**Portfolio 1**

**Faysal Ahmed**

**8696528**

**INFO8490**

**Allen Savard**

**Oct 6, 2020**

# Table of Contents

[Table of Contents 2](#_Toc52906305)

[Lab 1 - Simple Network 3](#_Toc52906306)

[Part 1 3](#_Toc52906307)

[Description 3](#_Toc52906308)

[Preparation 3](#_Toc52906309)

[Observations 3](#_Toc52906310)

[Screenshots 5](#_Toc52906311)

[Reflection 21](#_Toc52906312)

[Lab 2 - Static Routing 23](#_Toc52906313)

[Part 1 23](#_Toc52906314)

[Description 23](#_Toc52906315)

[Preparation 23](#_Toc52906316)

[Observations 23](#_Toc52906317)

[Screenshots 25](#_Toc52906318)

[Reflection 33](#_Toc52906319)

# Lab 1 - Simple Network

# Part 1

## Description

In this lab a simple network topology was created with the following components:

1. 4 x PC PT Objects
2. 2 x Cisco 2960 Layer 2 Switches
3. 1 x Cisco 2811 Router
4. 1 x PT Server
5. 1 x PT Laptop

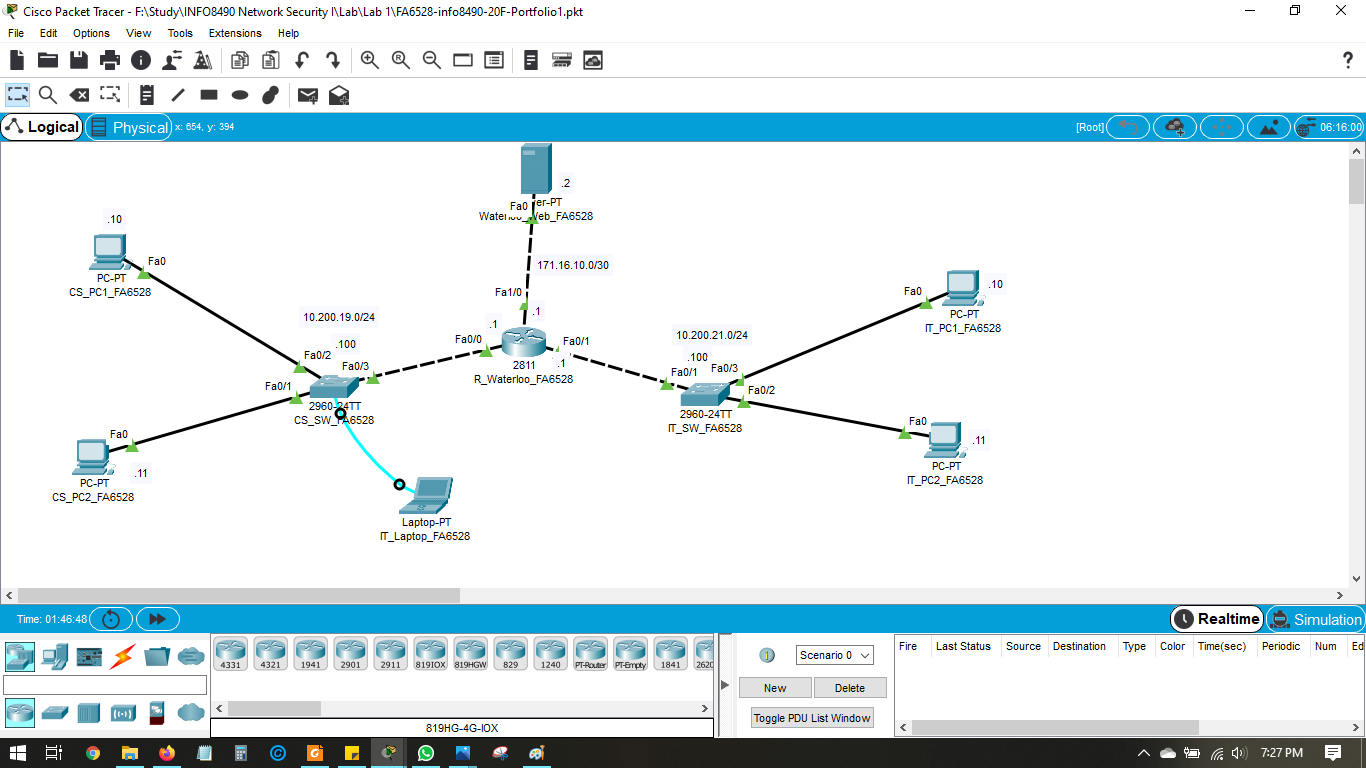
This topology is created to learn configuring network switch & router. Also to learn how to secure the networking device & how to access them remotely. Password encryption was also a part of ensuring security to the network devices.

## Preparation

Prior to configuring the network topology each network device were checked to see if there is extra module needed & the modules were added accordingly. Then we made sure that each device is connected by specified connections such as copper straight-trough & copper cross-over cable. Then we made sure the network devices are turned on to configure them.

## Observations

At first, network topology was created (Figure 1-1) as per the lab schematics. Then the massage of the day was created for each network devices by using “banner motd” command. It was then tested to check if the massage appears as the massage of the day.



**Figure 1-1 Lab 1 Network Topology**

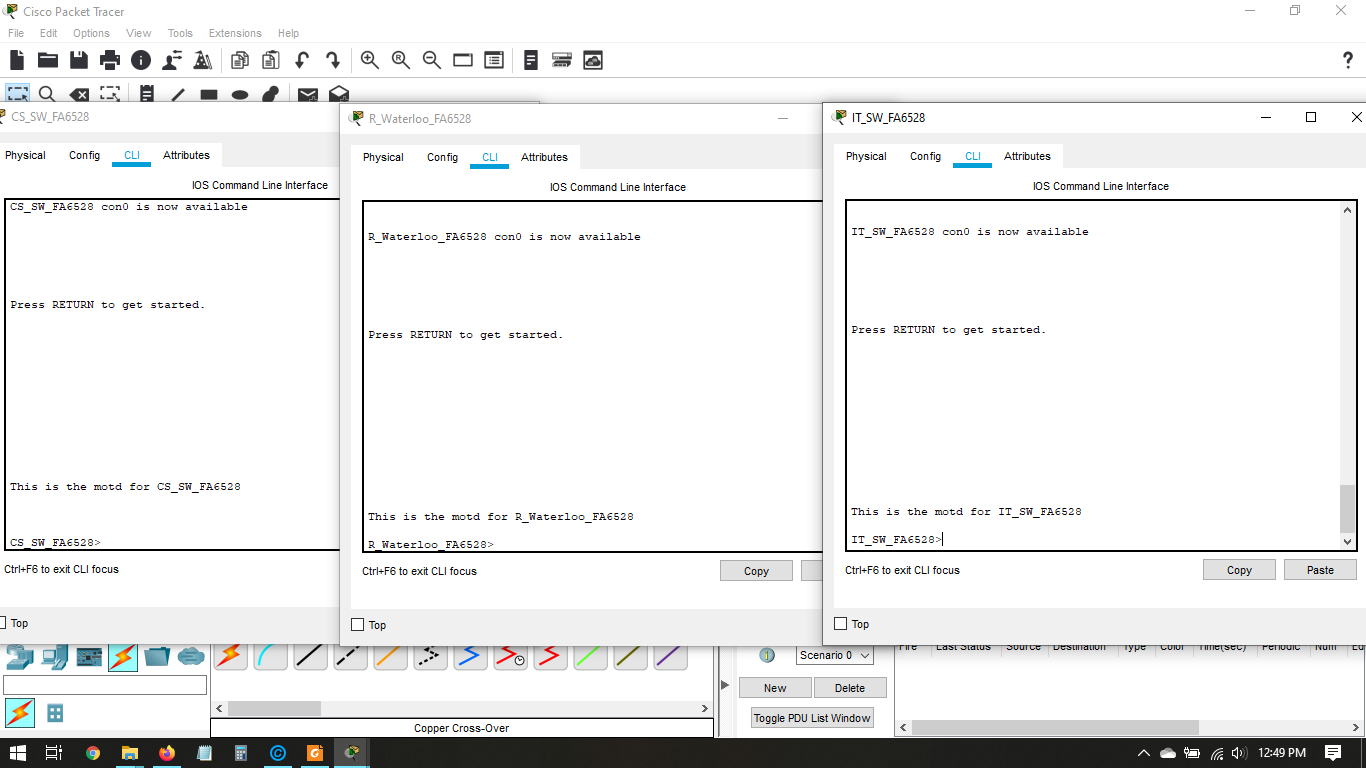
Secondly, password was created for privileged mode to Secret55 & ensured it works. Then line console & virtual line terminal was configured to force login with the password Secret55. Synchronous logging was configured. After testing login enforcement works, passwords were encrypted.

