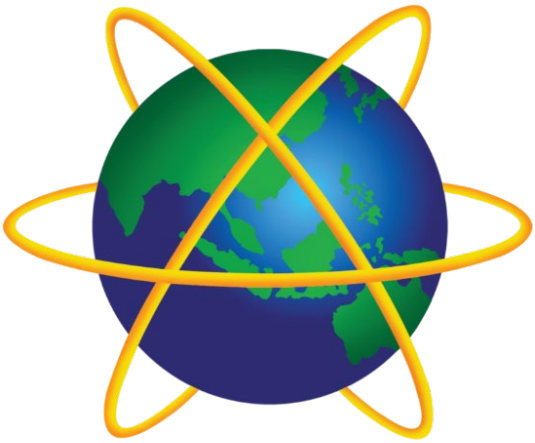

A · P · U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Switching and Routing Essentials (SRE)

Individual Assignment

Section B

Module Code: CT133-3-2-SRE

Name: Teo Kai Yii - TP058618

Intake code: APD2F2209CS(CYB)

Hand Out Date: 30th September 2022

Hand In Date: 4th December 2022

Lecturer:

SIR JOSHUA SAMUAL

Table of Contents

1.0 Introduction

In Section A, the proposed WLAN Architecture, Types of Security Attacks on Layer 2 and the Layer 2 Security Deployment to Mitigate the Attacks had been discussed. In this section, Section B, there will be further discussions on the design and the prototype of the High Dot Tech network. The WLAN configurations and port security is continued in this section.

The network of High Dot Tech company is configured and enhance with the requirements listed. There will be all the IP Addressing Table given. This assignment will include the basic device configuration, VLAN configuration, inter-VLAN configuration, DHCP configuration, routing configuration, WLAN configuration, security configuration and server configuration. Further configurations on the switches, routers, end devices, access points, WLC, and servers will be shown.

These configurations will help the High Dot Tech company to better manage or organize their network neatly. Whenever issues happen, they can also identify the problem easier and earlier. With this prototype configured Packet Tracer, the company can also try the configurations before configuring the network in the real world. This is due to the reason that any issues occur during the configuration may cause the company to have danger in the data security or affects the daily business.

In the basic configurations, the encrypted password is configured. To access the switches and routers, use the password “cisco” for all the switches and routers in the packet tracer. All the passwords are “cisco” is for easy access and easy to remember while prototyping the configurations of the High Dot Tech network. In the real world, the password configured must be stronger and much more complex.

2.0 IP Addressing Table

2.1 Subnets

Subnet	Prefix Length	Subnet Mask	Network Address	Range of Usable IP	Broadcast Address	Default Gateway
HR	/24	255.255.255.0	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255	172.16.1.1
Design	/24	255.255.255.0	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255	172.16.2.1
Manufacture	/24	255.255.255.0	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255	172.16.3.1
Management	/24	255.255.255.0	172.16.50.0	172.16.50.1 - 172.16.50.254	172.16.50.255	172.16.50.1
ServerFarm	/24	255.255.255.0	198.51.100.0	198.51.100.1 - 198.51.100.254	198.51.100.255	198.51.100.1
RBMgmt& Native	/24	255.255.255.0	192.168.100.0	192.168.100.1 - 192.168.100.254	192.168.100.255	192.168.100.1
R&D-Wireless	/24	255.255.255.0	192.168.10.0	192.168.10.1 - 192.168.10.254	192.168.10.255	192.168.10.1
WAN1	/30	255.255.255.252	200.100.100.0	200.100.100.1 - 200.100.100.2	200.100.100.3	N/A
WAN2	/30	255.255.255.252	200.100.100.4	200.100.1005 - 200.100.100.6	200.100.100.7	N/A
WAN3	/30	255.255.255.252	200.100.100.8	200.100.100.9 - 200.100.100.10	200.100.100.11	N/A
WAN4	/30	255.255.255.252	200.100.100.12	200.100.100.13 - 200.100.100.14	200.100.100.15	N/A

2.2 HQ Network – KL

KL Network

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
KL_Router	Se6/0	200.100.100.1	255.255.255.252 or /30	N/A
PC0-Management PC	Fa0	DHCP	DHCP	DHCP
HR-PC1	Fa0	DHCP	DHCP	DHCP
Design_PC1	Fa0	DHCP	DHCP	DHCP
Manufacture_PC1	Fa0	DHCP	DHCP	DHCP

Server Farm Network

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
SF_Router	Se1/0	200.100.100.2	255.255.255.252 or /30	N/A
	Se2/0	200.100.100.5	255.255.255.0 or /24	N/A
DNS Server	Fa0	198.51.100.10	255.255.255.0 or /24	198.51.100.1
Web Server	Fa0	198.51.100.20	255.255.255.0 or /24	198.51.100.1
FTP Server	Fa0	198.51.100.30	255.255.255.0 or /24	198.51.100.1

2.3 Remote Branch Network – Hanoi

Hanoi Network

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
Hanoi_Router	Se0/0	200.100.100.14	255.255.255.252 or /30	N/A
Hanoi Radius Server	Fa0	192.168.100.2	255.255.255.0 or /24	192.168.100.1
Admin PC0	Fa0	192.168.100.3	255.255.255.0 or /24	192.168.100.1
Hanoi-WLC	Gig1	192.168.100.4	255.255.255.0 or /24	192.168.100.1
User1-RB (1)	NIC	DHCP	DHCP	DHCP
User1-TabletRB	NIC	DHCP	DHCP	DHCP
User1-Smartphone (1)	NIC	DHCP	DHCP	DHCP
User2-Smartphone	NIC	DHCP	DHCP	DHCP
User2-RB (2)	NIC	DHCP	DHCP	DHCP
User2-TabletRB	NIC	DHCP	DHCP	DHCP
User2-RB (1)	NIC	DHCP	DHCP	DHCP
User3-RB (2)	NIC	DHCP	DHCP	DHCP
User3-Smartphone (1)	NIC	DHCP	DHCP	DHCP
User3-RB	NIC	DHCP	DHCP	DHCP
User3-TabletRB (1)	NIC	DHCP	DHCP	DHCP

2.4 WAN Connections

WAN Network and ISPs Network

Device (Hostname)	Interface	IP Address	Subnet Mask
KL_Router	Se6/0	200.100.100.1	255.255.255.252 or /30
SF-Router	Se1/0	200.100.100.2	255.255.255.252 or /30
	Se2/0	200.100.100.5	255.255.255.252 or /30
ISP1	Se2/0	200.100.100.6	255.255.255.252 or /30
	Se3/0	200.100.100.9	255.255.255.252 or /30
ISP2	Se2/0	200.100.100.10	255.255.255.252 or /30
	Se3/0	200.100.100.13	255.255.255.252 or /30
Hanoi_Router	Se0/0	200.100.100.14	255.255.255.252 or /30

2.5 VLAN

VLAN Number	VLAN Name
10	R&D
11	HR
22	Design
33	Manufacture
50	Management
51	ServerFarm
100	RBMgmt&Native

2.6 Port Assignments

Device (Hostname)	Ports	Assignment	Network
HR_SW	Fa0/3	VLAN 50 – Management	172.16.50.0/24
	Fa0/4-6	VLAN 11 - HR	172.16.1.0/24
Design_SW	Fa0/4-6	VLAN 22 - Design	172.16.2.0/24
Manufacturer_SW	Fa0/3-5	VLAN 33 - Manufacture	172.16.3.0/24
SF-SW	Fa0/4	VLAN 51 - ServerFarm	198.51.100.0/24
Hanoi-MLayerSW	Fa0/1-3	VLAN 10 – R&D	192.168.10.0/24
	Fa0/4-5	VLAN 100 – RBMgmt&Native	192.168.100.0/24

2.7 Router Subinterfaces

Device (Hostname)	Interface	Assignment	IP Address
KL_Router	Gig0/0.11	VLAN 11 - HR	172.16.1.1/24
	Gig0/0.22	VLAN 22 - Design	172.16.2.1/24
	Gig0/0.33	VLAN 33 - Manufacture	172.16.3.1/24
	Gig0/0.50	VLAN 50 – Management	172.16.50.1/24
SF-Router	Fa0/0.51	VLAN 51 - ServerFarm	198.51.100.1/24
Hanoi_Router	Gig1/0.10	VLAN 10 – R&D	192.168.10.1/24
	Gig1/0.100	VLAN 100 – RBMgmt&Native	192.168.100.1/24

3.0 Entire Network Layout

The entire network layout of High Dot Tech company is crucial as the network layout is crucial to ensure the smooth operation of High Dot Tech network. The chosen topologies for the High Dot Tech company's business operations will enhance performance while also assisting the company in locating problems, resolving problems, and strategically allocating resources throughout the High Dot Tech network to ensure optimal network health. High Dot Tech network is organized and maintained effectively which will increase energy and data efficiency. This will help High Dot Tech company to save operating and maintenance costs (DNSstuff, 2022).

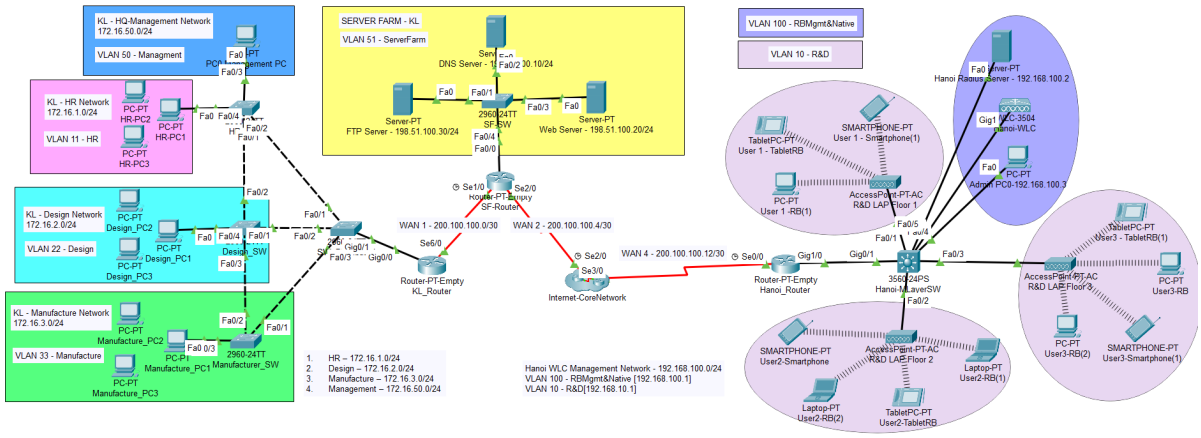

Figure 1 Network Layout of High Dot Tech

The network layout of High Dot Tech Network will be Hybrid Topology. The Hybrid topology of High Dot Tech network combines point to point topology, star topology, and bus topology. Due to the fact that the High Dot Tech company includes several departments, each of which has a specific network topology suited to their needs and network usage, the High Dot Tech network uses a hybrid topology (DNSstuff, 2022).

High Dot Tech Network will use a hybrid topology for its network design. High Dot Tech's network uses a hybrid architecture that incorporates point-to-point, star, and bus topologies. The High Dot Tech network has a hybrid topology since the organisation has a number of departments, each of which has a unique network design appropriate for their requirements and network consumption (DNSstuff, 2022).

Benefits

The main benefit of hybrid topology is flexibility since there are few restrictions on the network structure itself that a hybrid design cannot accept (DNSstuff, 2022).

