Simple network topology and Static Routing

Yogaraj Govindarajalu Prabagaran

# Table of Contents

[Table of Contents 2](#_Toc147440234)

[Lab 1 - Simple network topology 3](#_Toc147440235)

[Parts 3](#_Toc147440236)

[Description 3](#_Toc147440237)

[Preparation 4](#_Toc147440238)

[Observations 5](#_Toc147440239)

[Screenshots 7](#_Toc147440240)

[Reflection 42](#_Toc147440241)

[Lab 2 – Static Routing 46](#_Toc147440242)

[Parts 46](#_Toc147440243)

[Description 46](#_Toc147440244)

[Preparation 46](#_Toc147440245)

[Observations 47](#_Toc147440246)

[Screenshots 49](#_Toc147440247)

[Reflection 63](#_Toc147440248)

[References 65](#_Toc147440249)

# Lab 1 - Simple network topology

# Parts

## Description

Part 1 of this lab focuses on building the network topology based on the provided schematic. The goal is to physically represent the network by connecting the required devices, including layer two switches, a router, a web server, and multiple workstations. This initial setup is crucial as it forms the foundation for subsequent configurations. Per the lab instructions, we will ensure that the topology accurately reflects the assigned IP addresses and naming conventions. Part 2 involves configuring the network devices in the previously built topology. We will start by connecting to each network device using a console connection from the laptop. The primary configuration task in this part is to set up a Message of the Day (MOTD) banner on each network device, displaying a unique name. This banner configuration serves as a form of identification and ensures that users know their device's identity when accessing it. In Part 3, we focus on enhancing security by configuring each network device to require a password when changing to privileged mode. This password, set as "Secret55," adds a layer of protection to the devices. Whether it is a router or a switch, configuring the privileged mode password is the same. This step enhances the overall security posture of the network. Part 4 involves configuring each network device's console and virtual terminal ports to enforce login requirements. Users must enter a password (Secret55) when accessing the devices. This added layer of security ensures that only authorized users can access the devices, reducing the risk of unauthorized access and potential security breaches. Part 5 focuses on configuring Secure Shell (SSH) on each network device to enable secure remote access. SSH is a widely used protocol for secure communication and configuring it on routers and switches ensures that remote connections are encrypted and secure. This step enhances the network's overall security and allows for secure remote management of the devices. Part 6 involves configuring IP addresses on various network devices, including switches, routers, servers, and workstations, as per the lab schematic and assigned IP addresses. This step is essential for enabling communication within the network. Configuring IP addresses correctly ensures that devices can communicate with each other seamlessly. Setting default gateways and enabling network adapters is crucial for proper network functionality. In Part 7, we test the SSH configurations by connecting to switches and routers using SSH from different PCs. This step ensures the SSH setup functions correctly, allowing for secure remote access to network devices. Connecting to various devices from different PCs helps verify the overall security and accessibility of the network.

## Preparation

To prepare for building the network topology, the following components had to be ready:

The current version of Packet Tracer

4 x PC PT Objects

2 x Cisco 2960 Layer 2 Switches

1 x Cisco 2811 Router (with NM-2FE2W module)

1 x PT Server (with web services enabled)

1 x PT Laptop

In preparation for configuring the network devices in Part 2, I needed to establish a console connection from my laptop to each network device. Before configuring the privileged mode password in Part 3, I ensured the terminal session was set up on my laptop to access each network device. I also ensured that the password "Secret55" was ready for configuration, as it would be used to secure privileged mode access on routers and switches.

To prepare for enforcing login requirements in Part 4, I ensured that I had an active terminal session from my laptop, allowing access to the console ports and virtual terminal ports on each network device. Again, I ensured the password "Secret55" was readily available for configuration, as it would be used to enforce login on both console and virtual terminal lines.

Moving on to Part 5 – Configuring Secure Shell - Preparation, I made sure I had the following elements in place:

Access to the network devices.

A terminal session on my laptop for configuration.

The hostname and domain name for each network device.

A username based on my initials and the last four digits of my student ID.

The password "Secret55" for the user account.

In Part 6 – Configuring IP Addresses - Preparation, I ensured that I had access to the following:

A terminal session on my laptop.

IP addresses are assigned as per the lab schematic.

Default gateway information for VLAN1 on switches.

IP address configuration details for the server and workstations.

The correct IP address information and default gateway settings were crucial for successful network communication in Part 6.