Hostname was created as per device name given in the lab & domain name was to set to google.com. Username & password was set to FA6528 & Secret55 respectively for users who can access the network device remotely. Crypto key RSA was generated with 1024 bit modulus ssh version 2 was enabled.   
  
Afterwards, from a terminal session on the laptop, the IP on the VLAN1 virtual interface of each switch were configured so that users can connect remotely with ssh. Also the default gateway for the switch was configured. Then for each interface of the router ip was set & the link between the network devices was to set to state up from state down. For server & all the pc ip, subnet mask & the gateway ip was assigned manually.

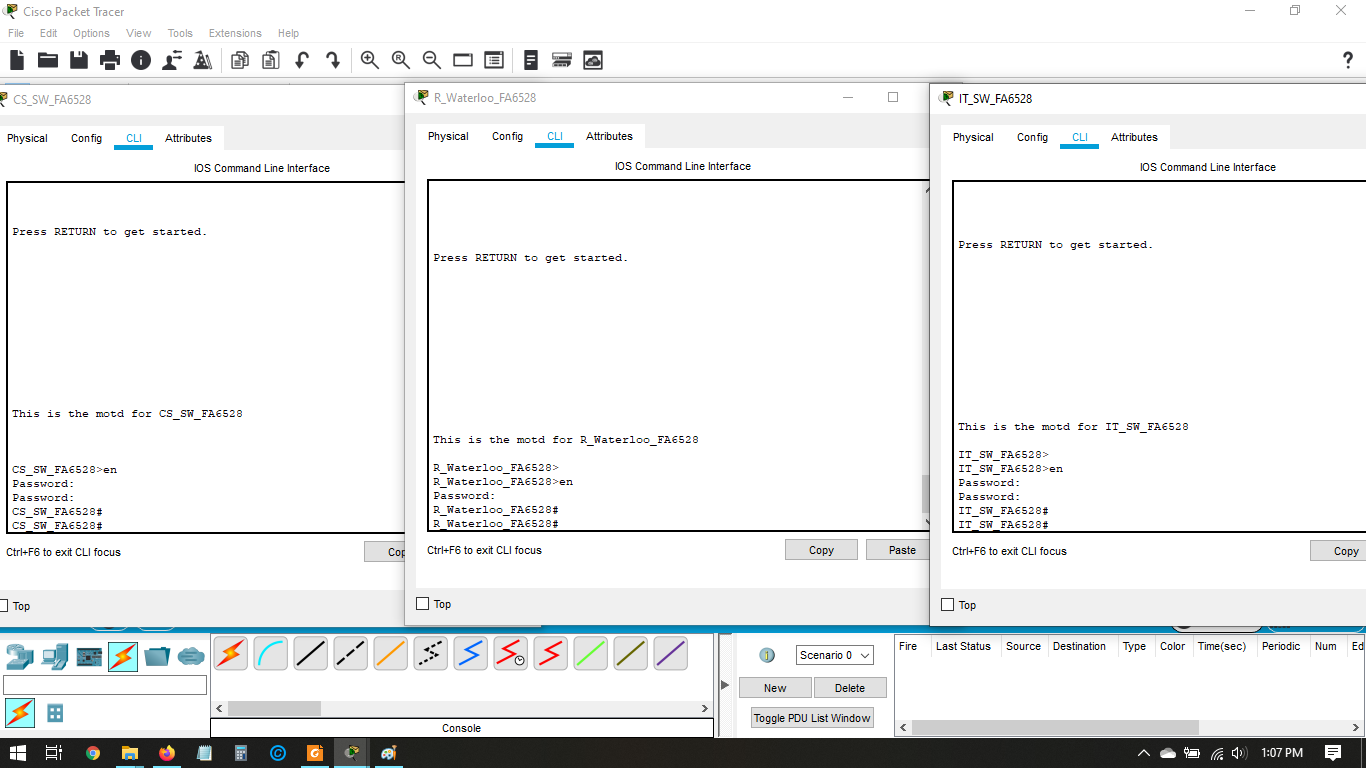
After each step, running config was saved to startup config before starting next step.

Via ssh –l command we were able to connect to IT\_Switch from CS\_PC1 & IT\_PC1. We followed the same command to connect CS\_Switch from CS\_PC2 & IT\_PC2 & also from router to each switch. Then we connected from IT\_Switch to CS\_Switch & vice versa using the same ssh –l command.