Since there are few limitations on the network structure itself that a hybrid design cannot accept, flexibility is the fundamental advantage of hybrid topology for the High Dot Tech network (DNSstuff, 2022).

Issues

Each network design has disadvantages of its own. As a network becomes more complex, the amount of skill and experience required of administrators to ensure optimal performance also rises. Financial expenses must be considered while creating a hybrid network topology (DNSstuff, 2022).

Network architecture of High Dot Tech network has drawbacks of its own. The level of expertise and knowledge needed by administrators to achieve optimum performance increases as a network's complexity increases. When designing a hybrid network architecture, costs must be taken into account (DNSstuff, 2022).

3.1 HQ Network – KL

3.1.1 KL Network

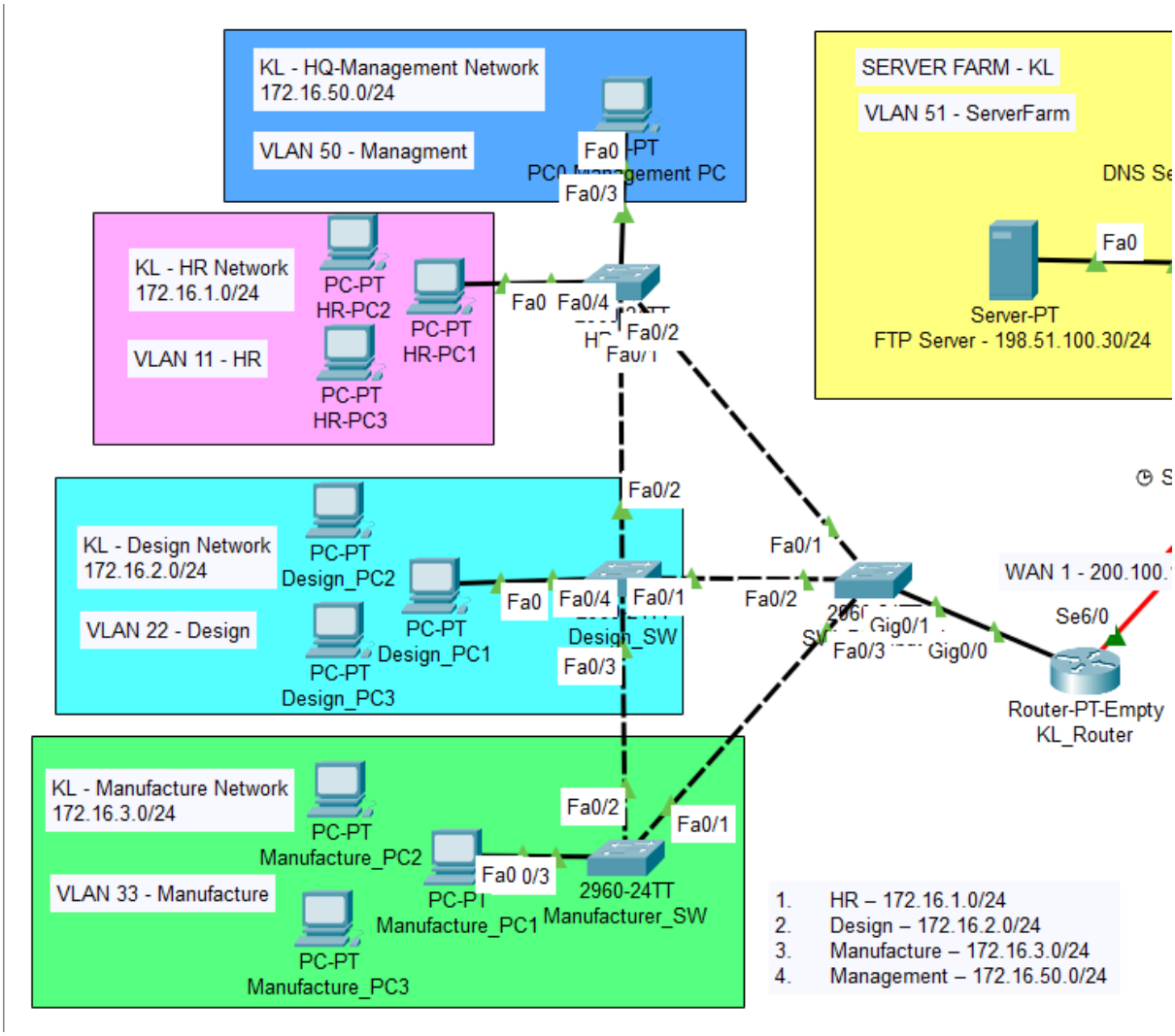

Figure 2 KL Network

The network layout of the KL network will be using the star topology. Star topology happens when all switches is directly linked to the SW_Distributed switch via Copper Cross-Over cable. The SW Distributed switch will function as a server, control data transmission, and repeater since all network traffic must pass through it before it can reach its destination in order to prevent data loss. Since all network traffic of KL network must travel through the SW_Distributed switch before it can reach its destination in order to avoid data loss, it will act as a server, regulate data transfer, and repeater (DNSstuff, n.d.).

3.1.2 Server Farm Network

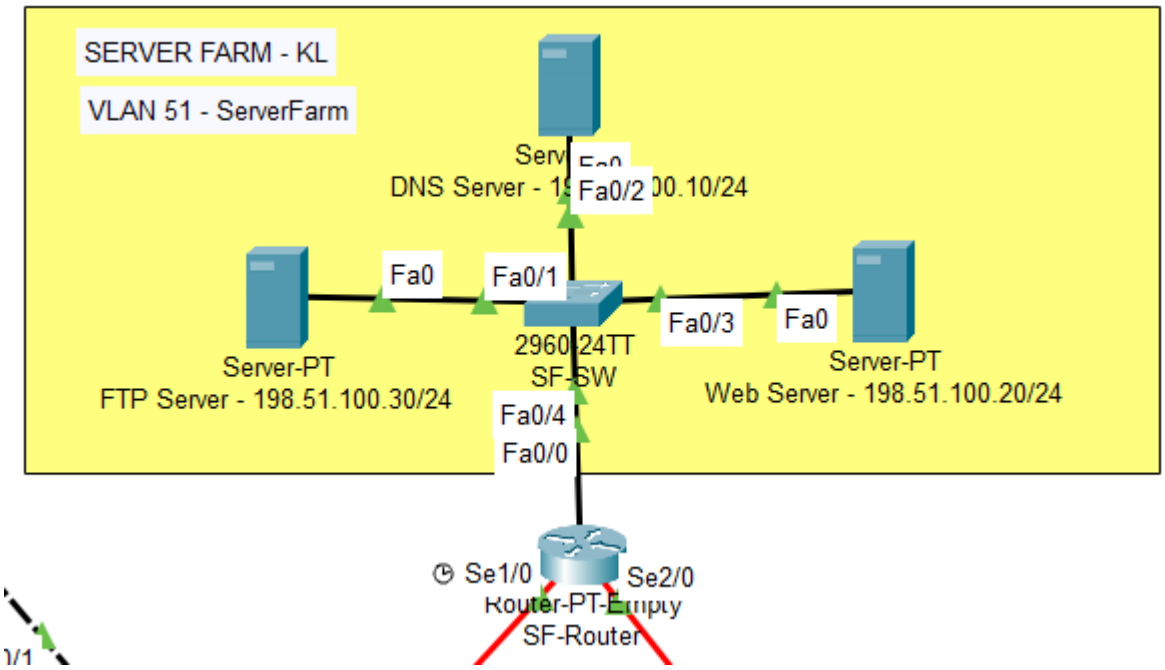

Figure 3 Server Farm Network

The network layout of the Server Farm network will be using the star topology as well. Star topology happens when all servers is directly linked to the SF-SW switch via Copper Straight-Through cable.

The star topology will also be used for the Server Farm network's network design. When all servers are connected directly to the SF-SW switch using copper straight-through cable, star topology occurs.

3.2 Remote Branch Network – Hanoi

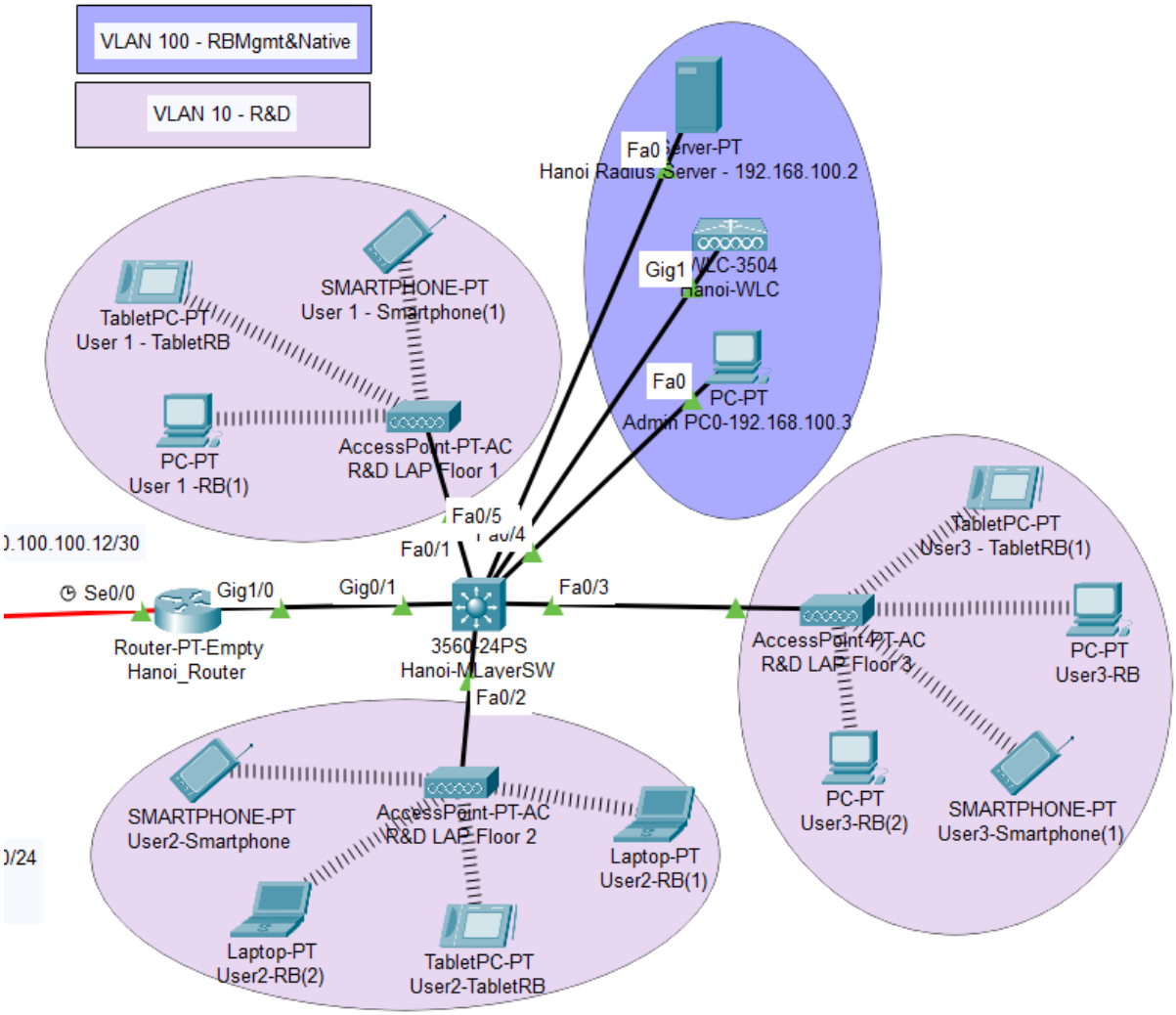

Figure 4 Hanoi Network

The network layout of the Hanoi network will be using the star topology as well. Star topology happens when all devices is directly linked to the Hanoi-MLayerSW switch via Copper Straight-Through cable.