Lastly, in Part 7 – Connecting Using SSH - Preparation, I set up terminal sessions on relevant PCs (CS\_PC1, IT\_PC1, CS\_PC2, IT\_PC2) for SSH access to the switches and router. I also verified that the SSH configurations, including hostname, domain name, username, and RSA crypto key, were correctly implemented on the network devices. This ensured a smooth SSH connection process in Part 7.

## Observations

Part 1 – Building the Topology - Observations

During the process of building the network topology in Part 1, several observations were made:

The network devices (2 layers, two switches, and one router) were physically connected per the lab schematic, ensuring proper connectivity.

The assigned IP addresses and naming conventions were applied to the devices as specified in the lab document.

Each device's interfaces were verified to match the schematic, avoiding misconfigurations.

These observations ensured that the initial topology setup was completed accurately and aligned with the lab's requirements.

Part 2 – Configuring the Topology - Observations

While configuring the network devices in Part 2, the following observations were noted:

The Message of the Day (MOTD) banners were successfully configured on each network device with their respective names.

Testing the MOTD banners confirmed that they displayed the designated message as expected.

The running configurations were checked to verify the MOTD banner configuration.

Running configurations were saved to startup configurations for persistence.

These observations confirmed that the MOTD banners were correctly set up, enhancing security and identifying network devices.

Part 3 – Configuring the Privileged Mode Password - Observations

During the configuration of privileged mode passwords in Part 3, the following observations were made: Privileged mode passwords were configured successfully on each network device, requiring the password "Secret55" for access.

Testing the password authentication confirmed that the required password was effective.

The part of the running configuration displaying the privileged mode password configuration was examined.

Running configurations were saved to startup configurations to maintain the password settings.

These observations validated the implementation of privileged mode passwords, enhancing device security.

Part 4 – Enforcing Login - Observations

While enforcing login requirements in Part 4, the following observations were recorded:

Console lines were configured to enforce login with the password "Secret55," ensuring secure access to the console ports.

Synchronous logging was enabled on the console lines to record login activities.

Testing the login enforcement verified that users were prompted for a password.

The part of the running configuration displaying the console line configuration was reviewed.

Virtual terminal lines were configured to enforce login with the same password, "Secret55."

Passwords configured in clear text were encrypted for enhanced security.

Running configurations were saved to startup configurations for persistent settings.

These observations demonstrated successful login enforcement and enhanced security measures on the network devices.

Part 5 – Configuring Secure Shell - Observations

During the configuration of Secure Shell (SSH) in Part 5, the following observations were made:

Host names and domain names were configured as specified for each network device.

User accounts with usernames based on initials and the last four digits of student IDs were created using the password "Secret55."

RSA crypto keys with a 1024-bit modulus were generated successfully.

SSH version 2 was enabled on the network devices.

Virtual terminal lines were configured to allow both telnet and SSH access.

The relevant parts of the running configuration displaying SSH configurations were reviewed.

Running configurations were saved to startup configurations to retain SSH settings.

These observations ensured the successful implementation of SSH for secure remote access.

Part 6 – Configuring IP Addresses - Observations

During the configuration of IP addresses in Part 6, the following observations were noted:

IP addresses were configured on the VLAN1 virtual interfaces of each switch, allowing remote access via SSH.

Default gateways were set for VLAN1 on both switches to facilitate routing.

IP addresses on the router's network interfaces were configured according to the lab schematic.

The server's IP address was set per the lab schematic, and web server services were enabled.

IP addresses were configured on each PC as specified in the lab schematic.

Default gateways were set for the PCs, and network adapters on the server and workstations were enabled.

These observations confirmed that the IP address configurations were accurate and enabled successful network communication.

Part 7 – Connecting Using SSH - Observations

During the process of connecting using SSH in Part 7, the following observations were made:

SSH connections to the IT\_Switch and the Router were successfully established from CS\_PC1 and IT\_PC1.

SSH connections to the CS\_Switch and the Router were successfully established from CS\_PC2 and IT\_PC2.

SSH connections from each switch to the router were tested and proven successful.

SSH connections were established from IT\_Switch to CS\_Switch and vice versa.

These observations verified the successful SSH connectivity between network devices, ensuring secure remote management.

## Screenshots

A diagram of a network

Description automatically generated

Figure 1-1 displays the completed network topology per the lab schematic. It includes the connections of two-layer two switches, one router, a web server, and the required workstations. The topology reflects the assigned IP addresses and naming conventions.

