification Commands: I used various verification commands to ensure the correct configuration of EIGRP:

Show IP protocols: This command helped me confirm that EIGRP was running on the routers.

Show ip eigrp interfaces: I used this command to verify the interfaces participating in EIGRP.

Show the IP route to verify the EIGRP routing table and learned routes.

Ping Tests: I conducted ping tests from PC1 to other PCs in the network, ensuring successful communication. These tests validated the functionality of EIGRP routing.

Part 3 - Configure and Test EIGRP Authentication:

EIGRP Authentication: I configured EIGRP authentication using MD5, creating a keychain and applying MD5 authentication to relevant interfaces. This security measure enhances the integrity of routing updates.

Debugging Mode: I employed debugging commands to ensure authentication was functioning correctly. Notably, I used the debug eigrp packet command to monitor EIGRP packets. This offered insights into the authentication process.

Ping Tests with Authentication: I verified that all PCs in the network could still communicate successfully after implementing EIGRP MD5 authentication. This step reassured me that security measures did not hinder normal network operations.

In conclusion, my observations throughout the lab provided valuable insights into deploying an EIGRP-based network topology. I gained a practical understanding of EIGRP configurations, loopback interfaces, and the significance of network security through authentication. These observations contribute to my growing expertise in network administration and routing protocols.

## Screenshots

A diagram of a network

Description automatically generated

Figure 2-1: Dynamic Routing Topology

This screenshot provides an overview of the network topology, highlighting the configuration of network devices, including routers, switches, workstations, and servers. It serves as a visual representation of the lab's network setup.

A screenshot of a computer

Description automatically generated

Figure 2-2: Enabling EIGRP and Network Addresses for the Spoke1.

In this screenshot, I am configuring EIGRP routing on Spoke1. It shows the steps to enable EIGRP, specify the network addresses for EIGRP advertisement, and configure passive interfaces. This is a critical step in setting up EIGRP routing.

A screenshot of a computer

Description automatically generated

Figure 2-3: Enabling EIGRP and Network Addresses for the Spoke2.

Similar to the previous screenshot, this one demonstrates the configuration of EIGRP routing, but this time on the Spoke2. The steps include enabling EIGRP, specifying network addresses, and configuring passive interfaces to ensure proper EIGRP functionality.

A screenshot of a computer

Description automatically generated

Figure 2-4: Enabling EIGRP and Network Addresses for the Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-5: Enabling EIGRP and Network Addresses for the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-6: Enabling EIGRP and Network Addresses for the HUB-A.

Continuing with EIGRP configurations, this screenshot showcases the setup on the HUB1. It involves enabling EIGRP, specifying network addresses, and configuring passive interfaces, aligning with the lab's EIGRP routing objectives.

A screenshot of a computer

Description automatically generated

Figure 2-7: Enabling EIGRP and Network Addresses for the HUB-B.

A screenshot of a computer

Description automatically generated

Figure 2-8: Verifying EIGRP Configuration for the Spoke1.

This screenshot displays the output of various commands to verify the EIGRP configuration on the Spoke1. It includes routing protocols, the routing database, EIGRP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure 2-8.1: Verifying EIGRP Configuration for the Spoke1.

A screenshot of a computer

Description automatically generated

Figure 2-8.2: Verifying EIGRP Configuration for the Spoke1.

A screenshot of a computer

Description automatically generated

Figure 2-8.3: Verifying EIGRP Configuration for the Spoke1.

A screenshot of a computer

Description automatically generated

Figure 2-8.4: Verifying EIGRP Configuration for the Spoke1.

A screenshot of a computer

Description automatically generated

Figure 2-9: Verifying EIGRP Configuration for the Spoke2.

Similar to the previous screenshot, this one focuses on verifying the EIGRP configuration, but this time for the Spoke2. It provides insights into routing protocols, routing databases, and EIGRP events in debug mode.

A screenshot of a computer

Description automatically generated

Figure 2-9.1: Verifying EIGRP Configuration for the Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-9.2: Verifying EIGRP Configuration for the Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-9.3: Verifying EIGRP Configuration for the Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-9.4: Verifying EIGRP Configuration for the Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-10: Verifying EIGRP Configuration for the Spoke3.