The star topology will also be used in the network design of the Hanoi network. When every device is connected directly to the Hanoi-MLayerSW switch via copper straight-through cable, star topology occurs.

3.3 WAN Connections

3.3.1 WAN Network

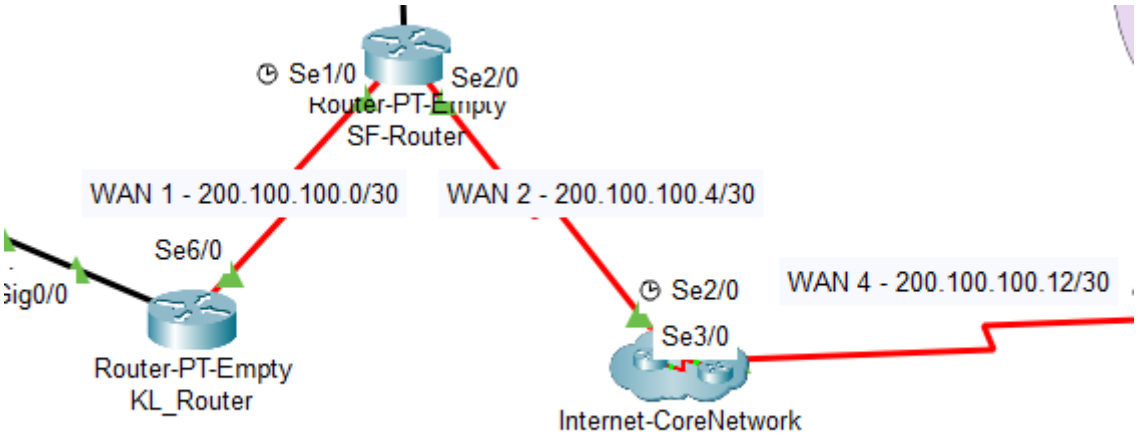

Figure 5 WAN Network

The point-to-point topology will be used for the WAN network's network design. When all servers are connected directly to the SF-SW switch using Copper Straight-Through wire, point-to-point topology is created. A serial cable is used to link two routers. Using this topology, helps enhancing the speed and bandwidth, reduce latency and simple to maintain (Indeed, 2022).

The WAN network's network architecture of High Dot Tech network will make use of the point-to-point topology. Point-to-point topology is established when all servers use Copper Straight-Through cable to connect directly to the SF-SW switch. Two routers are connected using a serial cable. Utilizing this design improves the bandwidth and speed, reduces latency, and is easy to maintain for High Dot Tech network (Indeed, 2022).

4.0 LAN and WAN configuration.

4.1 Basic Configuration

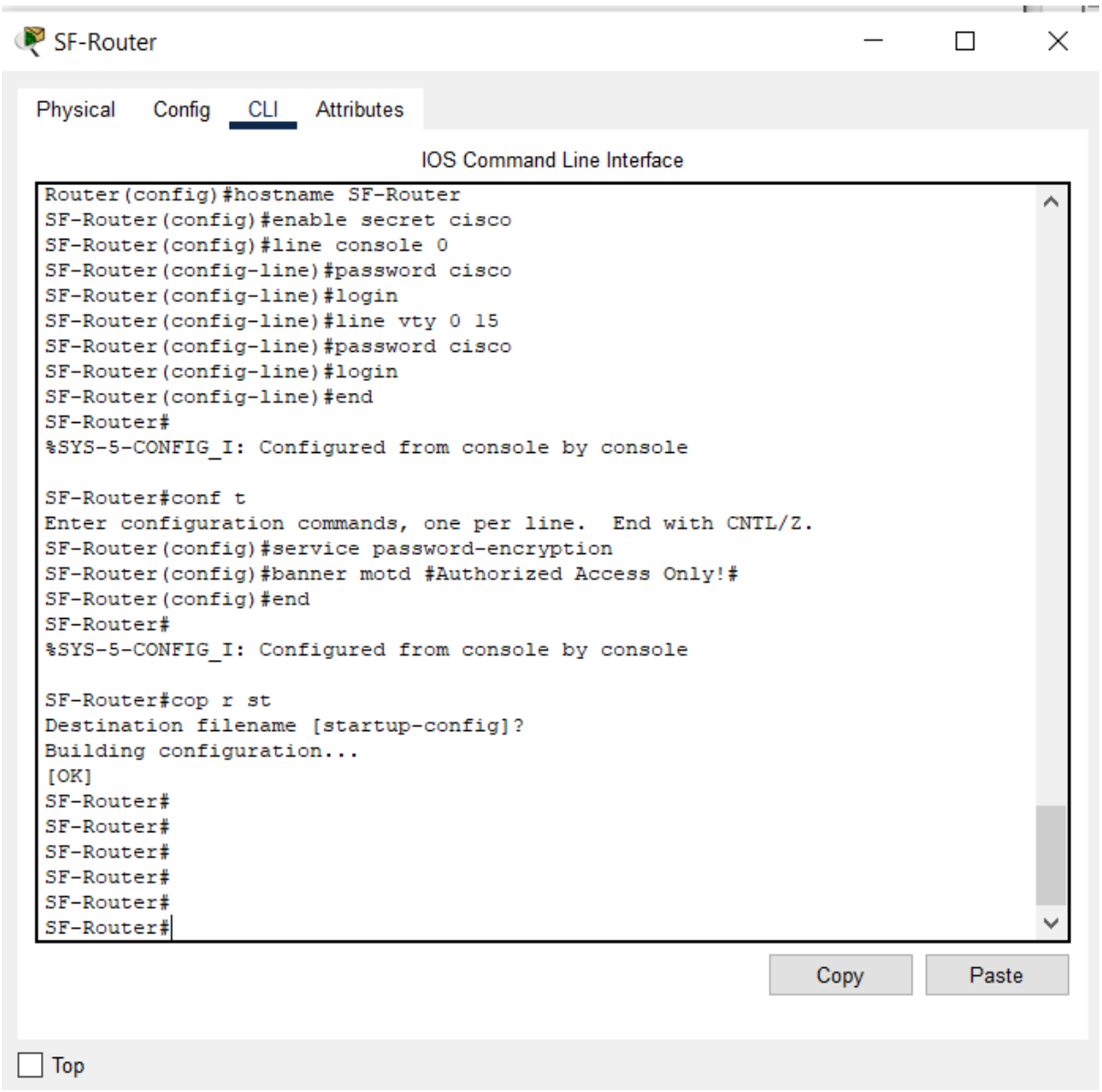

Figure 6 Basic Configuration

The routers and switches is configured with the basic configurations above. The first thing to configured will be the hostname. The password of user EXEC mode, priviledged EXEC mode, VTY line access is configured. The “login” command is used to enable the passwords. The password in the routers is encrypted. The banner message is given with the command above. The configurations is saved into NVRAM and RAM.

```
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
```

Figure 7 Encrypted Password

As shown above, the password is encrypted. The random alphabets and numbers code above will be the password that is encrypted.

```
Authorized Access Only!

User Access Verification

Password:
```

Figure 8 Banner

The banner appears before entering the password. The banner will warn the unauthorized user who tend to logged in to the system illegally.

