INFO8490 Lab 1 - Simple Network Topology

Overview

This Lab will be recorded in your lab book and requires you to create a simple network topology. You will configure two layer 2 switches and 1 router as well as a webserver and necessary workstations. This Lab will be similar to the exercises that you completed in the Network Security Fundamentals module in the course shell. You will gain practical experience configuring hosts, routers and switches on a network.

Read through the entire lab first so that you completely understand what you are trying to achieve and create a basic plan. This will likely save you problems and having to repeat work later on. Also, be sure to fully review the rubric for this lab.

Please note that this Lab is an individual activity you will not be sharing your network devices or work.

Preparation

You will need:

- Current version of Packet tracer
- 4 x PC PT Objects
- 2 x Cisco 2960 Layer 2 Switches
- 1 x Cisco 2811 Router (Be sure to add NM-2FE2W module to the Router)
- 1 x PT Server (web services enabled)
- 1 x PT Laptop

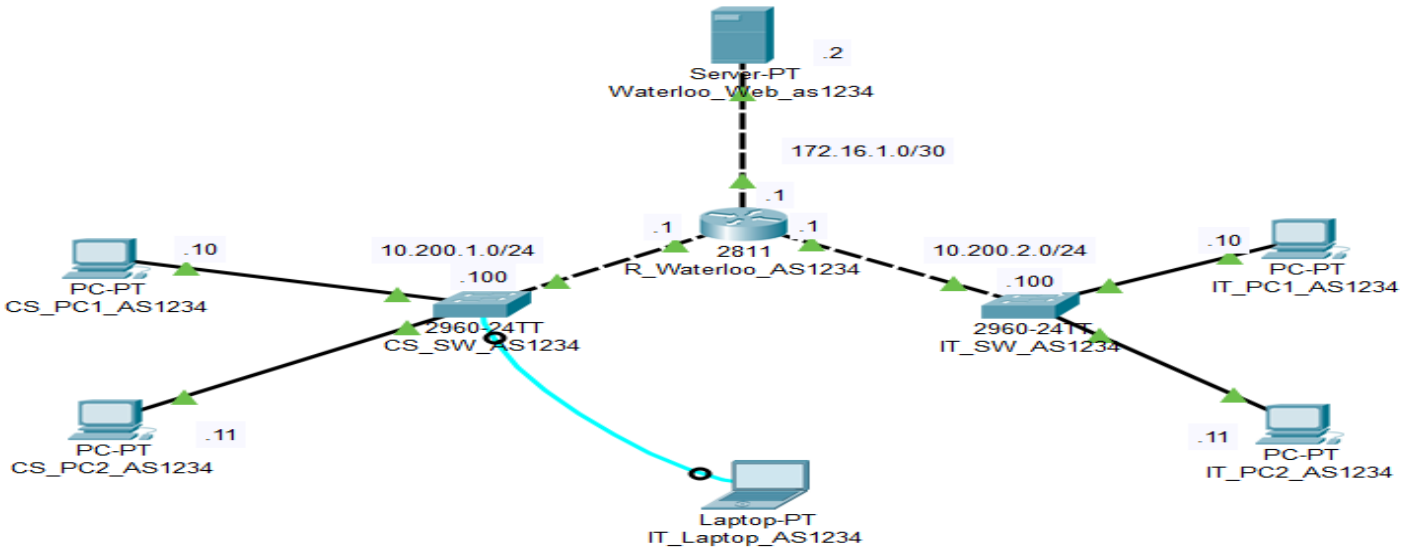
Your IP addresses will be assigned as per the file named INFO8490-20F-Portfolio-1-Subnets included in the assessment portal. The assigned numbers reflect the IP address that you will use on each network including the WAN connections.

Remember that as IT practitioners we will encounter many unknown variables in our day to day activities. Part of our learning is the requirement to be able to analyze, research and resolve problems or environments that are unfamiliar to us. As a graduate student it is your responsibility to apply the necessary problem-solving techniques before reaching out for assistance. If you do reach out for assistance be sure that are able to provide detailed evidence on how you have attempted to resolve the issue on your own.

Lab Schematic

(this is only an example)

Figure 1-1 Simple Network Topology



Description

In your own words, provide a description of the expected goals and results as you understand them.

Part 1 – Building the Topology

You will initially build out and configure your network topology as per lab schematic Figure 1-1. Completing this section will result in a topology that will be ready to configure. Make sure that the schematic that you include in your lab book reflects your assigned IP's and required naming conventions.