A screenshot of a computer

Description automatically generated

Figure 1-2: This figure showcases the Message of the Day (MOTD) banner configuration on one of the network devices (e.g., R\_Waterloo\_as1234). It verifies the successful configuration of the MOTD message.

A screenshot of a computer

Description automatically generated

Figure 1-3: This figure captures the part of the running configuration that displays the MOTD banner configuration on one of the network devices. It provides evidence of the MOTD banner setup.

A computer screen shot of a black screen

Description automatically generated

Figure 1-4: This figure confirms the successful saving of the running configuration to the startup configuration on one of the network devices.

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Figure 1-4: This figure confirms the successful saving of the running configuration to the startup configuration on one of the network devices.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Figure 1-5: This figure demonstrates the configuration of the privileged mode password (Secret55) on one of the network devices.

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 1-6: This figure validates successfully testing the privileged mode password configuration on one of the network devices.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 1-7: This figure displays the part of the running configuration that shows the privileged mode password configuration on one of the network devices.

A black screen with white text

Description automatically generated

Figure 1-8: This figure confirms saving the running configuration to the startup configuration on one of the network devices.

Part4:

Router

**Enforce login before encryption**

A screenshot of a computer

Description automatically generated

Figure 1-9: This figure showcases the configuration of enforced login on one of the network devices, including the console and virtual terminal ports.

**A screen shot of a computer screen

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

Figure 1-10: This figure displays the part of the running configuration that shows the console line configuration on one of the network devices.

**After the encryption command, output and save the config**

**A computer screen shot of a black screen

Description automatically generated**

Figure 1-11: This figure exhibits the configuration of enforced login on one of the network devices.

A computer screen shot of a black screen

Description automatically generated

Switch 0:

**Enforce login before encryption**

A screenshot of a computer

Description automatically generated

Figure 1-12 confirms the return to global configuration mode on one of the network devices.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Figure 1-13: This figure shows the encryption of previously configured passwords in clear text on one of the network devices.

**After the encryption command, output and save the config**

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

Switch 1:

**Enforce login before encryption**

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Figure 1-14: This figure validates the successful saving of the running configuration to the startup configuration on one of the network devices.

A screen shot of a computer

Description automatically generated

**After the encryption command, output and save the config**

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

Part 5:

A screen shot of a computer

Description automatically generated

Figure 1-15: This figure displays the configuration of Secure Shell (SSH) on one of the network devices, including generating an RSA crypto key and enabling SSH version 2.

A screenshot of a computer program

Description automatically generated

Figure 1-16: This figure shows the configuration of virtual terminal lines to allow telnet and SSH on one of the network devices.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

Part 6:

Router:

A computer screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

Figure 1-17: Displays the IP configuration.

A screenshot of a computer program

Description automatically generated

Figure 1-18: Displays the IP configuration.

A screenshot of a computer

Description automatically generated

Figure 1-19: Displays the IP configuration.

A screenshot of a computer

Description automatically generated

Figure 1-20: Pinging various devices.

This figure exhibits three successful pings from IT\_PC1 to each IP address on the network, including the local layer two switches. It verifies network connectivity.

A computer screen shot of a program

Description automatically generated

Figure 1-21: This figure exhibits three successful pings from IT\_PC1 to each IP address on the network, including the local layer two switches. It verifies network connectivity.

A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure1-22:

This figure exhibits three successful pings from IT\_PC1 to each IP address on the network, including the local layer two switches. It verifies network connectivity.

A screenshot of a computer

Description automatically generated

Figure 1-23: This figure demonstrates successful access to the web page on the server from CS\_PC1.

Part 7:

1

a

A screenshot of a computer

Description automatically generated

Figure 1-24 shows the successful connection to the IT\_Switch and the Router via SSH from CS\_PC1 & IT\_PC1.

B

A computer screen shot of a computer program

Description automatically generated

C

A screenshot of a computer

Description automatically generated

D

A screenshot of a computer program

Description automatically generated

2

a

A screenshot of a computer program

Description automatically generated

B

A screenshot of a computer program

Description automatically generated

C

A screenshot of a computer program

Description automatically generated

Figure 1-25: This figure captures the successful connection to the CS\_Switch and the Router via SSH from CS\_PC2 & IT\_PC2.