4.2 Server Configurations

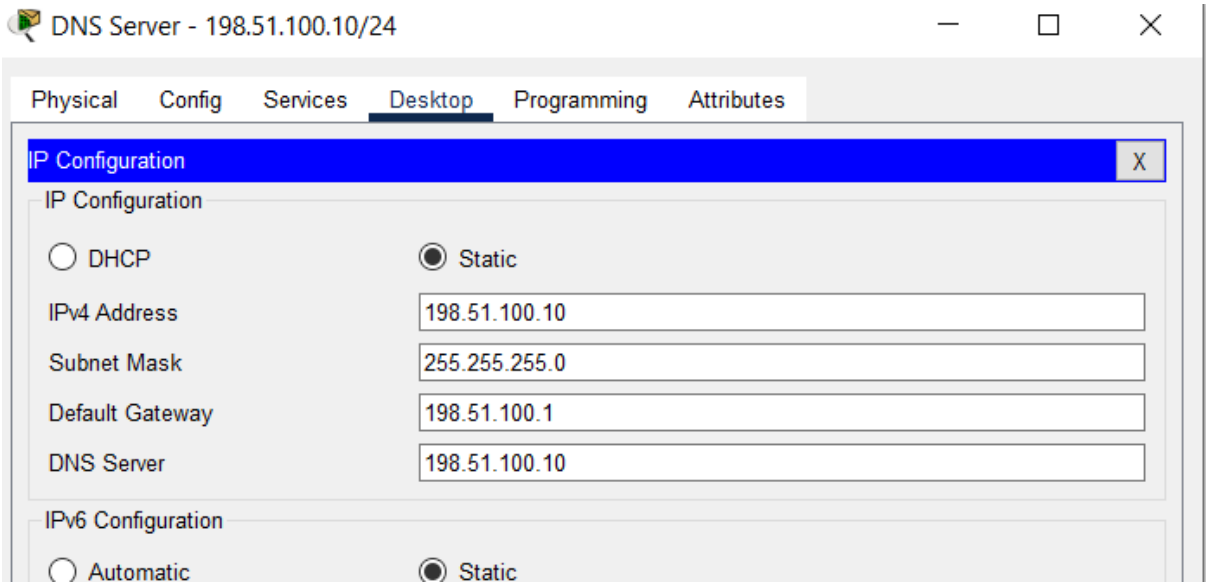

Figure 9 DNS Server

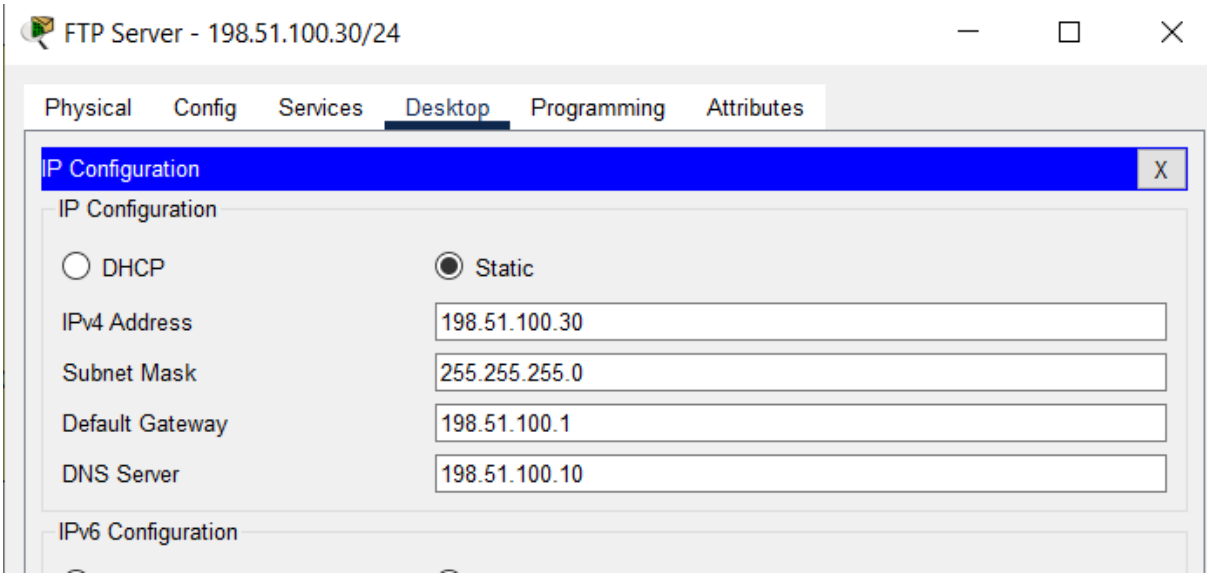

Figure 10 FTP Server

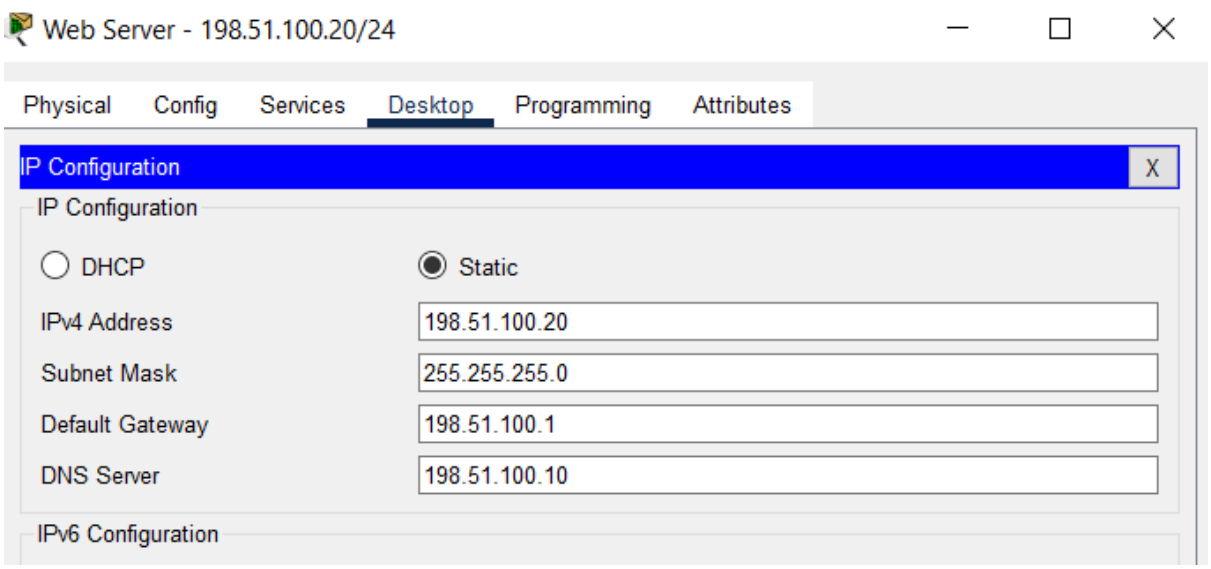

Figure 11 Web Server

The given Ip address is used to configure the DNS server's IP address. The Server Farm network's gateway is assigned the first usable IP address.

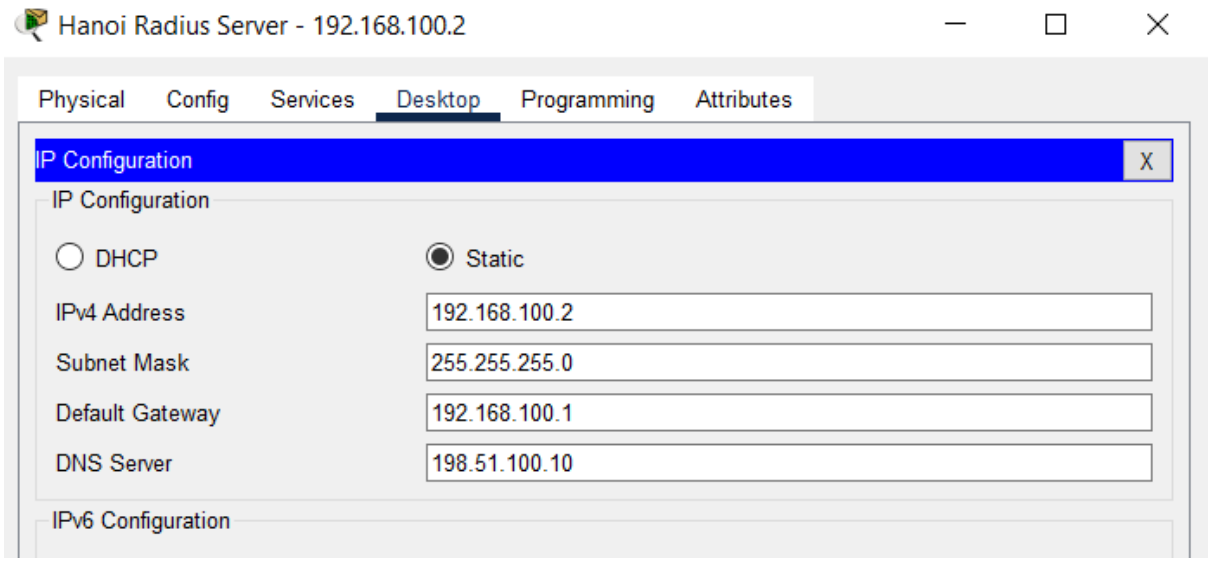

Figure 12 Hanoi Radius Server

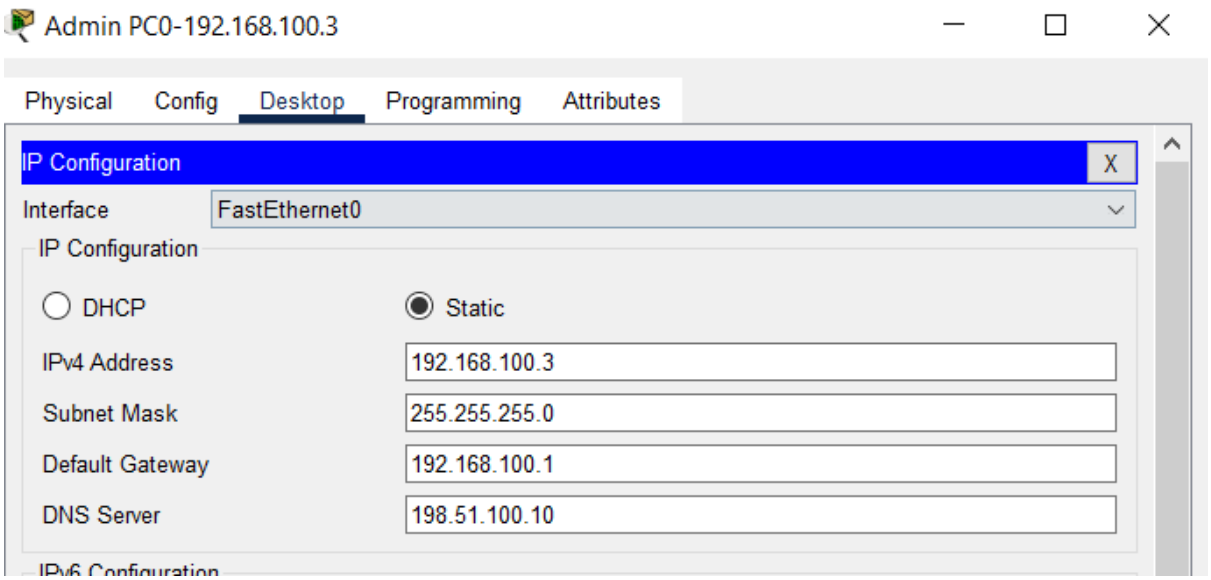

Figure 13 Admin PC0

The DNS server, Admin PC 0, and radius server all have the specified IP addresses set for them. The first useable IP address is chosen for the Hanoi network's gateway.

4.2.1 Web Server

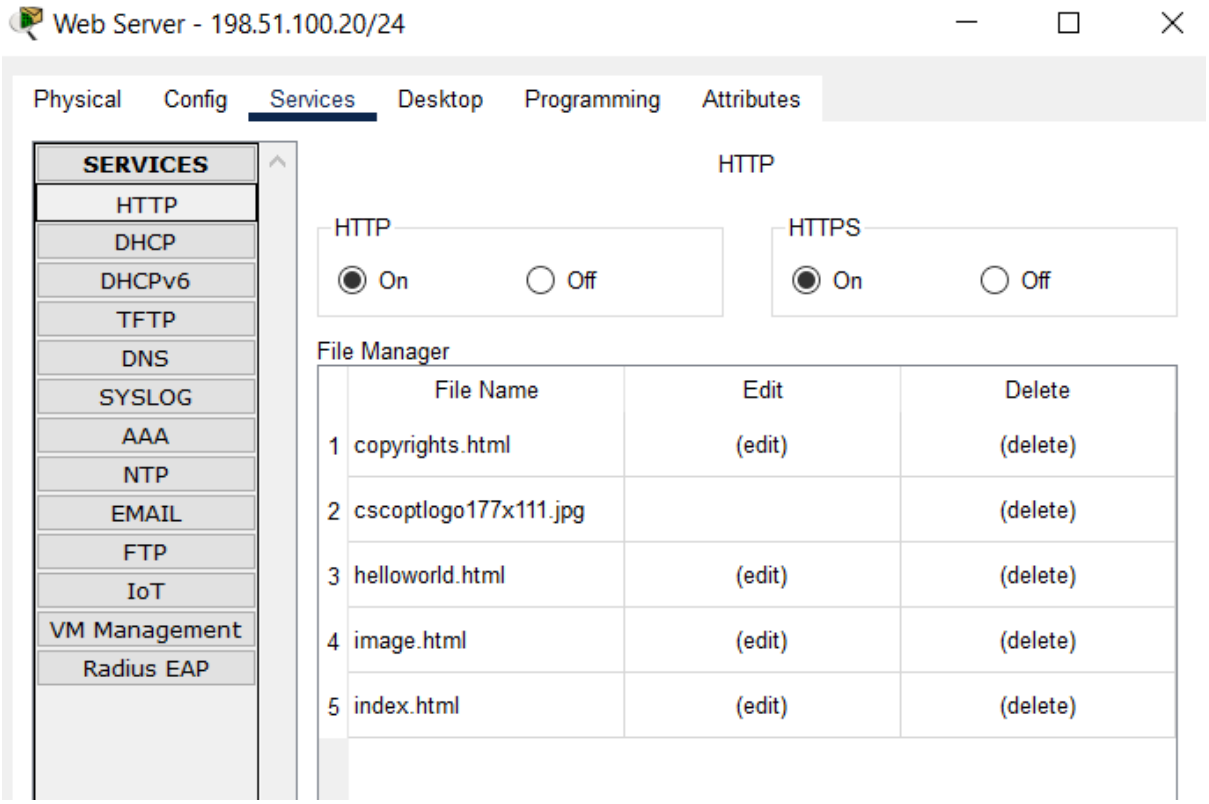

Figure 14 HTTP Services

The HTTP and HTTPS services is enabled in the Web Server. The index.html file can be edited with the "(edit)" button.