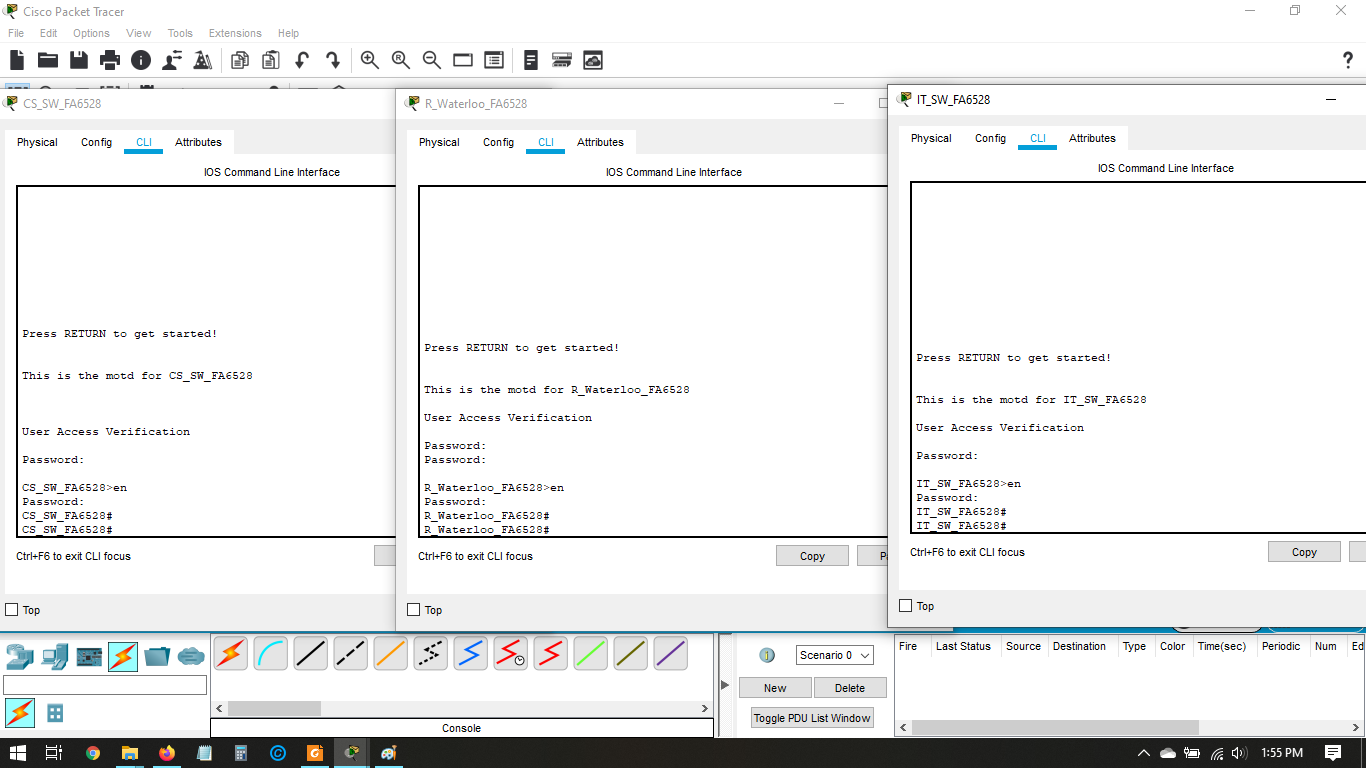
## Screenshots



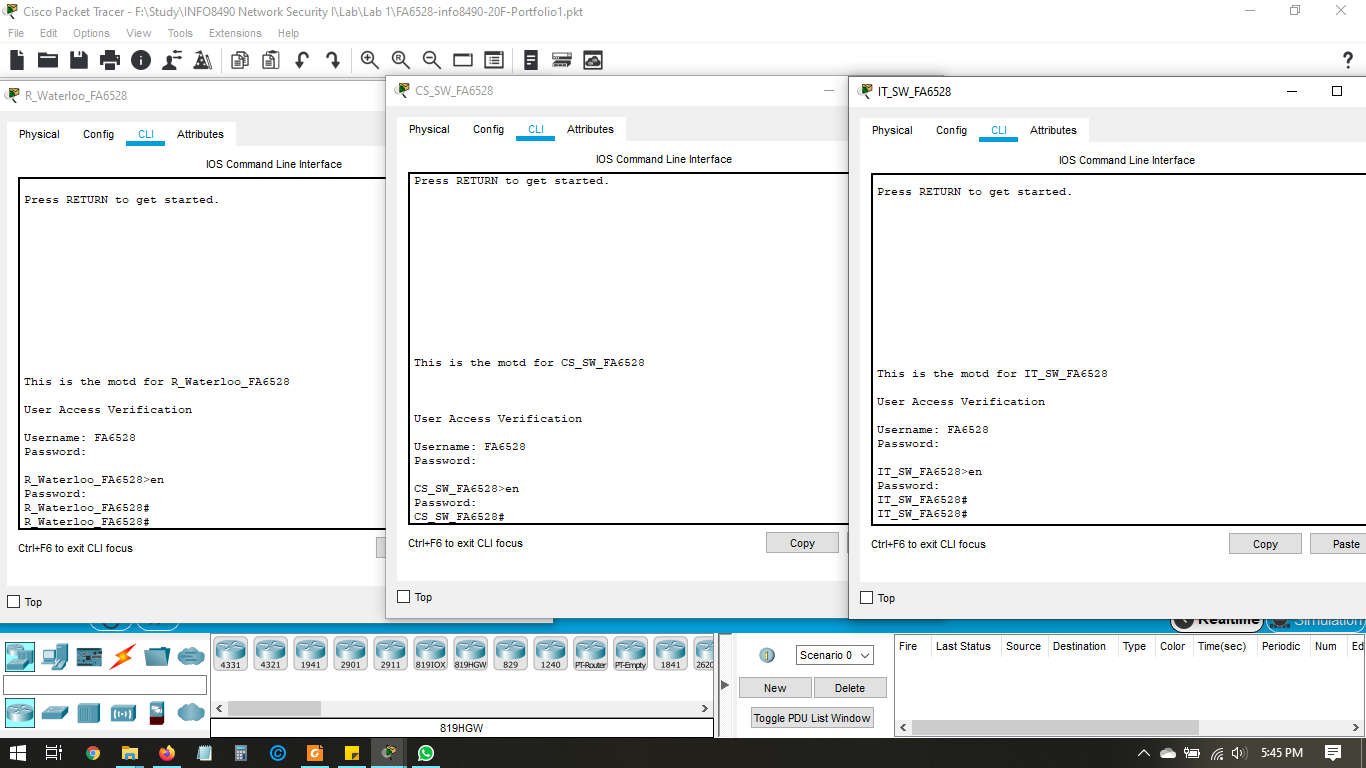
**Figure 1-2 MOTD Banner is displayed in each network device.**