D

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 1-26 confirms the successful connection to each switch from the router using SSH.

A screenshot of a computer

Description automatically generated

Figure 1-27: This figure displays the successful connection from IT\_Switch to the Waterloo Router using SSH.

A screenshot of a computer

Description automatically generated

Figure 1-27: This figure displays the successful connection from IT\_Switch to CS\_Switch using SSH.

A screenshot of a computer

Description automatically generated

Figure 1-28: This figure showcases the successful connection from CS\_Switch to IT\_Switch using SSH.

## Reflection

Part 1 – Building the Topology - Reflection

Reflecting on Part 1, building the network topology was a fundamental step in this lab. It allowed me to establish the physical connectivity of the network devices, ensuring they were interconnected correctly according to the lab schematic. This initial setup was crucial in preparing the network for configuration and testing.

One key takeaway from this section is the importance of attention to detail. Ensuring that the assigned IP addresses and naming conventions matched the lab documentation was critical to prevent any potential misconfigurations down the line. This experience reinforced the significance of meticulous planning and adherence to guidelines in network setup.

As I progress with the lab, completing Part 1 gives me confidence in the foundational aspects of network configuration, setting a solid base for the subsequent tasks.

Part 2 – Configuring the Topology - Reflection

In Part 2, configuring the network devices involved the implementation of Message of the Day (MOTD) banners on each device. This security measure serves as a visual indication of device identity and helps distinguish network devices during access.

The reflection on this section highlights the significance of MOTD banners as a security best practice. They enhance security and identify devices, especially in a network with multiple interconnected components. Testing the banner display and saving configurations reinforced the importance of persistence in device configurations.

Part 2 has provided valuable insights into implementing security measures within a network environment, setting the stage for more advanced configurations in subsequent sections.

Part 3 – Configuring the Privileged Mode Password - Reflection

Part 3 involved configuring privileged mode passwords for each network device. This added layer of security ensures that only authorized personnel can access and make changes to the device's privileged configuration mode.

Reflecting on this section, enforcing password requirements for privileged mode access is a fundamental security practice. Configuring the password "Secret55" and testing its functionality emphasized the importance of strong, unique passwords in network security. Additionally, observing the password configuration in the running configuration highlighted the need for administrators to review and maintain password settings regularly.

The successful implementation of privileged mode passwords in Part 3 contributes to a more secure network environment, laying the groundwork for additional security measures.

Part 4 – Enforcing Login – Reflection

Part 4 focused on enforcing login requirements for console and virtual terminal access to network devices. This step enhances security by ensuring users authenticate themselves before gaining access.

Reflecting on this section, it is evident that enforcing login requirements, including password authentication and synchronous logging, adds an essential layer of protection to network devices. Testing the login enforcement confirmed that unauthorized access attempts are thwarted, and the running configurations provided insights into how these settings are configured.

Encrypting previously configured passwords in clear text further strengthens security and safeguards sensitive information. This section reinforced the principle that robust security measures should be in place at every level of network access.

Part 5 – Configuring Secure Shell - Reflection

Part 5 involved configuring Secure Shell (SSH) for secure remote access to network devices. SSH is a critical component of network security, and its proper configuration is essential.

Reflecting on this section, configuring SSH demonstrated the importance of secure remote management. Creating user accounts with strong passwords and generating RSA crypto keys ensures encrypted communication, enhancing network security. Enabling SSH version 2 and configuring virtual terminal lines to allow telnet and SSH access further expanded the secure access options.

The successful setup of SSH is a significant milestone in securing the network, allowing for remote management while maintaining the highest standards of security.

Part 6 – Configuring IP Addresses - Reflection

In Part 6, configuring IP addresses on network devices and workstations was a crucial step in establishing connectivity within the network.

Reflecting on this section, setting IP addresses default gateways and ensuring network adapters were enabled on PCs and servers were fundamental tasks. These configurations lay the foundation for successful communication within the network.

This section reinforced the importance of IP addressing and proper network configuration, as misconfiguration could disrupt network connectivity. It also highlighted the significance of testing connectivity through ping tests and web page access, ensuring that devices could communicate effectively.

Part 7 – Connecting Using SSH - Reflection

Part 7 involved testing SSH connectivity between network devices, including switches and the router, to ensure secure remote management. Reflecting on this section, successfully establishing SSH connections between devices demonstrates the effective implementation of secure access methods. It reaffirmed the importance of SSH as a secure remote management protocol and validated that the configured settings were functioning as intended.