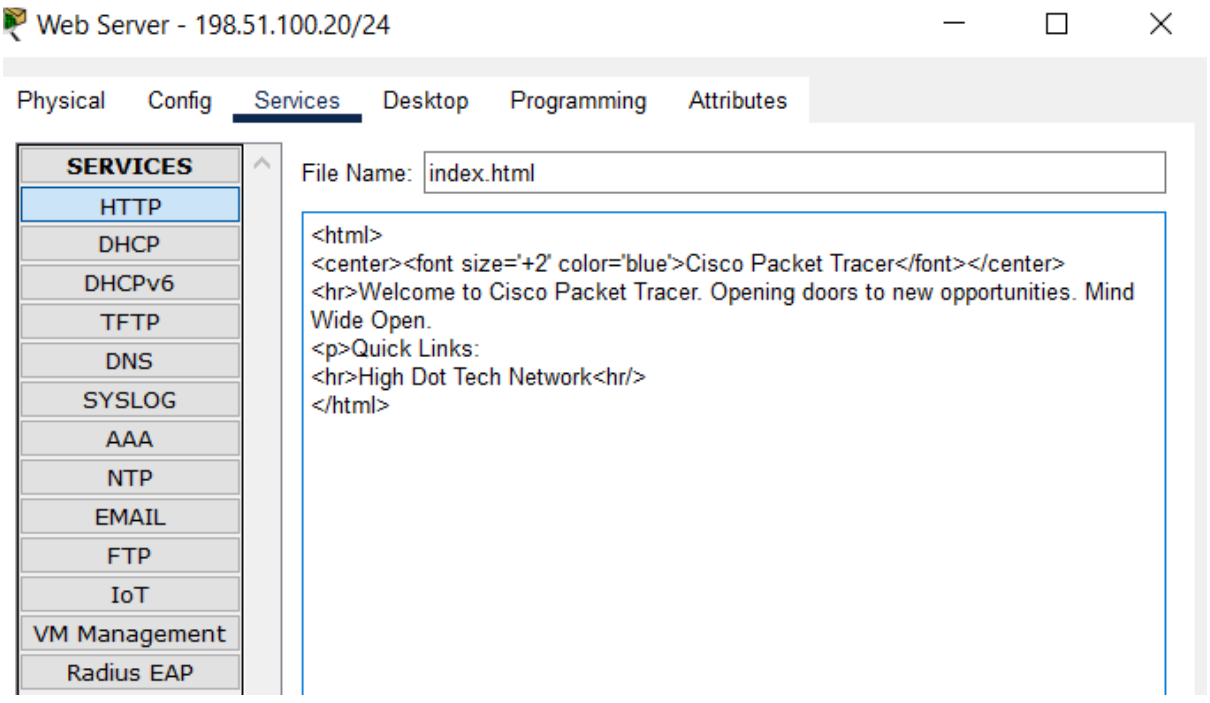

Figure 15 index.html

The index.html file is configured with the High Dot Tech Network text in order to identity the correct webpage is connected. Other texts under the welcome message is removed and replaced with the header of “High Dot Tech Network”. Users will get to see this page when they try connecting to this webpage.

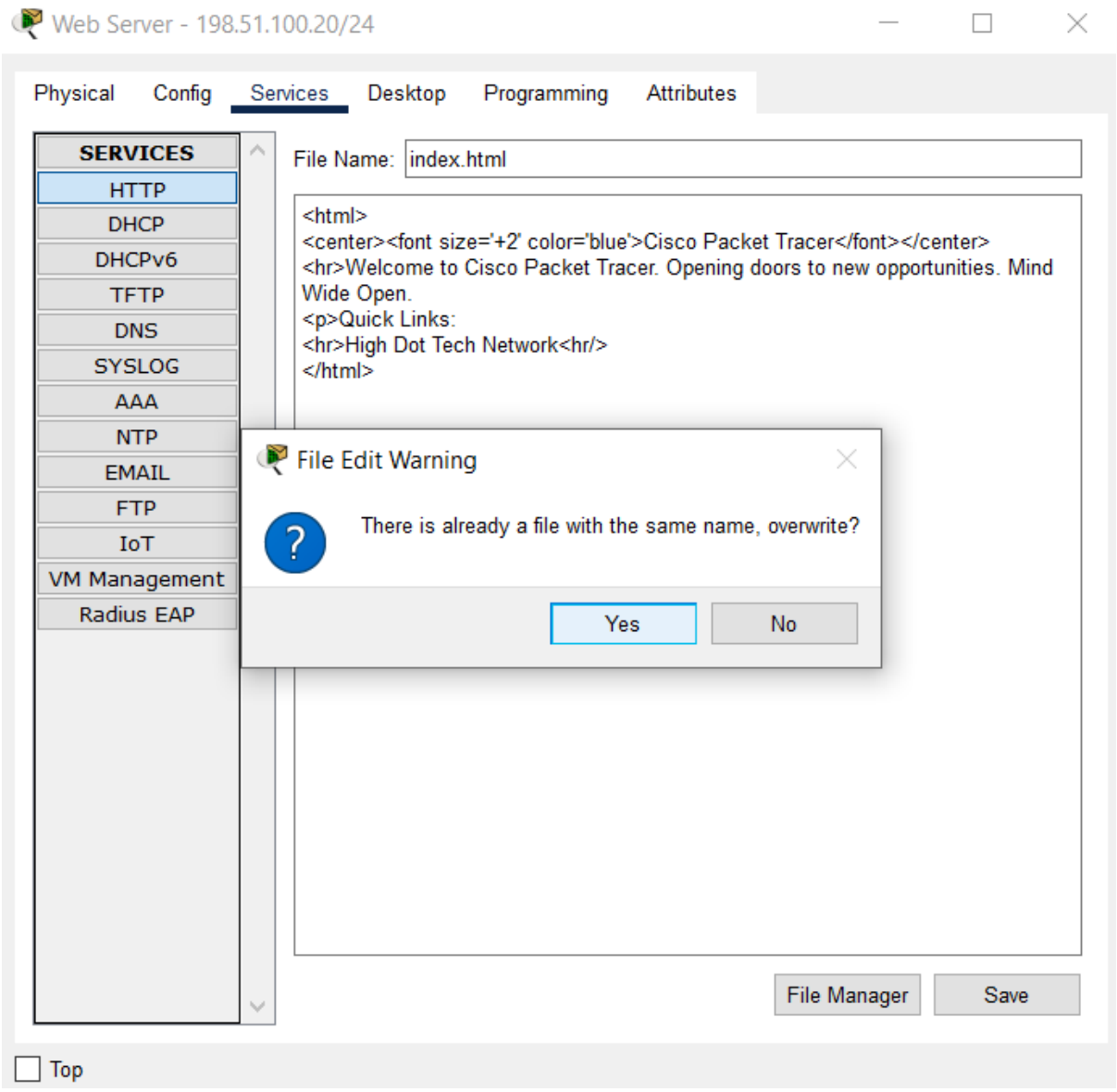

Figure 16 Dialog

Click “Yes” on the File Edit Warning dialog box in order to modify the file content of index.html. The index.html file in the server will write with the new file content.

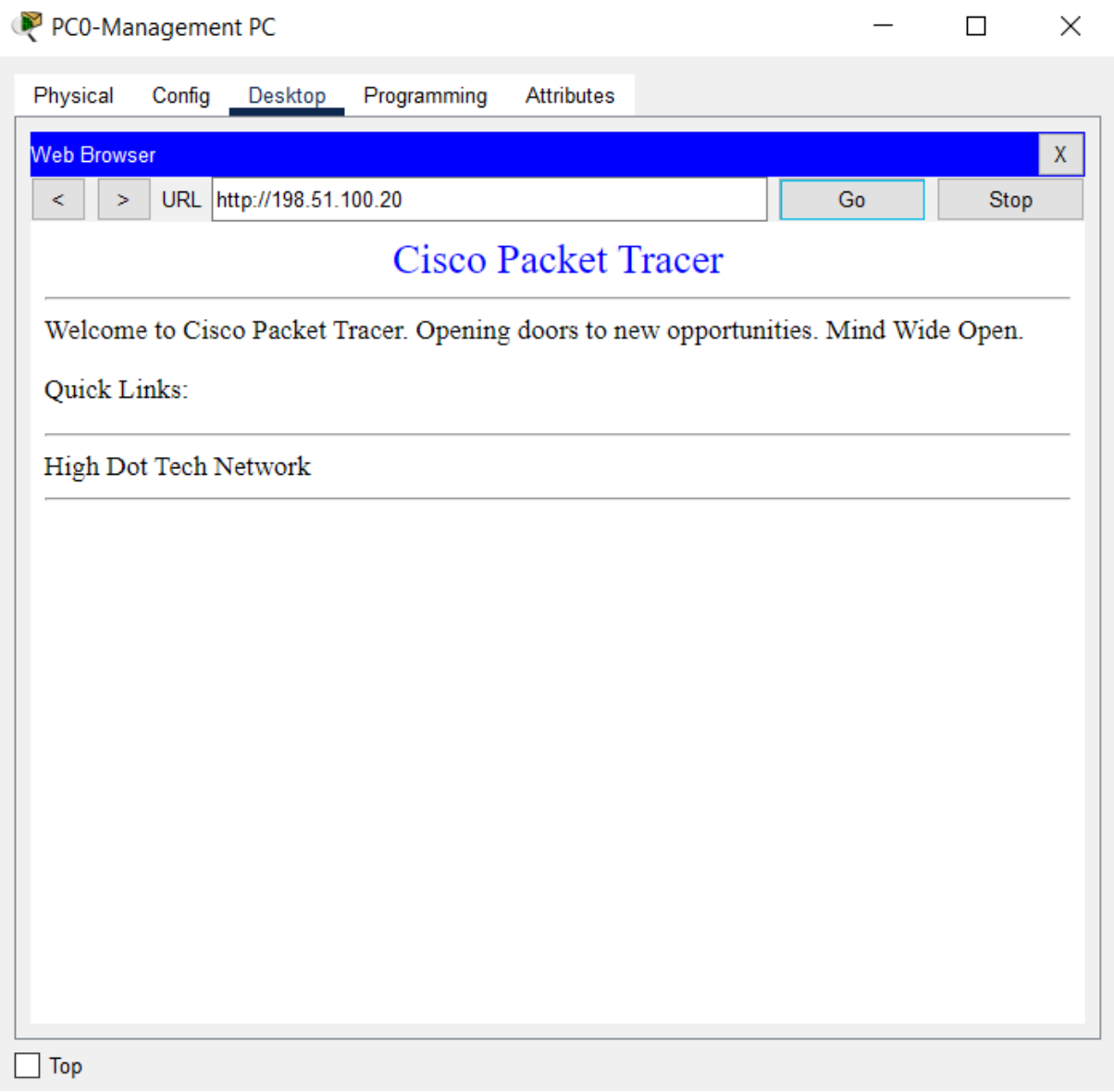

Figure 17 PC0-Management PC

As shown in the Figure 15 PC0-Management PC, the webpages with the text of the High Dot Tech Network text are connected with the IP address of the Web Server.