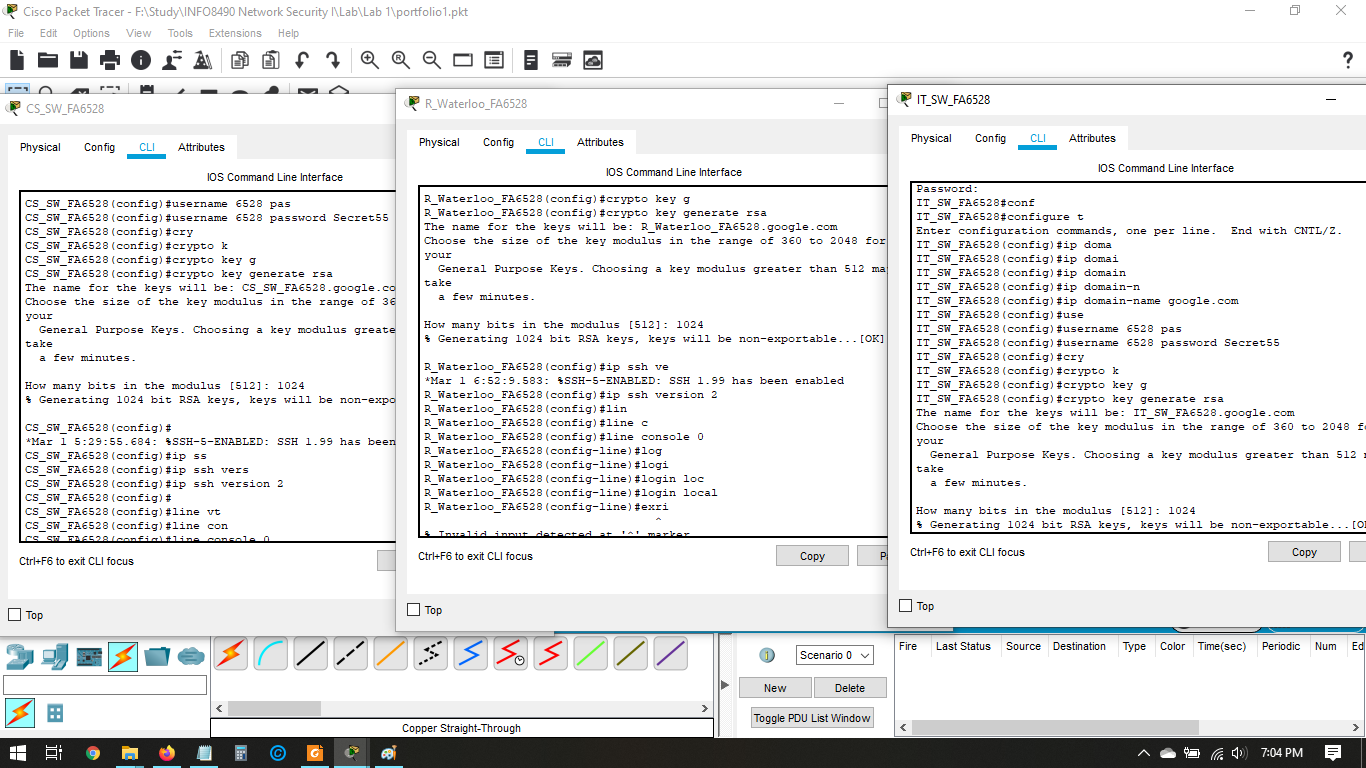
**Figure 1-3 Privilege Password Mode**



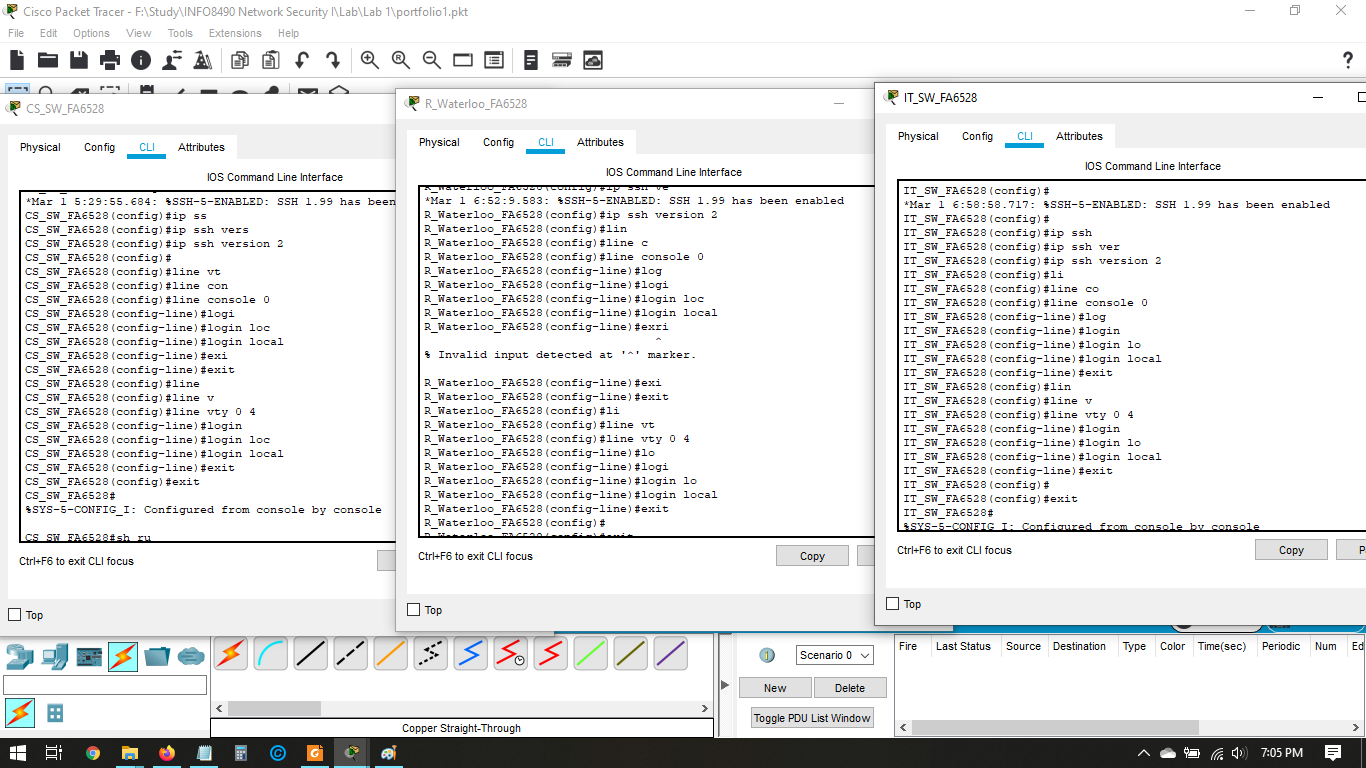
**Figure 1-4 Enforce Login**



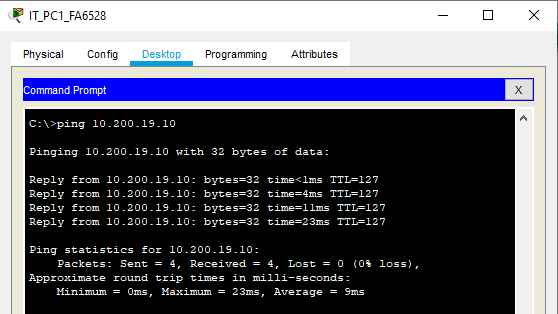
**Figure 1-5 Username & Password**



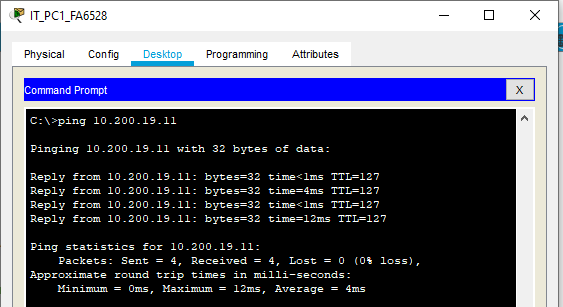
**Figure 1-6 Configuration of Crypto Key RSA**



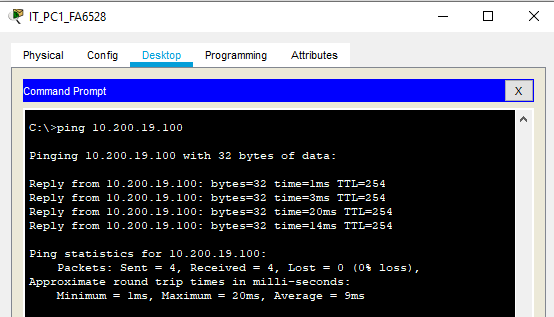
**Figure 1-7 Configuring ssh version 2**

****

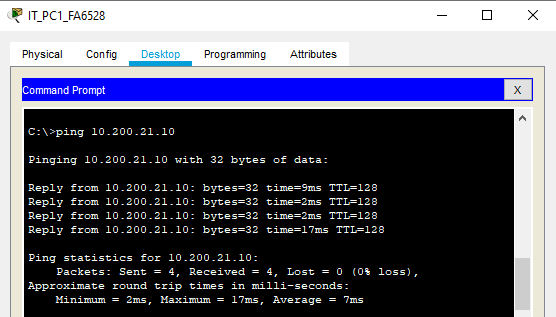
**Figure 1-8 Pinging from IT\_PC1 to CS\_PC1**

****

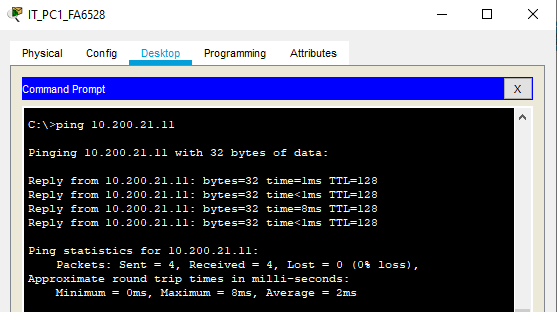
**Figure 1-9 Pinging from IT\_PC1 to CS\_PC2**