Furthermore, connecting between switches using SSH highlighted the interconnectivity of network devices and the seamless communication established within the network.

In conclusion, each part of this lab has contributed to enhancing network security and configuration skills. As I progress in my network security journey, the experiences and knowledge gained in this lab will serve as a valuable foundation for more complex network security tasks and challenges.

# Lab 2 – Static Routing

# Parts

## Description

The initial phase involved building the network's physical foundation. This encompassed creating physical connections between network devices and assigning IP addresses in alignment with the schematic. Ensuring the accuracy of the schematic's representation of the assigned IPs was crucial for proper network functionality.

Following the physical setup, we moved on to configuring the network devices. Our key focus was establishing console connections and implementing Message of the Day (MOTD) banners. These banners were designed to display device names, enhancing personalization and aiding in the swift identification of network components. Beyond aesthetics, this step also contributed to network security.

Security remained paramount as we configured privileged mode passwords for all network devices. The unified implementation of the "Secret55" privileged mode password added a layer of protection, guarding against unauthorized access to privileged modes.

Further fortifying security, we enforced login requirements for both console and virtual terminal ports. Console lines were configured to mandate login using the "Secret55" password, and synchronous logging was enabled to monitor login activities closely. Simultaneously, virtual terminal lines enforced login with the same password, creating a robust security framework against unauthorized access attempts.

In the pursuit of secure remote management, we implemented Secure Shell (SSH) for network devices. This encompassed configuring hostnames and domain names, creating user accounts, generating RSA crypto keys, and enabling SSH version 2. These measures established a secure channel for remote management, effectively safeguarding the network.

With security measures in place, we focused on configuring IP addresses. Each IP address was meticulously configured following the lab schematic, covering VLAN1 on the switch, network interfaces on routers, the Server, and individual PCs. This meticulous IP address configuration ensured seamless network communication and routing.

In the final phase, we set up static routes to facilitate efficient routing within the network topology. This involved configuring default static routes and routing on R\_Kitchener to ensure uninterrupted connectivity between workstations and the server.

## Preparation

Before I dive into constructing the network topology, gathering all the hardware and devices listed in the lab instructions is imperative. This includes the Cisco 2960 Switch, Cisco 3750 Switch, Cisco 2811 Router, PC PT Objects, PT Server with web services enabled, and PT Laptop. Additionally, it is essential to ensure that all passwords are uniformly set to "Secret55" to maintain consistency and bolster security throughout the lab.

As I prepare for this part, the primary focus is on setting up access to the console of each network device.

Before configuring the privileged mode password, I must confirm that I have console access to each network device. This access is a prerequisite for making the necessary changes to the configurations of these devices.

Like Part 3, console access to the network devices is paramount for this segment. It is imperative to ensure that I have a means of connecting to the console ports of each device, as this will be crucial for enforcing login requirements.

I needed to gather the essential information, such as the hostname, domain name, and student ID, as these details will be utilized in creating the user account required for SSH configuration.

Before configuring IP addresses, I needed to review the lab schematic thoroughly. This will provide me with a clear understanding of how IP addresses are assigned to different devices within the network. Ensuring I have access to console connections for configuration purposes is also crucial.

To effectively configure static routes, I needed to ensure that I had access to the network devices' console. A comprehensive review of the lab schematic is necessary to grasp the routing requirements and the configuration of default static routes.

## Observations

Part 1 - Building the Topology

Observations:

In this part, I physically connected the network devices as per the lab schematic provided in Figure 1-1. This included connecting the Cisco 2960 Switch, Cisco 3750 Switch, and Cisco 2811 Routers. I added 2 PC PT Objects, 1 PT Server, and 1 PT Laptop to the topology.

The lab schematic accurately reflects each device's assigned IP addresses and naming conventions. I included my initials and the last four digits of my student ID as unique identifiers for all objects and resources created.

Part 2 – Configuring the Topology

Observations:

For this part, I connected to the console of each network device using the laptop. Once connected, I configured a Message of the Day (MOTD) banner to display a custom message on each device.

The MOTD banners were successfully configured, and I verified that they were displayed upon logging in to each device. I also reviewed the running configuration to ensure the banner configuration was correctly applied.