4.2.2 FTP Server

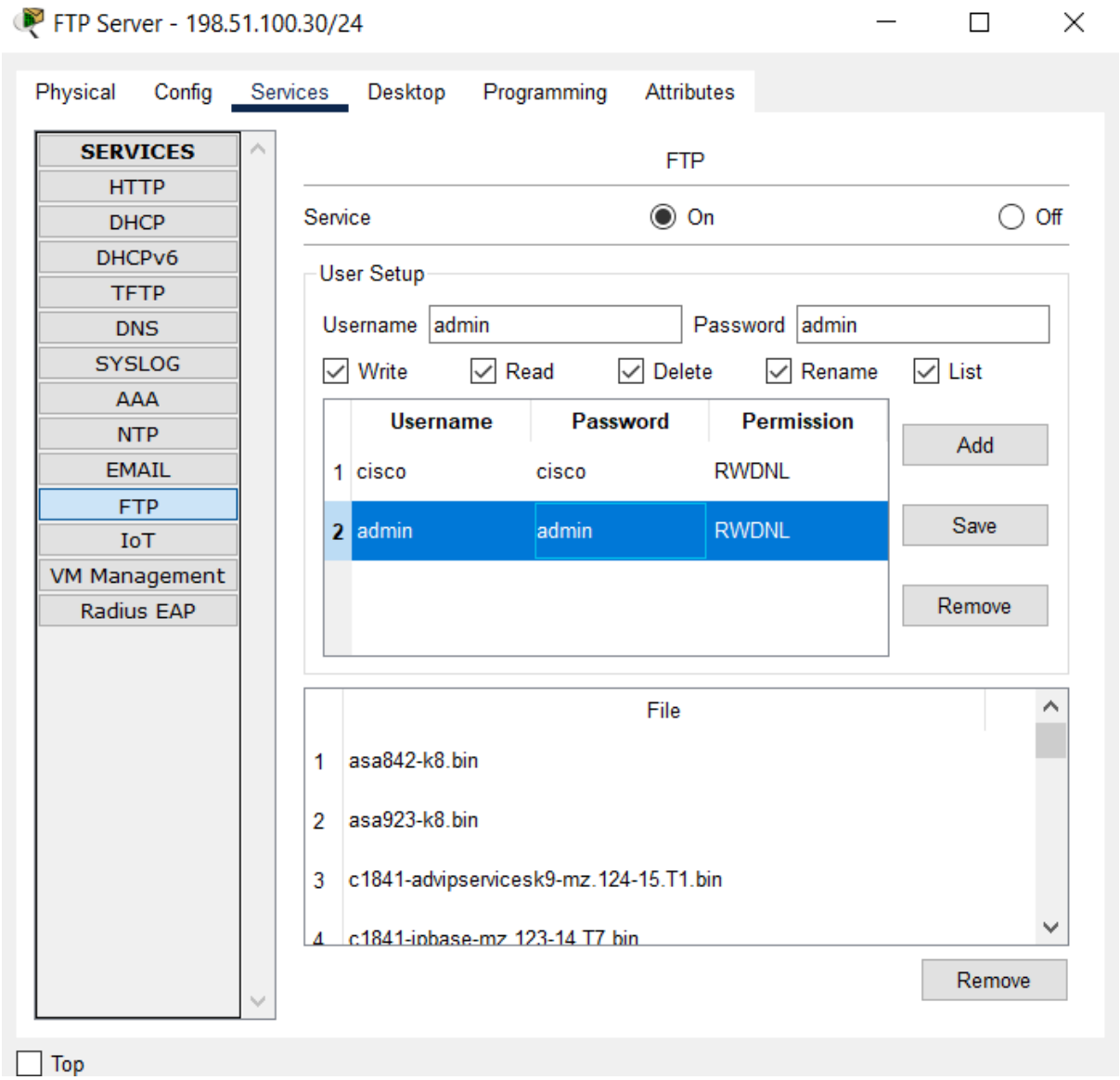

Figure 18 FTP Server

The FTP server is configured by enabling the FTP services. User with username of "admin" and password of "admin" is created by giving this user the permission of write, read, delete, rename and list.

4.2.3 DNS Server

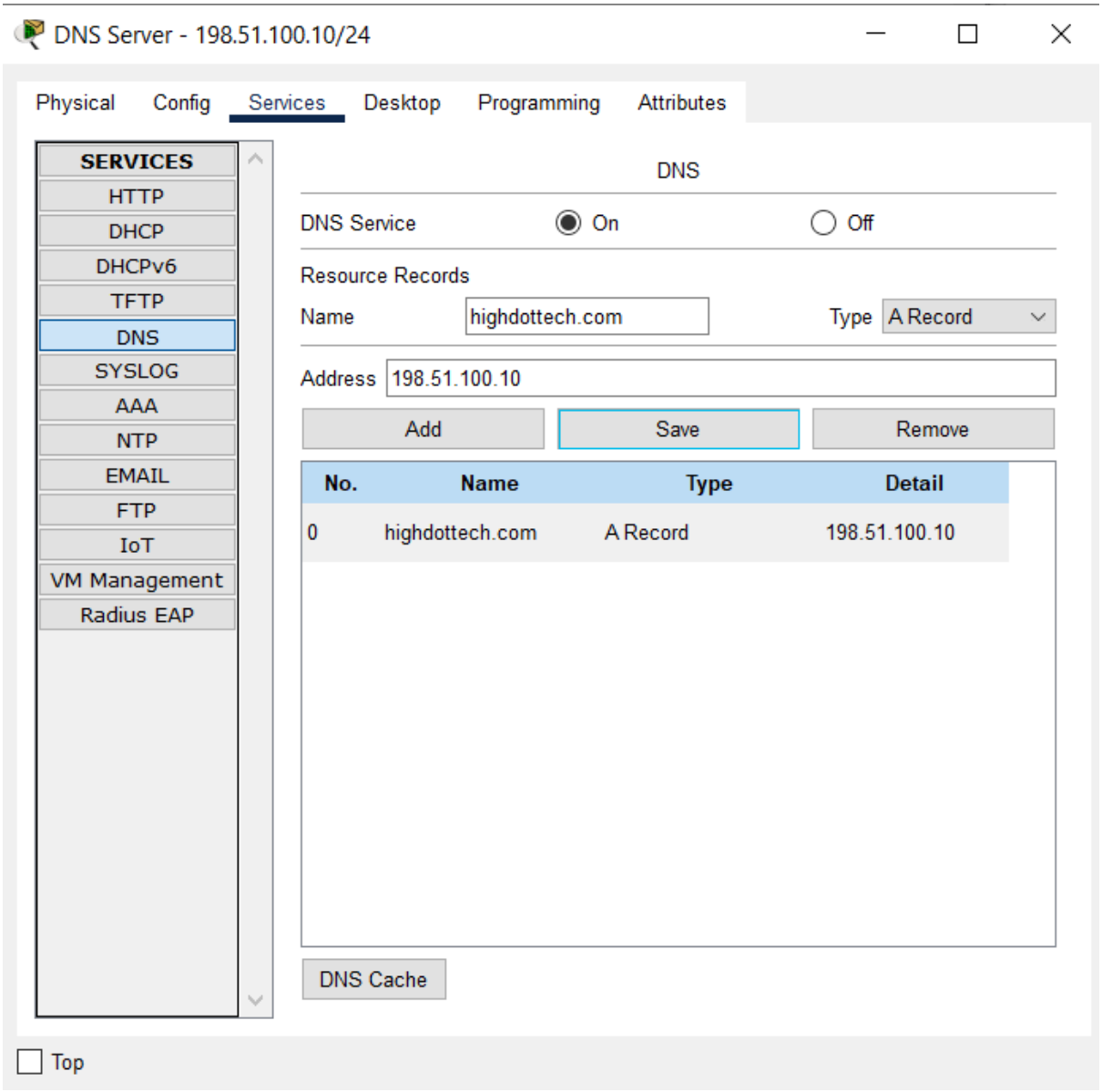

Figure 19 DNS Server

DNS Server is configured by enabling the DNS service. The name, address, and type are given to add new record.

4.3 Static IP Addressing

Static IP Addressing means the IP address does not change. High Dot Tech network have static Ip addresses to operate the web server, dns server, ftp server, radius server, WLC, and Admin PC0. This will make it easier to recall the IP address. Static IP addresses, however, must be manually configured (WatchGuard, n.d.).

The IP address is static when it doesn't change. Static IP addresses are used by the High Dot Tech network to run the web server, DNS server, FTP server, Radius server, WLC, and Admin PC0. The IP address will be simpler to remember as a result.

```
KL_Router(config)#int se6/0
KL_Router(config-if)#ip address 200.100.100.1 255.255.255.252
KL_Router(config-if)#no shut
```

```
SF-Router(config)#int se1/0
SF-Router(config-if)#ip address 200.100.100.2 255.255.255.252
SF-Router(config-if)#no shut
```

```
SF-Router(config)#int se2/0
SF-Router(config-if)#ip address 200.100.100.5 255.255.255.252
SF-Router(config-if)#no shut
```

```
ISP1(config)#int se2/0
ISP1(config-if)#ip address 200.100.100.6 255.255.255.252
ISP1(config-if)#no shut
```

```
ISP1(config)#int se3/0
ISP1(config-if)#ip address 200.100.100.9 255.255.255.252
ISP1(config-if)#no shut
```

```
ISP2(config)#int se2/0
ISP2(config-if)#ip address 200.100.100.10 255.255.255.252
ISP2(config-if)#no shut
ISP2(config-if)#ex
ISP2(config)#int se3/0
ISP2(config-if)#ip address 200.100.100.13 255.255.255.252
ISP2(config-if)#no shut
ISP2(config-if)#ex
```

```
Hanoi_Router(config)#int se0/0
Hanoi_Router(config-if)#ip address 200.100.100.14 255.255.255.252
Hanoi_Router(config-if)# no shut
```

In the figures above above, the IP address and subnet mask are shown to indicate how they are configured. The specified router's port is enabled by the "no shutdown" command.

4.4 Dynamic IP Addressing

The dynamic address could be automatically given to another device if it is not currently in use. Dynamic Host Configuration Protocol (DHCP) is used in the High Dot Tech network to assign dynamic IP addresses. An IP address is automatically assigned to the end devices when the device connected to the DHCP server. It can be a different IP address or the one the end device previously had. The DHCP server will provide a new client a dynamic IP address if the connection is terminated (WatchGuard, n.d.). In High Dot Tech network, DHCP Server is configured for the dynamic IP addressing of the LANs. For all the subnet of the DHCP configured, the first five IP address is reserved for other configurations.