****

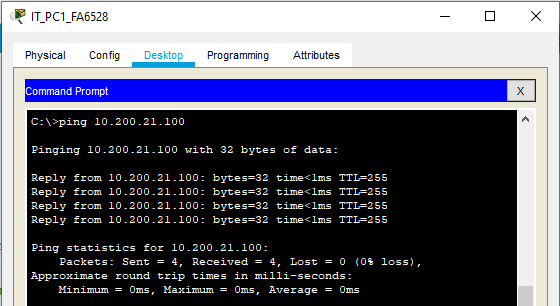
**Figure 1-10 Pinging from IT\_PC1 to CS\_SW**

****

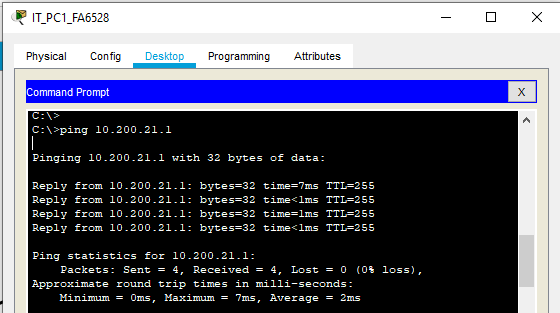
**Figure 1-11 Pinging from IT\_PC1 to CS\_PC1**

****

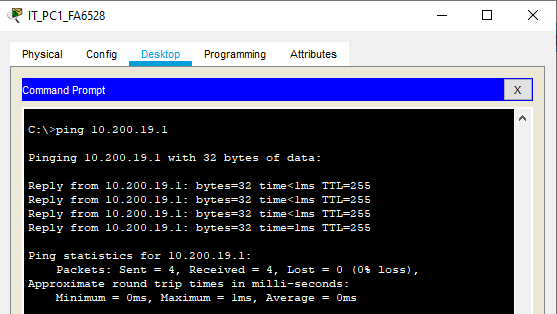
**Figure 1-12 Pinging from IT\_PC1 to CS\_PC2**

****

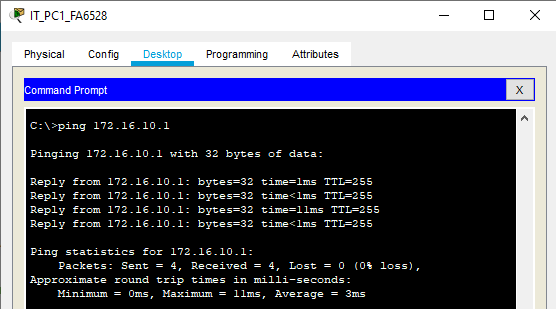
**Figure 1-13 Pinging from IT\_PC1 to IT\_SW**

****

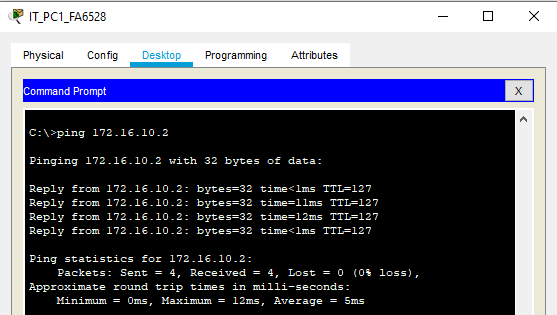
**Figure 1-14 Pinging from IT\_PC1 to R\_Waterloo Fa0/1 port**

****

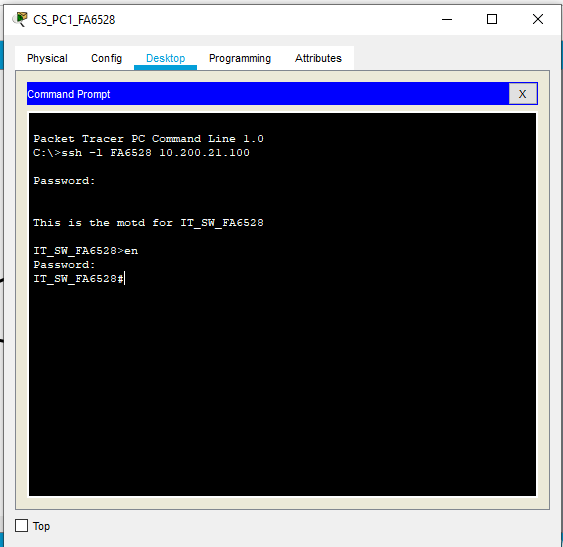
**Figure 1-15 Pinging from IT\_PC1 to R\_Waterloo Fa0/0 port**

****

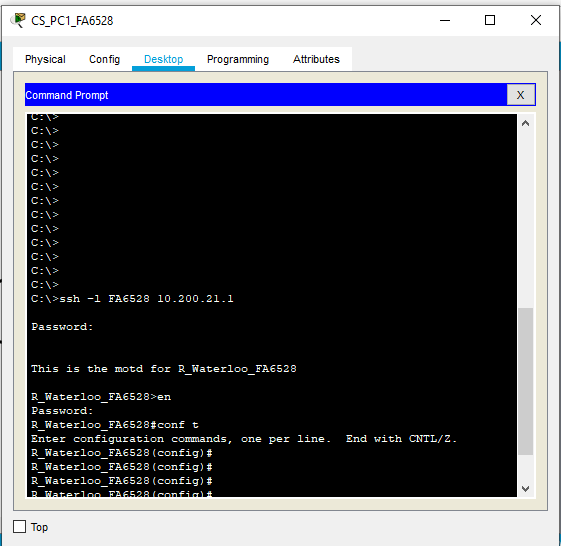
**Figure 1-16 Pinging from IT\_PC1 to R\_Waterloo Fa1/0 port**

****

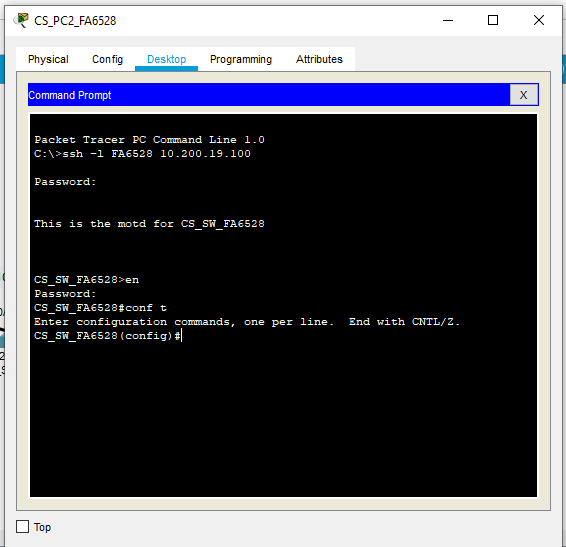
**Figure 1-17 Pinging from IT\_PC1 to Web Server**



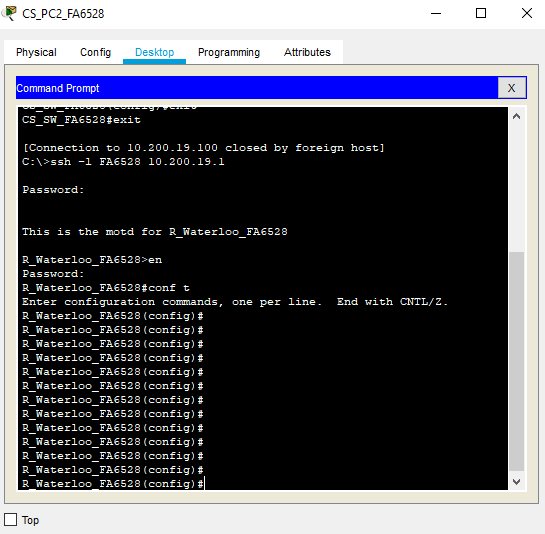
**Figure 1-18 Accessing IT\_SW from CS\_PC1**



