Design and Implementation of Secure and Scalable Network Infrastructure for Multi-Site Organizations

Yogaraj Govindarajalu Prabagaran

# Table of Contents

[Table of Contents 2](#_Toc153054972)

[Lab - Project 3](#_Toc153054973)

[Parts 3](#_Toc153054974)

[Description 3](#_Toc153054975)

[Preparation 3](#_Toc153054976)

[Observations 4](#_Toc153054977)

[Screenshots 5](#_Toc153054978)

[Reflection 27](#_Toc153054979)

[References 28](#_Toc153054980)

# Lab - Project

# Parts

## Description

The project aims to create a comprehensive network solution for a three-site organization (Waterloo, Kitchener, and Guelph), adhering to specific policy requirements. The network design includes a single IP address with a /28 CIDR and features Access and Edge routers at each site. The routers are connected to a daisy chain using EIGRP for routing updates with MD5 authentication. Security measures encompass Message of the Day banners, privileged mode passwords, enforced console logins, encrypted service passwords, and SSH login on switches. Each site has unique requirements, such as Tacacs Server authentication for remote SSH login at Site A, OSPF with authentication at Site B, and RIP for routing at Site C. Additionally, specific VLAN configurations, inter VLAN routing, and secure redistribution of routing information are implemented across the sites. The project documentation will cover design details, topology schematics, running-config files, and Packet Tracer files.

## Preparation

In preparation for the network design and implementation project, I meticulously gathered and analyzed the specific requirements outlined in the assignment document, identifying the unique needs of each site, including routing protocols, security measures, VLAN configurations, and routing information redistribution. I compiled an inventory of all necessary networking devices, verified Packet Tracer compatibility, and assigned IP addresses following the provided base address. I ensured uniqueness by including my initials and the last four digits of my student ID in all node names. Adhering to strict naming conventions, I planned and visualized the topology for each site using tools like Visio while also determining authentication methods for remote access and configuring secure authentication for routing protocols. Additionally, I detailed security measures, such as banners, passwords, console logins, encrypted service passwords, and SSH login on switches. This comprehensive preparation lays the groundwork for a well-organized and successful network solution, ensuring a smooth transition into the subsequent design and implementation phases.