Part 2 – Configuring the Topology

Start by configuring the network devices as per the following steps:

Connect to each network device using a console connection from the Laptop (You will not need to set an IP address on the Laptop)

On each network device, configure a Message of the Day (MOTD) banner. Configuring a MOTD banner on a router is the same as configuring on a switch.

1. Configure the message of the day to state This is the motd for <name>where name is the name of your network device (eg. R_Waterloo_as1234).
2. Test to ensure the banner is displayed.
3. Display the part of the running config that shows the banner configuration.
4. Save the running config to startup config.

Screenshots

Provide a screenshot for showing the MOTD for each network device.

Part 3 – Configuring the Privileged Mode Password

From a terminal session on the laptop, configure each network device such that changing to privileged mode requires a password. Configuring a privileged mode password on a router is the same as a switch.

1. Configure the privileged mode password to Secret55.
2. Test to ensure the password works.
3. Display the part of the running config that shows the privileged mode password configuration.
4. Save the running config to startup config.

Screenshots

Provide a screenshot for showing the privilege password mode works for each network device.

Part 4 – Enforcing Login

Using a terminal session from the laptop, configure connections to the console port and virtual terminal ports on each network device such that the user must log in. Enforcing login on a router is the same as a switch.

1. Configure the console line to force login with a password of Secret55.
2. Configure synchronous logging on the console line.
3. Test to ensure that the login enforcement works.
4. Display the part of the running config that shows the console line configuration.
5. Configure the virtual terminal lines to force login with a password of Secret55.
6. Display the part of the running config that shows the virtual terminal configuration.
7. Return to the global config mode.
8. Encrypt the previously configured passwords that are in clear text.
9. Save the running config to startup config.

Screenshots

Provide a screenshot for each network device showing enforced login.

Part 5 – Configuring Secure Shell

Using a terminal session on the laptop, configure secure shell on each network device to be used for remote access. Configuring ssh on a router is the same as a switch.

1. Configure the hostname and domain name if you have not already done so.
2. Create a user with username based on your initials and last 4 digits of your student ID (e.g. as-1234) and password
   Secret55.
3. Generate an RSA crypto key with a 1024 bit modulus.
4. Display your crypto key to ensure it was generated correctly.
5. Enable ssh version 2.

6. Configure the virtual terminal lines to allow both telnet and ssh.
7. Display the parts of running config to show what you configured.
8. Save the running config to startup config.

Screenshots

Provide a screenshot for each network device showing the above steps.

Part 6 – Configuring IP Addresses

On the switches:

From a terminal session on the laptop, configure the IP on the VLAN1 virtual interface of each switch so that you can connect remotely with ssh. Remember that the switches are layer 2 devices. Don't forget to set the default gateway for VLan 1 on each of the switches.

On the router:

From a terminal session on the Laptop, configure IP's on the network interfaces as per the lab schematic using the IP addresses assigned.

On the Server:

Configure the IP address as per the lab schematic using the IP's assigned in Appendix A.

Make sure the Web server service is enabled on the Server.

On each PC:

Configure the IP address as per the lab schematic using the IP's assigned in Appendix A.

*Don't forget to set default gateways and make sure the network adapter on the server and workstations are turned on.

Save the running config to startup config

Screenshots

Provide screenshots showing 3 successful pings from IT_PC1 to each IP on the network, including the local layer 2 switch (Should be a total of 9 IP addresses x 3 pings each)

If any of the pings are not successful, fix the problem prior to proceeding.

Provide a screenshot from CS_PC1 showing successful access to the web page on the server.

NOTICE THAT WE ARE NO LONGER USING THE LAPTOP

Part 7 – Connecting Using and ssh

In this task, you test connecting to your switches and router using ssh. Connecting to a router using ssh is the same as a switch.

1. Connect to the IT_Switch and the Router via ssh from CS_PC1 & IT_PC1
2. Connect to the CS_Switch and the Router via ssh from CS_PC2 & IT_PC2
3. Connect to each switch from your router using ssh.
4. Connect from IT_Switch to CS_Switch using SSH
5. Connect from CS_Switch to IT_Switch using SSH

Screenshots

Include screenshots (as described above) of each step 1-5 successfully connecting to each of the switches and the router using SSH

Include screenshots connecting to each of the switches from the router using SSH.

Observations and Reflection

Write down your observations and reflections including details on any problems encountered or solved.

Wrap Up

Make sure you save and backup your configuration.