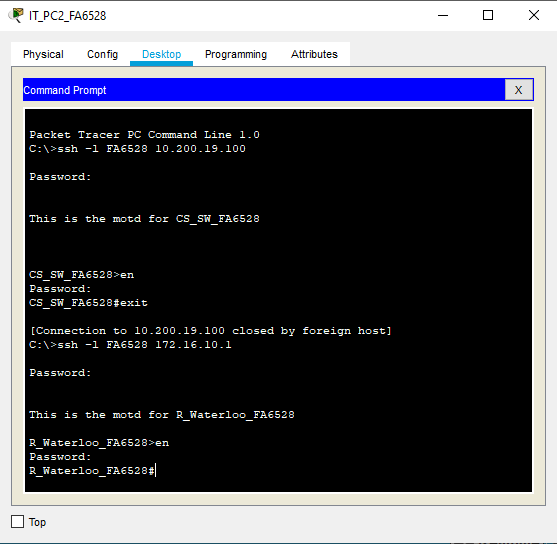
**Figure 1-19 Accessing R\_Waterloo from CS\_PC1**

****

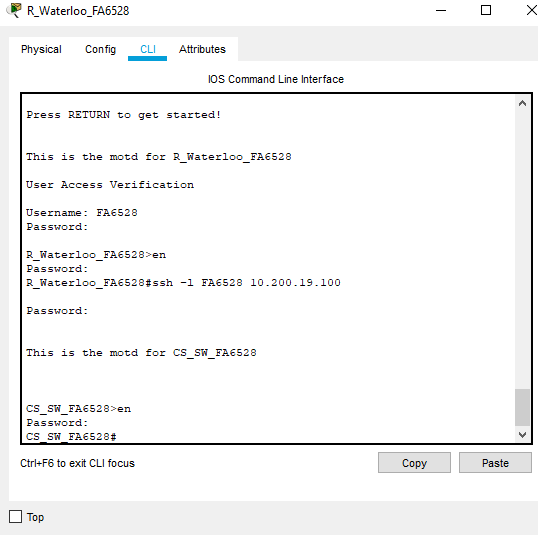
**Figure 1-20 Accessing CS\_SW from CS\_PC2**

****

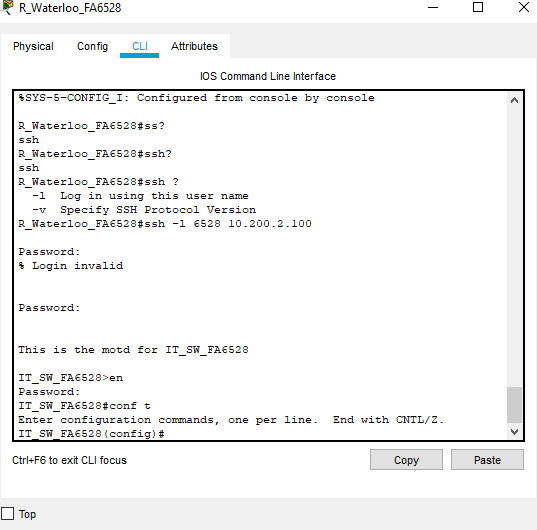
**Figure 1-21 Accessing R\_Waterloo from CS\_PC2**

****

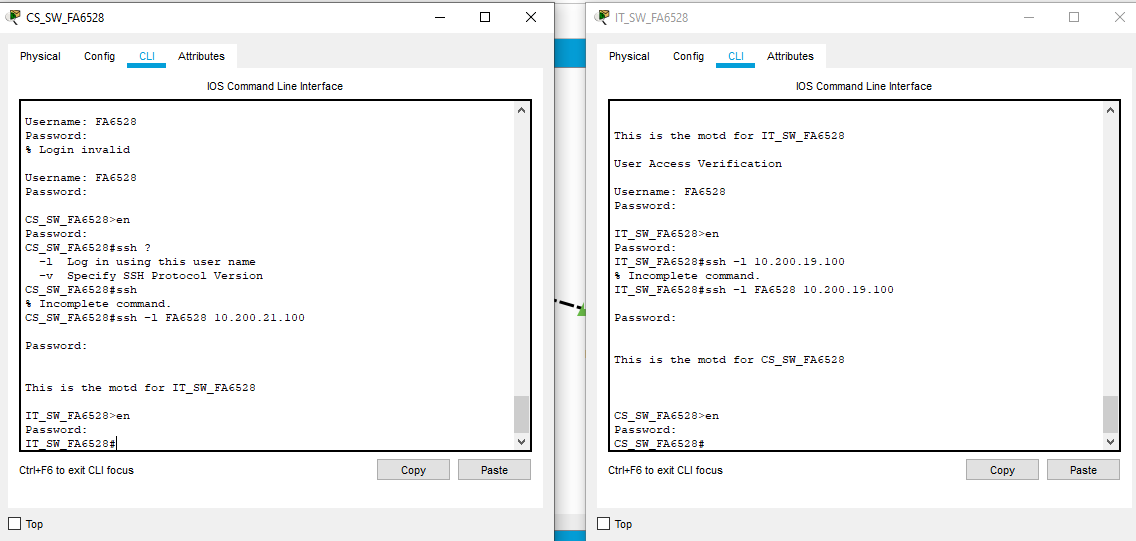
**Figure 1-22 Accessing CS\_SW & R\_Waterloo from IT\_PC2**



**Figure 1-23 Accessing CS\_SW from R\_Waterloo**

****

**Figure 1-24 Accessing IT\_SW from R\_Waterloo**

****

**Figure 1-25 Accessing IT\_SW from CS\_SW & CS\_SW from IT\_SW.**

## Reflection

As per the lab instruction massage of the day (MOTD) banner was created & it helped to understand which network device we’re about to enter as the banner was created with the name of the network device.

Privileged mode password was created to ensure that unauthorized personal can’t make any changes to network device.

Password for line console was created so that unauthorized personal can’t enter using the console connection into the network device without the password. Same way virtual terminal lines were configured to force login. Synchronous logging was also configured on the console line. Then passwords were encrypted so that no one can see the password in plain text & can easily access the devices.

Hostname & domain name were created. Username & password were created so that specific user can access the network device remotely. Crypto key RSA were configured to 1024 modulus. SSH version 2 was enabled and the virtual terminal were configured to allow access to network device using ssh and telnet.

The switches were configured as per the instruction & the IP’s were configured as well. Default gateway was also configured in the switches.

IP’s were assigned to router, server & all the pc as per the lab instructions. Default gateway were configured manually on each pc & made sure the network adapter on the server and workstations are turned on.

From CS\_PC1 & IT\_PC1 we tried to connect to IT\_Switch and the Router via ssh & we were successful. Same way, we connected from CS\_PC2 & IT\_PC2 to the CS\_Switch and the Router. We were also able to connect each switch from router via ssh –l command. We also connected from IT\_Switch to CS\_Switch & vice versa.