Part 3 – Configuring the Privileged Mode Password

Observations:

In this part, I used a console connection to configure each network device to require a privileged mode password for access. The password "Secret55" was the privileged mode password for security purposes.

I tested the password to ensure it worked correctly by attempting to access privileged mode on each device. Additionally, I reviewed the running configuration of each device to confirm that the privileged mode password configuration was in place.

Part 4 – Enforcing Login

Observations:

I enforced login requirements for each network device's console and virtual terminal ports using a console connection. This involved configuring the console line to force login with the password of "Secret55" and enabling synchronous logging. I also configured the virtual terminal lines to require login with the same password.

I thoroughly tested the login enforcement by attempting to access the console and virtual terminal ports. Successful login enforcement was observed. The configuration of the console and virtual terminal lines was reviewed in the running configuration.

Part 5 – Configuring Secure Shell

Observations:

I configured Secure Shell (SSH) on each network device for this part to enable secure remote access. This included setting up the hostname and domain name, creating a user account based on my initials and student ID (e.g., as-1234), and configuring an RSA crypto key with a 1024-bit modulus. SSH version 2 was enabled, and virtual terminal lines were configured to allow telnet and SSH.

I verified that the crypto key was generated correctly and checked the running configuration to ensure the SSH configuration was applied.

Part 6 – Configuring IP Addresses

Observations:

In this part, I configured IP addresses on the network devices based on the lab schematic. I used console connections through the assigned access server to configure IP addresses on the VLAN1 virtual interface of the Cisco 2960 switch, network interfaces on the Cisco 2811 routers, and the Server and PCs.

I tested the initial configuration by ensuring that each workstation could ping its default gateway and the IP address on the other interface of its site router. Per the lab requirements, I also confirmed that workstations could not ping beyond the site router.

Part 7 – Configuring Static Routes

Observations:

I configured static routes in this part to enable proper routing within the network topology. Default static routes were configured on R\_Waterloo and R\_Stratford, using R\_Kitchener as the gateway of last resort. Static routes were also set on R\_Kitchener to route to both remote site LAN networks.

I conducted tests to ensure that workstations could ping the server and that the server could ping each workstation. Additionally, I verified that each workstation could access the custom website on the Server Object.

## Screenshots

A diagram of a computer network

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

Figure 2-1: Console Routing Table (Router R\_Waterloo)

Description: Figure 2-1 shows the console output of Router R\_Waterloo, displaying the routing table highlighting the applicable routing information.

A computer screen shot of a black screen

Description automatically generated

Figure 2-2: Console Routing Table (Router R\_Stratford)

Description: Figure 2-2 displays the console output of Router R\_Stratford, presenting the routing table with relevant routing information highlighted.

A computer screen shot of a black screen

Description automatically generated

Figure 2-3: Console Routing Table (Router R\_Kitchener)

Description: Figure 2-3 exhibits the console output of Router R\_Kitchener, showcasing the routing table and emphasizing the pertinent routing details.

A screenshot of a computer

Description automatically generated

Figure 2-4: Successful Pings from Workstations to Server (Workstation 1)

Description: Figure 2-4 captures three successful ping commands from Workstation 1 to the Server using the command line interface, confirming network connectivity.

A computer screen shot of a black screen

Description automatically generated

Figure 2-5: Successful Pings from Workstations to Server (Workstation 2)

Description: Figure 2-5 displays three successful ping commands executed from Workstation 2 to the Server through the command line interface, verifying network connectivity.

A computer screen shot of a black screen

Description automatically generated

Figure 2-7: Successful Pings from Server to Workstation (Server)

Description: Figure 2-7 exhibits three successful ping commands executed from the Server to a Workstation using the command line interface, validating bidirectional network connectivity.

**A screenshot of a computer

Description automatically generated**

Figure 2-8: Accessing Custom Website (Workstation 1)

Description: Figure 2-8 shows Workstation 1 successfully accessing the custom website hosted on the server object, demonstrating web service availability.

**A screenshot of a computer

Description automatically generated**

Figure 2-9: Accessing Custom Website (Workstation 2)

Description: Figure 2-9 demonstrates Workstation 2 accessing the custom website hosted on the server object, indicating the availability of web services.

**A computer screen shot of a black screen

Description automatically generated**

Figure 2-10: SSH Access from PC1 to Router R\_Waterloo

Description: Figure 2-10 proves successful SSH access from PC1 to Router R\_Waterloo, validating remote access to the network device.