**SITE A (Waterloo)**

Waterloo\_EDGE\_YP9578 - 10.150.123.146/28

Waterloo\_ACCESS\_ YP9578 - 10.150.123.1/28

Waterloo\_TACACS-SRV\_ YP9578 - 10.150.123.5/28

Waterloo\_WEB-SRV\_ YP9578- 10.150.123.14/28

Waterloo\_SW1\_ YP9578

Waterloo\_SW2\_ YP9578

Waterloo\_SW3\_ YP9578

**SITE B (Kitchener)**

kitchener\_EDGE\_ YP9578 - 10.150.123.161/28

kitchener\_ACCESS\_ YP9578 - 10.150.123.162/28

kitchener\_SW1\_ YP9578 - 10.150.123.49/28

kitchener\_SW2\_ YP9578 - 10.150.123.65/28

kitchener\_PC1\_ YP9578 - 10.150.123.50/28

kitchener\_PC2\_ YP9578 - 10.150.123.52/28

kitchener\_PC3\_ YP9578 - 10.150.123.66/28

kitchener\_PC4\_ YP9578 - 10.150.123.67/28

kitchener\_Radius-SRV\_ YP9578 - 10.150.123.51/28

kitchener\_Multilayer\_ YP9578

**SITE C (Guelph)**

Guelph\_ACCESS\_ YP9578 - 10.150.123.34/28

Guelph\_EDGE\_ YP9578 - 10.150.123.33/28

Guelph\_PC1\_ YP9578 - 10.150.123.82/28

Guelph\_PC2\_ YP9578 - 10.150.123.98/28

Guelph\_PC3\_ YP9578 - 10.150.123.114/28

## Observations

Throughout the implementation and testing phases of the network design, I diligently observed and verified key aspects to ensure the successful deployment of the configured infrastructure. This included testing the functionality of routing protocols at each site (EIGRP at Site A, OSPF at Site B, and RIP at Site C), confirming secure authentication methods, such as Tacacs Server at Site A and Radius Server at Site B, and validating security measures like banners, passwords, and SSH login on switches. Additionally, I thoroughly tested VLAN configurations and inter-VLAN routing at Site B to ensure seamless communication between computers on different VLANs. Critical observations were made regarding the secure redistribution of routing information between Edge routers at different sites and the correct implementation of remote access and management configurations, including authenticated remote logins. The designed topology for each site was visually verified to ensure consistency with the implemented configuration, collectively confirming the successful adherence to policy requirements and design specifications, with prompt resolution of any identified issues to ensure the reliability of the deployed network infrastructure.

## Screenshots

A diagram of a network

Description automatically generated

Figure 1.1: Depicts the network topology designed in a daisy chain configuration, encompassing three sites—WATERLOO, KITCHENER, and GUELPH.

SITE A:

A screenshot of a computer

Description automatically generated

Figure 2.1: Illustrates SW1’s root port, blocking port, and corresponding cost.

A screenshot of a computer

Description automatically generated

Figure 2.2 presents information on SW2's root port and associated costs.

A screenshot of a computer screen

Description automatically generated

Figure 2.3: Displays details of SW3 as the root bridge, displaying port status and associated costs.

A screenshot of a computer

Description automatically generated

Figure 2.4: Highlights the presence of a web server with a custom homepage.

A screenshot of a computer

Description automatically generated

Figure 2.5: Exhibits the output following access to a custom website.

A computer screen shot of a black screen

Description automatically generated

Figure 2.6: Captures the process of remote SSH login to the Access router utilizing a Tacacs Server.

A computer screen shot of a black screen

Description automatically generated

Figure 2.7: Demonstrates the remote SSH login to the Edge router, authenticated through a Tacacs Server.

A screenshot of a computer

Description automatically generated

Figure 2.8: Showcase the configuration involving MD5 and EIGRP

A screenshot of a computer

Description automatically generated

Figure 2.9: Showcase the configuration involving MD5 and EIGRP.

SITE B:

A screenshot of a computer program

Description automatically generated

Figure 3.1: Depicts the MD5 and OSPF configuration in the Edge router.

A screenshot of a computer program

Description automatically generated

Figure 3.2: Presents the MD5 and OSPF configuration in the Access router.

A screenshot of a computer

Description automatically generated

Figure 3.3: Provides insights into the redistribution configuration.

A screenshot of a computer

Description automatically generated

Figure 3.4: Display the remote login process to the Access and Edge routers utilizing a Radius Server.

A computer screen shot of a computer screen

Description automatically generated

Figure 3.5: Display the remote login process to the Access and Edge routers utilizing a Radius Server.

A screenshot of a computer

Description automatically generated

Figure 3.6: Show the VLAN status in SW1.

A screenshot of a computer

Description automatically generated

Figure 3.7: Show the VLAN status in SW2.

A screenshot of a computer program

Description automatically generated

Figure 3.8: Demonstrate successful pings between computers on the same switch and different switches.

A computer screen shot of a black screen

Description automatically generated

Figure 3.10

Figure 3.10, Figure 3.11, Figure 3.12, and Figure 3.13 Illustrate successful pings to devices within SITE C and from the Guelph site to SITE B.

A computer screen shot of a black screen

Description automatically generated

Figure 3.11

Figure 3.10, Figure 3.11, Figure 3.12, and Figure 3.13 Illustrate successful pings to devices within SITE C and from the Guelph site to SITE B.

A screenshot of a computer program

Description automatically generated

Figure 3.12

Figure 3.10, Figure 3.11, Figure 3.12, and Figure 3.13 Illustrate successful pings to devices within SITE C and from the Guelph site to SITE B.