# Lab 2 - Static Routing

# Part 1

## Description

In this lab a simple network topology was created with the following components:

1. 1 x Cisco 2960 Switch
2. 1 x Cisco 3750 Switch
3. 2 x Cisco 2811 Router
4. 2 x PC PT Objects
5. 1 x PT Server
6. 1 x PT Laptop

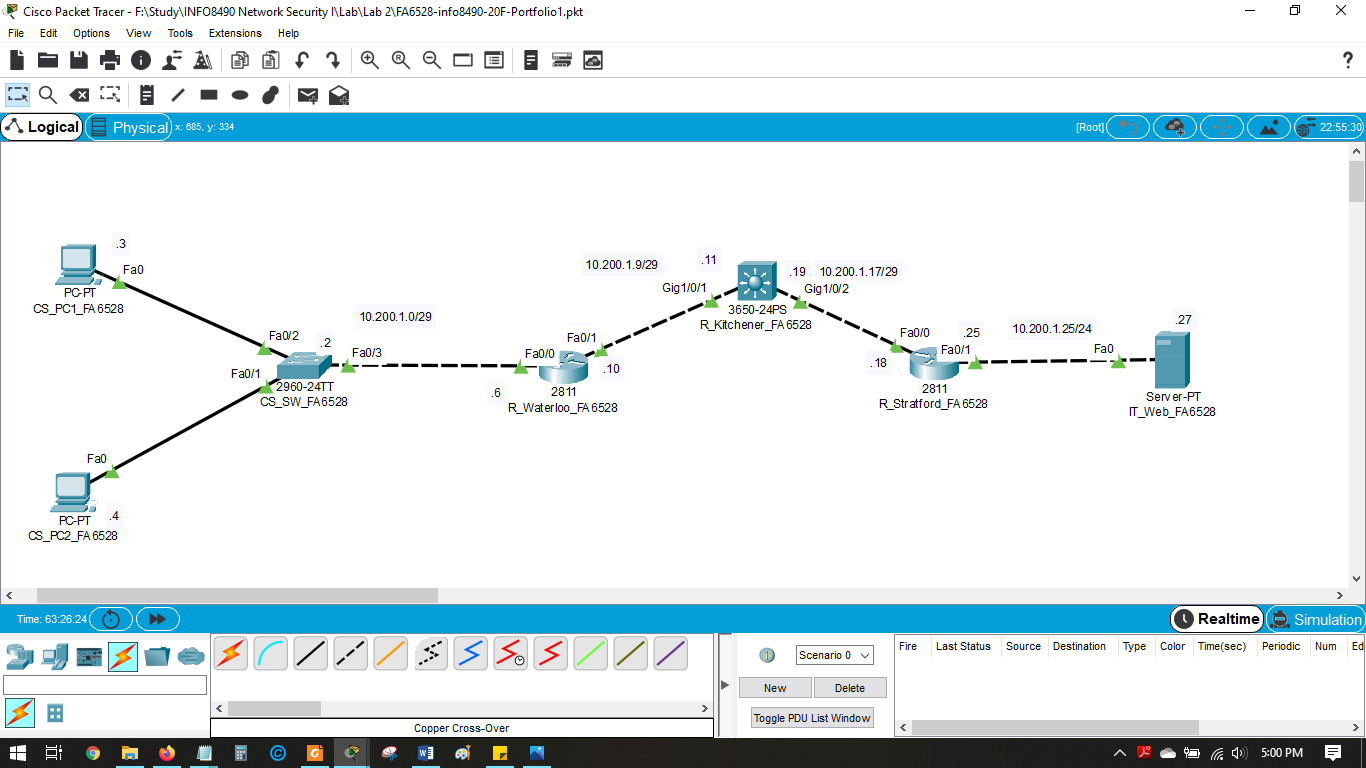
This topology is created to gain practical experience configuring and documenting the deployment of a statically routed network topology using a single subnetted address and to learn configuring network switch & router. Also to learn how to secure the networking device & how to access them remotely.

## Preparation

Prior to configuring the network topology each network device were checked to see if there is extra module needed & the modules were added accordingly. Then we made sure that each device is connected by specified connections such as copper straight-trough & copper cross-over cable. Then we made sure the network devices are turned on to configure them.

## Observations

At the beginning network topology was created (Figure 2-1) as per the lab schematics. Here, we deployed a hub and spoke network using the Layer 3 (Cisco Catalyst 3750) switch as the hub router and add an additional Cisco 2811 router as your spoke (Stub) Network devices. This topology includes 2 Workstations and 1 Web Server.



**Figure 2-1 Lab 2 Network Topology**

First, the massage of the day was created for each network devices by using “banner motd” command. It was then tested to check if the massage appears as the massage of the day.

Then as we stated in lab 1, all the procedures such as configuring privileged mode password, enforce login, password creation, terminal line password creation, password encryption, crypto key generation, enabling ssh version 2 etc were followed in lab 2 as well.

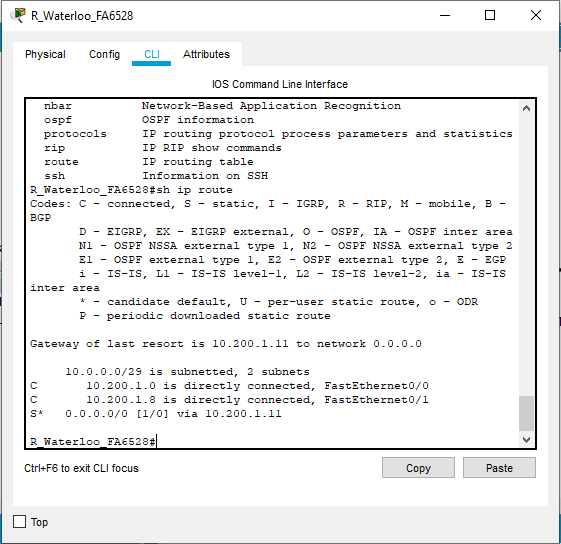
IP’s for all the switch, routers & workstations we configured as per the assigned IP.

Then we made sure that each workstation can ping its default gateway & the IP address on the other interface of its site router.

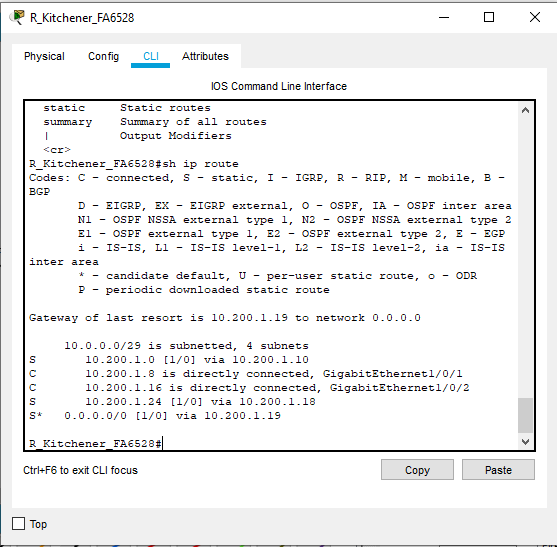
After that, we configured default static routes on R\_Waterloo and R\_Stratford using R\_Kitchener as gateway of last resort. Static routes on R\_Kitchener to both remote site LAN networks were also configured. We also made sure that each workstation can access the Server.

After each step, running config was saved to startup config before starting next step.