**A screenshot of a computer

Description automatically generated**

Figure 2-11: SSH Access from PC1 to Router R\_Stratford

Description: Figure 2-11 displays successful SSH access from PC1 to Router R\_Stratford, confirming remote connectivity to the network device.

**A screenshot of a computer

Description automatically generated**

Figure 2-12: SSH Access from PC1 to Router R\_Kitchener

Description: Figure 2-12 showcases successful SSH access from PC1 to Router R\_Kitchener, verifying remote connectivity to the network device.

**A computer screen shot of a black screen

Description automatically generated**

Figure 2-13: SSH Access from PC1 to CS\_SW\_YP9578(Switch)

Description: Figure 2-13 showcases successful SSH access from PC1 to CS\_SW\_YP9578(Switch), verifying remote connectivity to the network device.

## Reflection

Building the network topology according to the lab schematic was a crucial initial step. It ensured that the physical connections and layout of devices matched the intended design. This part helped me understand the importance of careful planning and attention to detail in network deployment. Including my initials and student ID in object naming conventions is a valuable practice for identifying resources in a complex network.

Configuring the Message of the Day (MOTD) banners on each network device was straightforward. It highlighted the importance of providing informational messages to users, such as login reminders or contact information for support. This step also emphasized the consistency of configuration across various devices in the network, making it easier to manage and troubleshoot.

Setting up a privileged mode password adds an essential layer of security to network devices. It ensures that only authorized personnel can access the highest level of device configuration. The choice of "Secret55" as the password is a reasonable practice, but it is vital to consider more complex passwords for real-world scenarios. Testing the password functionality reassured me about the device's security settings.

Enforcing login requirements on both console and virtual terminal ports is crucial for network security. It ensures that only authorized users can access network devices remotely. Configuring synchronous logging also helps monitor and troubleshoot. This part of the lab reinforced the importance of securing access to network devices and maintaining consistent security practices across all devices.

Enabling Secure Shell (SSH) for remote access is a best practice for securing network devices. It provides encryption and authentication, enhancing overall network security. Generating an RSA crypto key and configuring SSH was educational and a valuable skill for network administrators. Remembering to turn off weaker protocols like telnet to prevent security vulnerabilities is essential.

Configuring IP addresses is a fundamental task in network setup. It is the foundation for communication between devices. Subnetting the single IP address into four separate networks using /29 CIDR notation was practical. It helped me understand how subnetting works and how to allocate IP addresses efficiently. Testing the initial configuration and ensuring proper communication between workstations and routers validated the correctness of the IP addressing scheme.

Configuring static routes is essential for proper routing within a network. It allows devices to forward traffic to the correct destinations. Setting up default static routes and routes to remote LAN networks was critical in this lab. Testing the routing functionality by verifying ping connectivity between workstations and servers ensured the routing configuration was accurate. This part emphasized the importance of routing in network connectivity.

Completing this lab provided valuable hands-on experience in network configuration and security practices. It reinforced the significance of careful planning, consistency, and security in network deployments. Subnetting, password management, and routing configuration are essential skills for any network administrator.

# References

1. Odom, W. (n.d.). *CCENT/CCNA ICND1 100-105 Official Certification Guide, First Edition*. O’Reilly Online Learning. https://www.oreilly.com/library/view/ccentccna-icnd1-100-105/9780134440903/ch18.html#ch18
2. J. D. (2017, December 6). *Cisco IOS Configuring Static Routing*. YouTube. https://www.youtube.com/watch?v=9P\_FLYXnnGQ
3. J. D. (2017, September 23). *Cisco IOS Configuring Hostname And Domain Name*. YouTube. https://www.youtube.com/watch?v=FD\_8OrMwge4
4. J. D. (2017, September 23). *Cisco IOS Privileged Password Configuration*. YouTube. https://www.youtube.com/watch?v=K7ifKkz8wro
5. J. D. (2017, September 23). *Securing Cisco IOS Console*. YouTube. https://www.youtube.com/watch?v=toMLW6vArF4
6. J. D. (2017, September 23). *Cisco IOS Interface IP Configuration*. YouTube. https://www.youtube.com/watch?v=fGWxolRO3i8
7. J. D. (2017, September 23). *Cisco IOS Enabling SSH Access*. YouTube. https://www.youtube.com/watch?v=nACQKjCW5BY