This screenshot examines the EIGRP configuration on Spoke3, ensuring that the routing protocols, databases, and EIGRP events align with the desired configurations.

A screenshot of a computer

Description automatically generated

Figure 2-10.1: Verifying EIGRP Configuration for the Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-10.2: Verifying EIGRP Configuration for the Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-10.4: Verifying EIGRP Configuration for the Spoke3.

A screenshot of a computer program

Description automatically generated

Figure 2-10.5: Verifying EIGRP Configuration for the Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-11: Verifying EIGRP Configuration for the Spoke4.

This screenshot examines the EIGRP configuration on the Spoke4, ensuring that the routing protocols, databases, and EIGRP events align with the desired configurations.

A screenshot of a computer

Description automatically generated

Figure 2-11.1: Verifying EIGRP Configuration for the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-11.2: Verifying EIGRP Configuration for the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-11.3: Verifying EIGRP Configuration for the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-11.4: Verifying EIGRP Configuration for the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-12: Verifying EIGRP Configuration for the HUB-A.

This screenshot displays the output of various commands to verify the EIGRP configuration on the HUB1. It includes routing protocols, the routing database, EIGRP routing information, and events captured in debug mode.

A screenshot of a computer

Description automatically generated

Figure 2-12.1: Verifying EIGRP Configuration for the HUB-A.

A screenshot of a computer

Description automatically generated

Figure 2-12.2: Verifying EIGRP Configuration for the HUB-A.

A screenshot of a computer program

Description automatically generated

Figure 2-12.3: Verifying EIGRP Configuration for the HUB-A.

A screenshot of a computer program

Description automatically generated

Figure 2-12.4: Verifying EIGRP Configuration for the HUB-A.

A screenshot of a computer

Description automatically generated

Figure 2-13: Verifying EIGRP Configuration for the HUB-B.

Continuing with EIGRP configurations, this screenshot showcases the setup on the Stratford Router. It involves enabling EIGRP, specifying network addresses, and configuring passive interfaces, aligning with the lab's EIGRP routing objectives.

A screenshot of a computer

Description automatically generated

Figure 2-13.1: Verifying EIGRP Configuration for the HUB-B.

A screenshot of a computer

Description automatically generated

Figure 2-13.2: Verifying EIGRP Configuration for the HUB-B.

A screenshot of a computer

Description automatically generated

Figure 2-13.3: Verifying EIGRP Configuration for the HUB-B.

A screenshot of a computer program

Description automatically generated

Figure 2-13.4: Verifying EIGRP Configuration for the HUB-B.

A computer screen shot of a computer program

Description automatically generated

Figure 2-14: Testing EIGRP Routing on the PC1.

In this screenshot, I conduct tests to ensure the functionality of EIGRP routing. It showcases successful access to the pings on all the other PCs from PC1.

A screenshot of a computer program

Description automatically generated

Figure 2-14.1: Testing EIGRP Routing on the PC1.

A screenshot of a computer

Description automatically generated

Figure 2-15: Shows EIGRP events using debug mode for Spoke1.

This screenshot captures EIGRP events using debug mode for Spoke1, providing a detailed view of the EIGRP routing behavior and any events or issues encountered during the testing process.

A screenshot of a computer

Description automatically generated

Figure 2-16: Shows EIGRP events using debug mode for Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-17: Shows EIGRP events using debug mode for Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-18: Shows EIGRP events using debug mode for Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-19: Shows EIGRP events using debug mode for HUB-A.

A screenshot of a computer

Description automatically generated

Figure 2-20: Shows EIGRP events using debug mode for HUB-B.

Md5

A screenshot of a computer

Description automatically generated

Figure 2-21: This screenshot displays EIGRP debug events in the Spoke1.

A screenshot of a computer

Description automatically generated

Figure 2-22: This screenshot displays EIGRP debug events in the Spoke2.

A screenshot of a computer

Description automatically generated

Figure 2-23: This screenshot displays EIGRP debug events in the Spoke3.

A screenshot of a computer

Description automatically generated

Figure 2-24: This screenshot displays EIGRP debug events in the Spoke4.