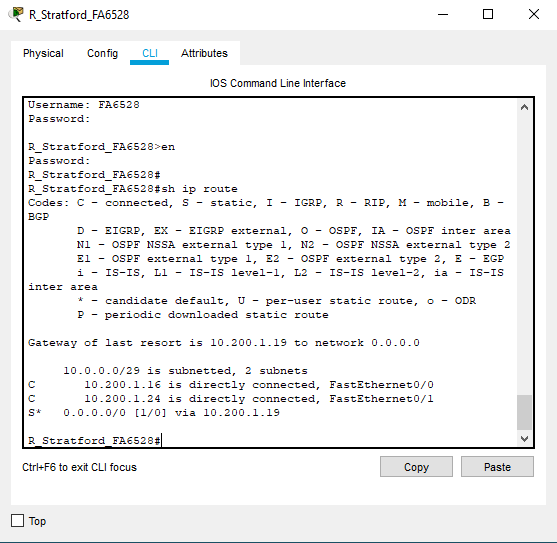
## Screenshots



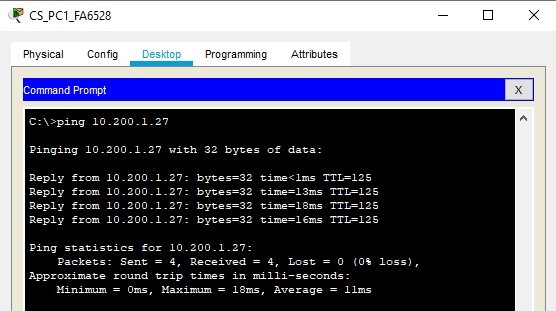
**Figure 2-2 Route table of R\_Waterloo**



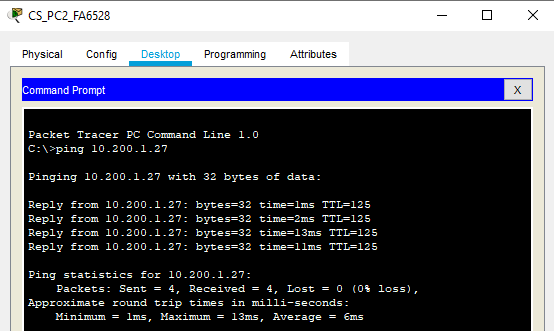
**Figure 2-3 Route table of R\_Kitchener**

****

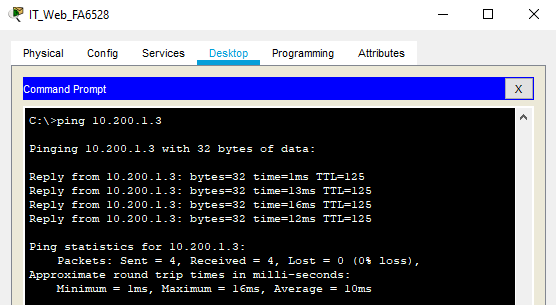
**Figure 2-4 Route table of R\_Stratford**

****

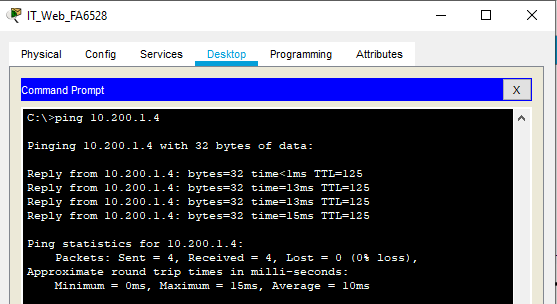
**Figure 2-5 Ping from CS\_PC1 to Server**

****

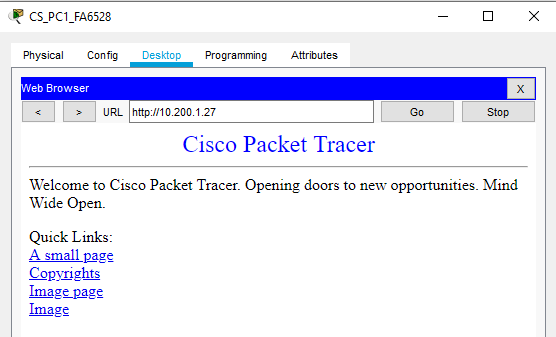
**Figure 2-6 Ping from CS\_PC2 to Server**

****

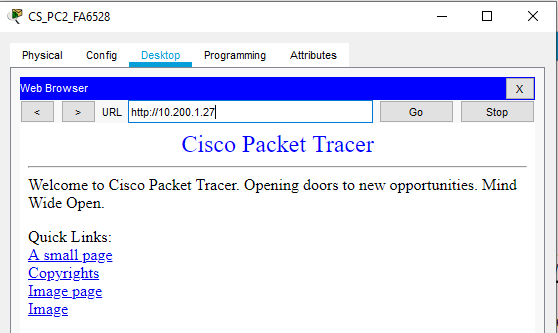
**Figure 2-7 Ping from Server to CS\_PC1**

****

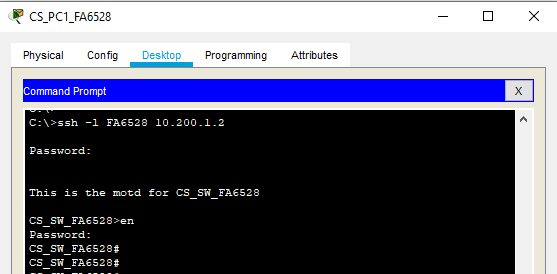
**Figure 2-8 Ping from Server to CS\_PC2**

****

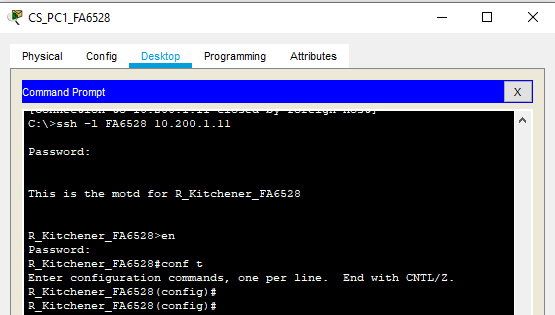
**Figure 2-9 Accessing from CS\_PC1 to Web**

****

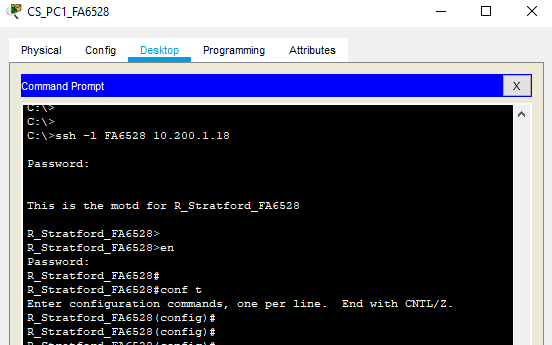
**Figure 2-10 Accessing from CS\_PC2 to Web**

****

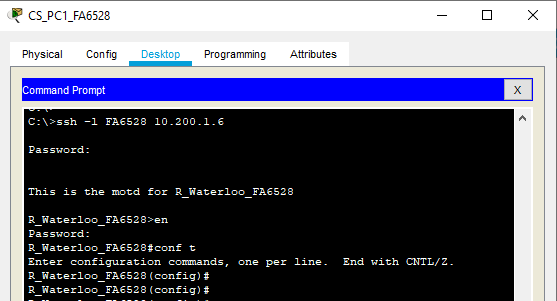
**Figure 2-11 SSH from CS\_PC1 to CS\_SW**

****

**Figure 2-12 SSH from CS\_PC1 to R\_Kitchener**

****

**Figure 2-13 SSH from CS\_PC1 to R\_Stratford**

****

**Figure 2-14 SSH from CS\_PC1 to R\_Waterloo**

## Reflection

From Part 1-6, we configures banner, privileged mode password, hostname, domain name, username, password encryption, ssh version 2, crypto key, line console etc. But when tried to ping beyond site router we were unable to do so.

Then we configured the default static routes, gateway, ip route on each routers. As a result we can now ping beyond the site router from work station to server & we can ping back to work station from server. This step was important to go beyond the site router.