A screenshot of a computer program

Description automatically generated

Figure 3.13

Figure 3.10, Figure 3.11, Figure 3.12, and Figure 3.13 Illustrate successful pings to devices within SITE C and from the Guelph site to SITE B.

A computer screen shot of a computer program

Description automatically generated

Figure 3.14: Showcase successful pings from the Guelph site to all devices in SITE B.

A computer screen shot of a black screen

Description automatically generated

Figure 3.15: Showcase successful pings from the Guelph site to all devices in SITE B.

SITE C:

A screenshot of a computer

Description automatically generated

Figure 4.1: Displays the RIP configuration and redistribution in the Edge router.

A screenshot of a computer

Description automatically generated

Figure 4.2: Highlights the RIP configuration in the Access router.

## Reflection

Embarking on this immersive network design and implementation project, I've gained profound insights into the complexities of creating a resilient and secure infrastructure. Challenges in designing a daisy chain topology underscored the need for meticulous consideration of routing protocols and authentication methods to ensure that connectivity and security standards were upheld. The strategic and security-centric approaches applied to configure and connect Sites A, B, and C align with the overarching theme of this project. The selection and implementation of routing protocols like EIGRP, OSPF, and RIP were instrumental, emphasizing the importance of aligning protocol choices with specific network requirements. The configuration requirements for Site A, including EIGRP with secure authentication for routing updates and TACACS-enhanced SSH access control, exemplify a stable and regulated routing environment. The loop-free Layer 2 switching design at Site A, with careful selection and configuration of the Root Bridge, Root Ports, Designated Ports, Blocking Ports, and Port Costs, adds to the network's stability. Including a web server necessitates careful configuration and security precautions to ensure flexibility while maintaining security. In Site B, with authentication and secure data redistribution between SITE A and SITE B, OSPF showcases a commitment to scalability and consistent routing protocols. Credential management using a Radius server enhances security, and the configuration of VLANs, VLAN trunking, and Inter VLAN Routing on a Layer 3 switch supports efficient traffic management and segmentation. Thorough testing is evident in the requirement to ensure connectivity between computers on various VLANs and the ability to log in remotely and PING every device. Site C introduces simplicity with RIP for routing, emphasizing the need for proper planning to ensure network integrity during the secure redistribution of routing information between SITE A and SITE C. Network segmentation and security are further indicated by the Access Router's three distinct linked subnets and local authentication for remote management. Granular control over access is achieved through configuring remote management with local authentication on every network device, contributing to a distributed security architecture. The consistent use of various authentication methods for remote access and routing across all sites reflects a shared dedication to security. The widespread usage of VLANs throughout the network enhances performance and security, showcasing a commitment to segmentation. It becomes evident that thorough testing and comprehensive documentation are essential components and integral to guaranteeing correct operation, troubleshooting capabilities, and facilitating future network adjustments.

## **References**

1. S. A. (2020, May 13). Configuring RIP OSPF and EIGRP Redistribution in Cisco Packet Tracer in Hindi/Urdu | CCNA CCNP |. YouTube. <https://www.youtube.com/watch?v=LdqGCYZ0P7Q>
2. M. (2011, May 20). *Redistributing OSPF/EIGRP and RIP*. TechExams Community. <https://community.infosecinstitute.com/discussion/66303/redistributing-ospf-eigrp-and-rip>
3. L. (2017, January 13). *Part 1: EIGRP, RIP, OSPF Redistribution configuration*. The DEVNET GRIND! <https://loopedback.com/2017/01/09/part-1-eigrp-rip-ospf-redistribution-configuration/>
4. Molenaar, R. (2022, October 20). *Redistribution between EIGRP and OSPF*. NetworkLessons.com. <https://networklessons.com/cisco/ccie-enterprise-infrastructure/redistribution-between-eigrp-and-ospf>