A screenshot of a computer

Description automatically generated

Figure 2-25: This screenshot displays EIGRP debug events in the HUB-A.

A screenshot of a computer

Description automatically generated

Figure 2-26: This screenshot displays EIGRP debug events in the HUB-B.

A computer screen shot of a computer program

Description automatically generated

Figure 2-27: Testing EIGRP Routing with MD5 Authentication on the PC1.

In this screenshot, I conduct tests to ensure the functionality of EIGRP routing. It showcases successful access to the pings on all the other PCs from PC1.

A computer screen shot of a program

Description automatically generated

Figure 2-28: Testing EIGRP Routing with MD5 Authentication on the PC1.

## Reflection

This lab built upon the knowledge and skills gained from previous labs, pushing me to understand and implement EIGRP in a hub and spoke network topology. Here is my reflection on various aspects of this lab:  
Completing Labs 1, 2, and 3: These earlier labs were instrumental in laying the groundwork for Lab 4. The gradual progression of complexity allowed me to grasp critical concepts. My understanding of subnetting and IP addressing proved essential in the successful completion of Lab 4.

Initial Topology Configuration: In Part 1, I began by building and configuring the network topology as per the schematic provided. This process was well-structured and intuitive. Following the steps and guidelines provided in the lab manual ensured that my network topology was accurately set up.

Initial IP Configuration: The IP configuration step was quickly the most frustrating in this lab, yet it was also straightforward. Configuring the IP addresses on the Workstation Objects, routers, and switches was a crucial step. Ensuring that the assigned IP addresses and naming conventions were correctly implemented was vital. Seeing that my workstations could ping all interfaces on their respective routers and switches was satisfying. Additionally, the ability to establish SSH connections was a testament to the proper configuration of the devices.  
EIGRP Routing Configuration: Part 2 focused on enabling EIGRP routing on each device acting as a router. This required setting up loopback interfaces, specifying network addresses for EIGRP, and configuring passive interfaces. EIGRP's features, such as route summarization and route filtering, were essential in managing routing information effectively.

EIGRP Verification: The verification step was critical in ensuring EIGRP functions as expected. By running various commands, I could confirm the correct operation of EIGRP. The output of these commands provided insights into routing protocols, routing databases, neighbors, topology, and traffic.

EIGRP Testing: Testing EIGRP routing from PC1 to all other PCs was a satisfying part of the lab. The successful pinging of all PCs in the topology validated the correctness of the EIGRP configuration. Debugging mode allowed me to monitor EIGRP events, ensuring the routing protocol operated optimally.

EIGRP Authentication: In Part 3, I introduced an extra layer of security by implementing EIGRP authentication using MD5. Creating keychains and configuring MD5 authentication within the EIGRP router process significantly enhanced the network's security. Testing EIGRP routing with MD5 authentication assured the authentication's effectiveness.

In conclusion, INFO8490 Lab 4 – EIGRP Routing provided a hands-on opportunity to apply theoretical knowledge in a real-world scenario. The lab's structured approach, well-defined tasks, and hands-on experience with EIGRP, subnetting, and IP addressing have significantly enriched my understanding of network routing and security.

# References

1. Wallace, K. (n.d.). CCNA Routing and Switching 200-125. O’Reilly Online Learning. <https://learning.oreilly.com/videos/ccna-routing-and/9780134580715/9780134580715-CCNA_03_05_02/>
2. *CCNP Routing and Switching ROUTE 300-101 Complete Video Course*. (n.d.). O’Reilly Online Learning. <https://learning.oreilly.com/videos/ccnp-routing-and/9780133962123/9780133962123-4_8_0_0_Basic_EIGRP_Configuration_Example/>?
3. *CCNP Routing and Switching ROUTE 300-101 Complete Video Course*. (n.d.). O’Reilly Online Learning. <https://learning.oreilly.com/videos/ccnp-routing-and/9780133962123/9780133962123-3_1_0_0_RIP_Fundamentals/>?
4. *Cisco CCNA Routing and Switching 200-120*. (n.d.). O’Reilly Online Learning. <https://learning.oreilly.com/videos/cisco-ccna-routing/9780133553734/9780133553734-3_9_2_1_1_OSPF_Basics/\>