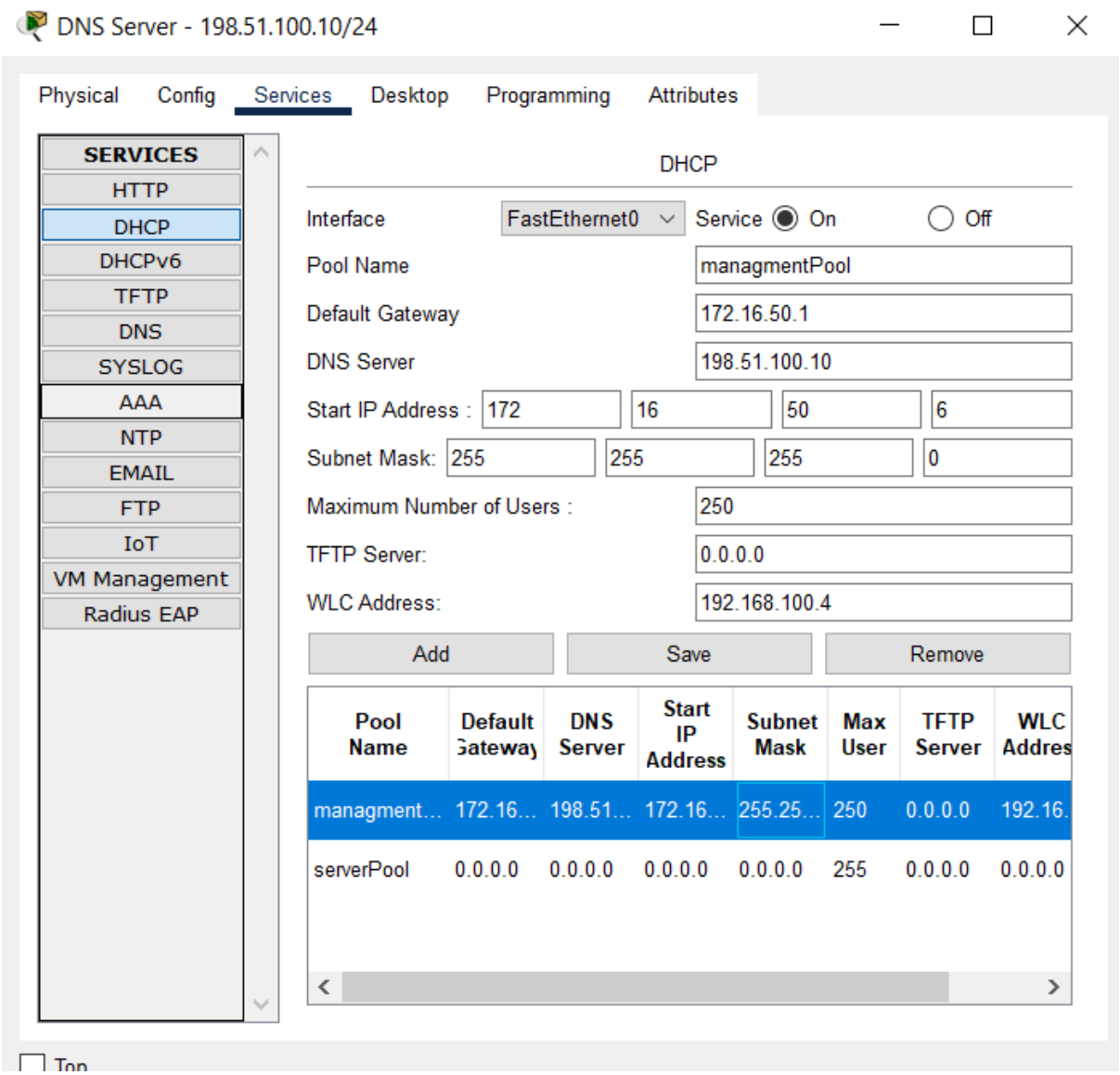

Figure 20 managementPool

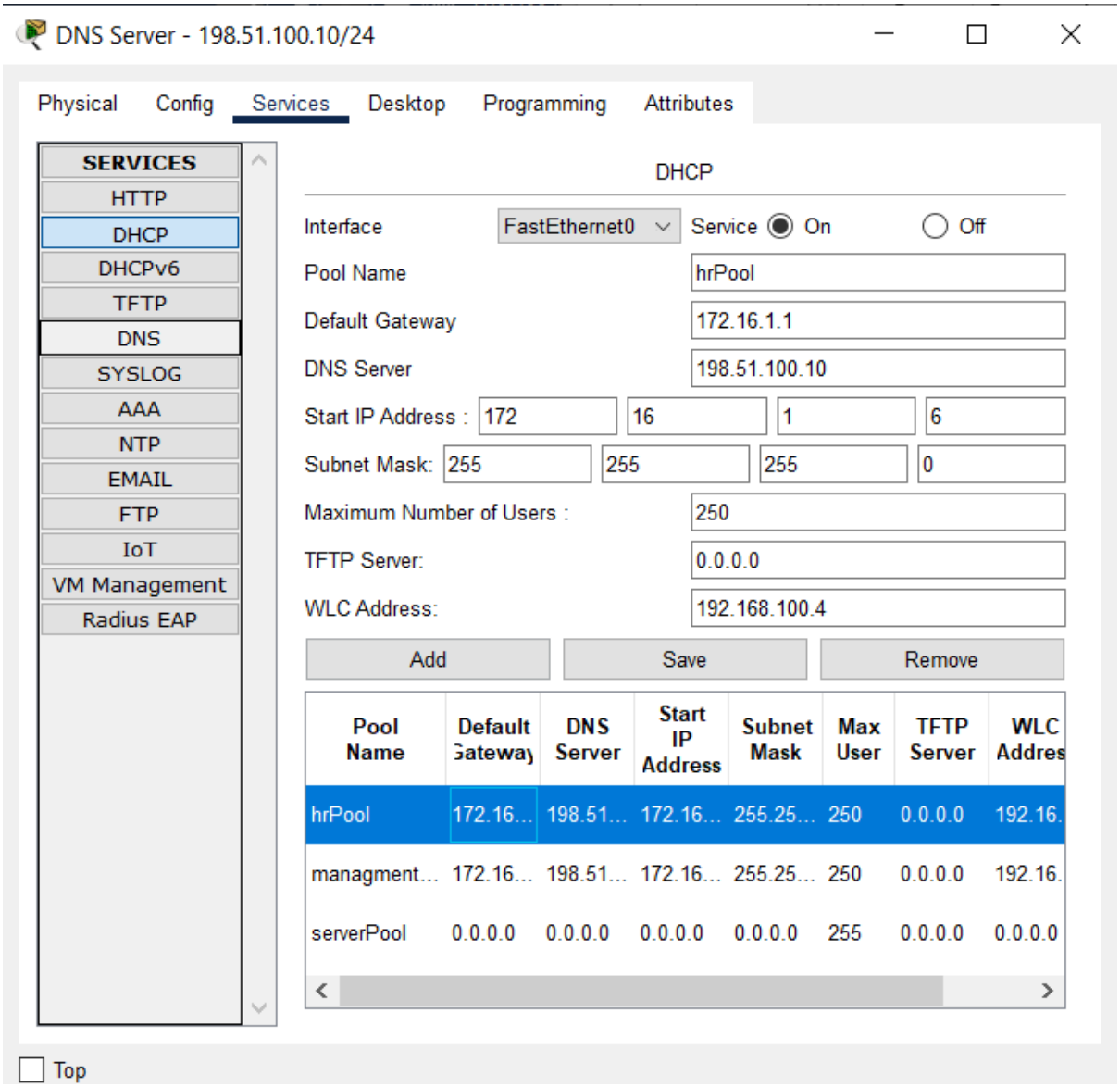

Figure 21 hrPool

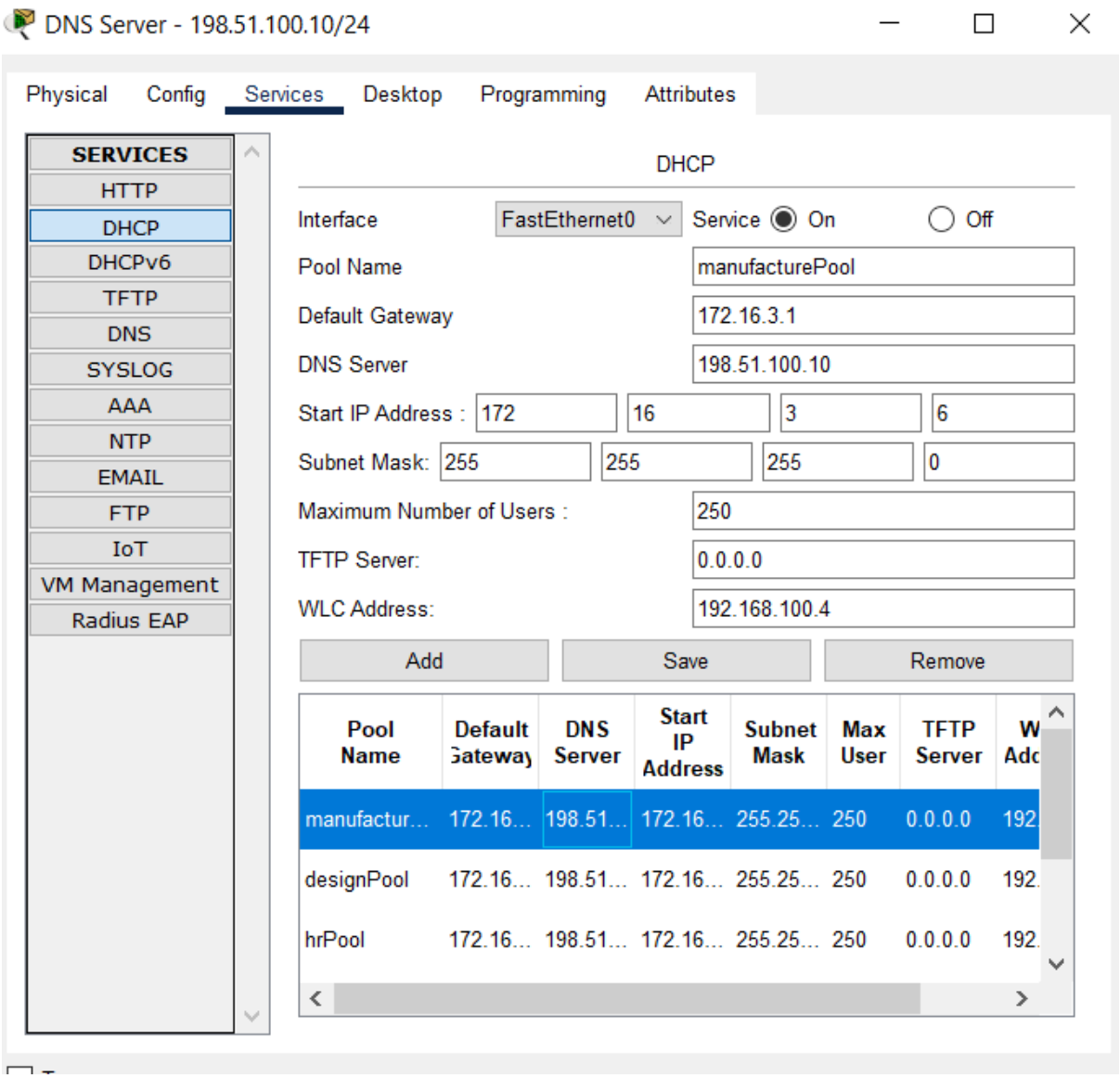

Figure 22 manufacturePool

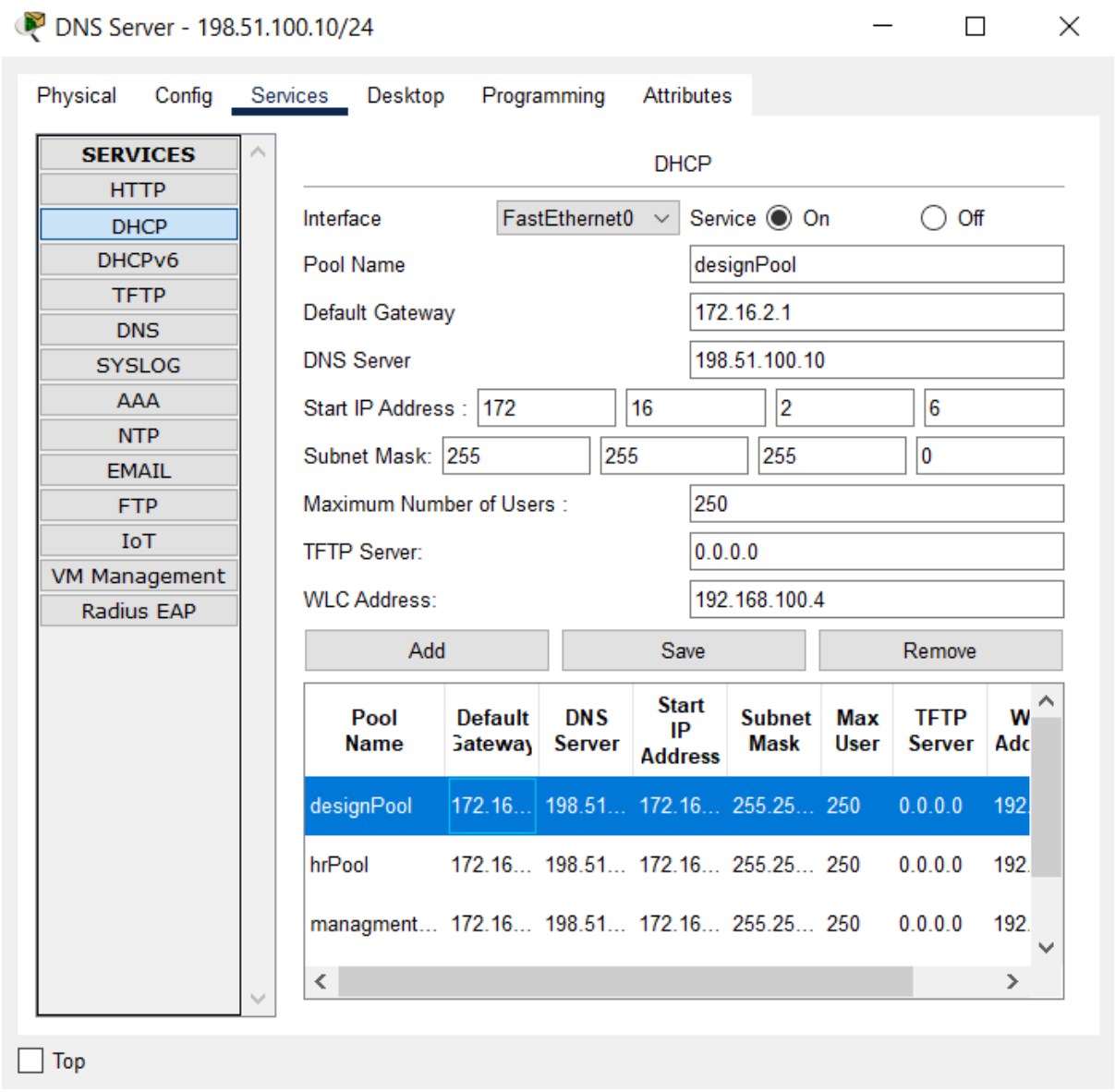

Figure 23 designPool

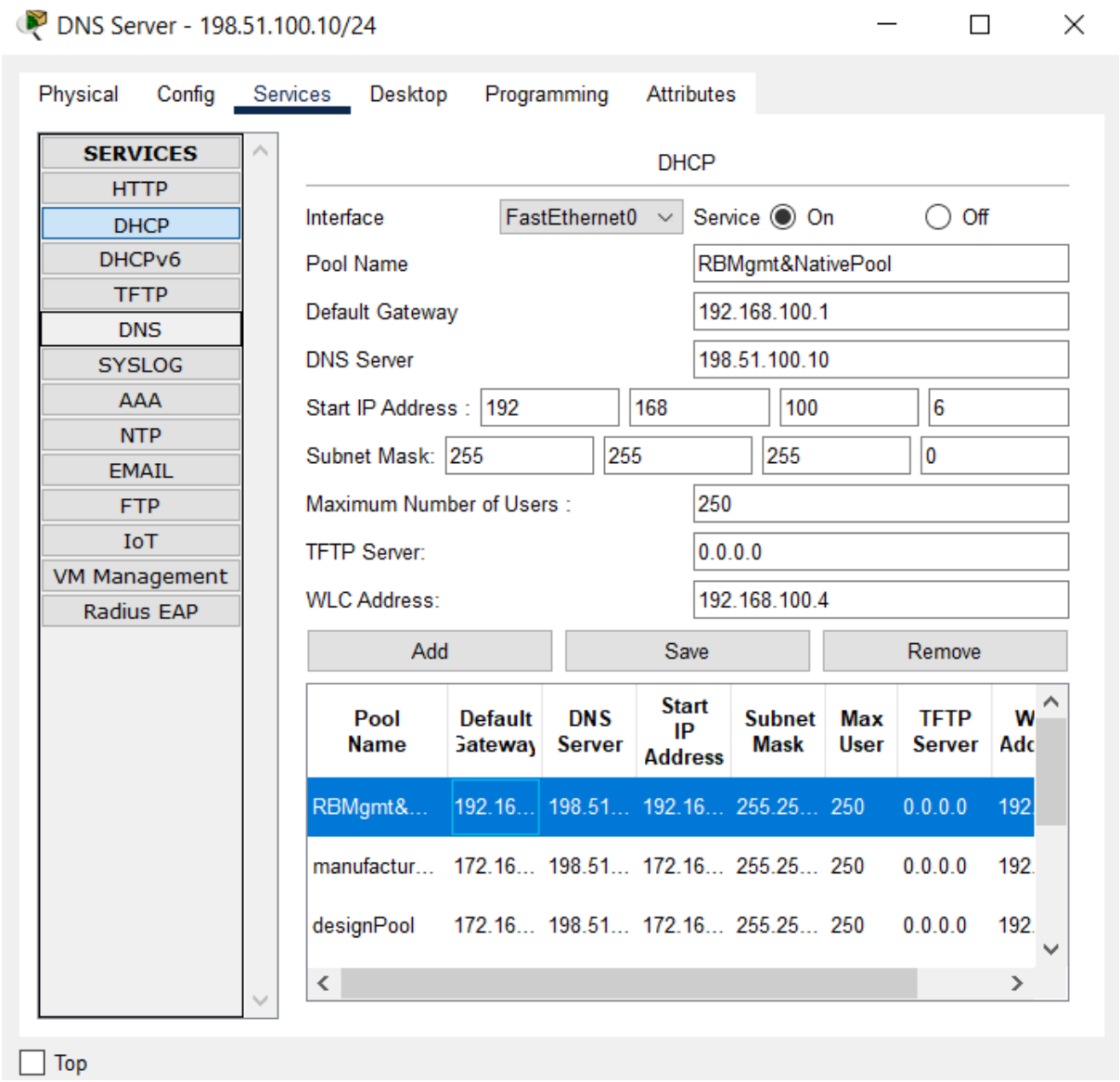

Figure 24 RBMgmt&NativePool

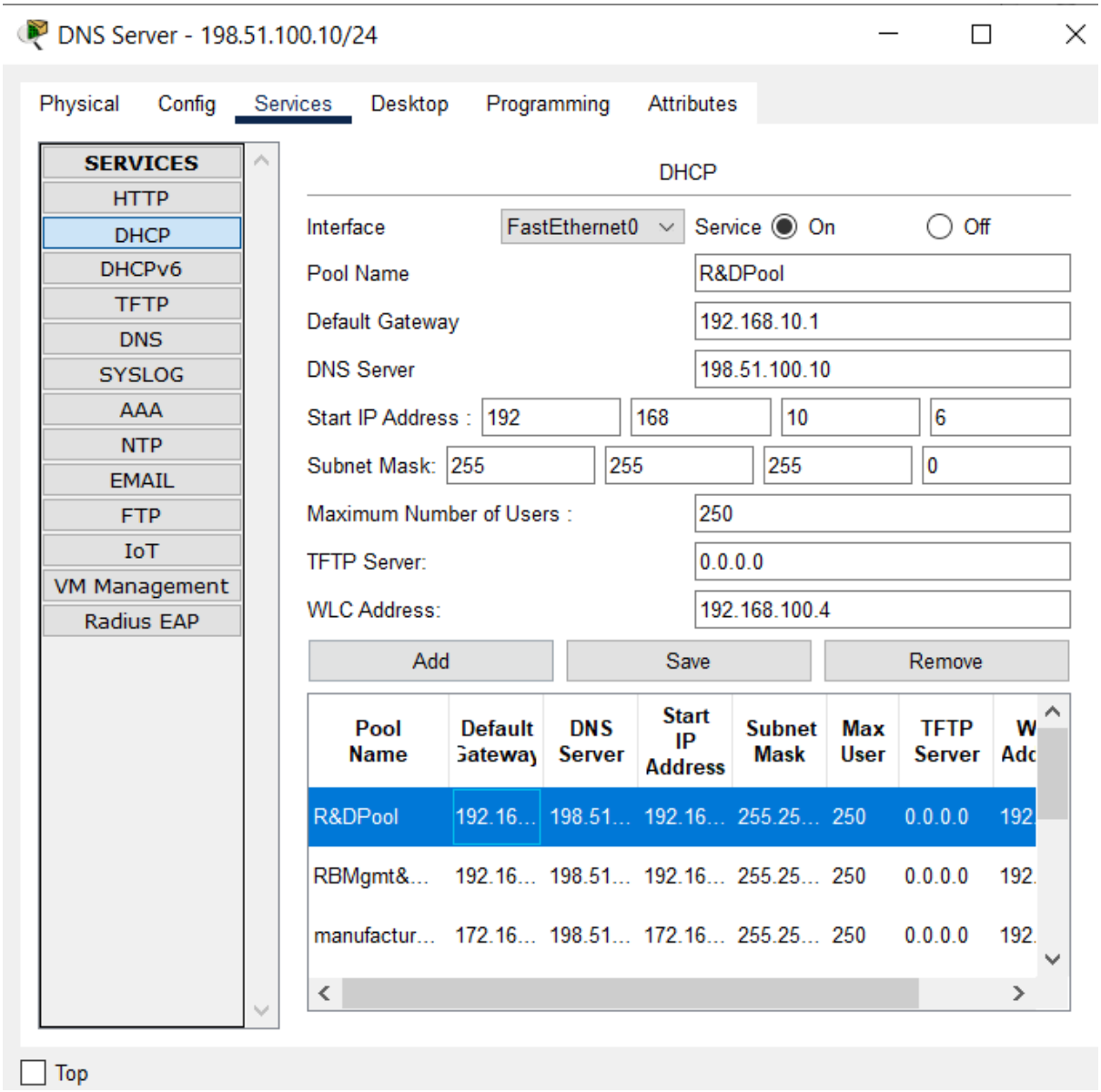

Figure 25 R&DPool

To start DHCP server, the DHCP service is enabled. All required details is given to the DHCP pool. The DHCP can be added, modified, and removed.

IP Helper Address

```
KL_Router(config)#int g0/0.50
KL_Router(config-subif)#ip helper-address 198.51.100.10
KL_Router(config-subif)#int g0/0.11
KL_Router(config-subif)#ip helper-address 198.51.100.10
KL_Router(config-subif)#int g0/0.22
KL_Router(config-subif)#ip helper-address 198.51.100.10
KL_Router(config-subif)#int g0/0.33
KL_Router(config-subif)#ip helper-address 198.51.100.10
KL_Router(config-subif)#do wr
Building configuration...
[OK]
```

Figure 26 KL_Router

```
Hanoi_Router(config)#int g1/0.10
Hanoi_Router(config-subif)#ip helper-address 198.51.100.10
Hanoi_Router(config-subif)#int g1/0.100
Hanoi_Router(config-subif)#ip helper-address 198.51.100.10
Hanoi_Router(config-subif)#do wr
Building configuration...
[OK]
```

Figure 27 Hanoi_Router

On the High Dot Tech network, the "ip helper-address" command helps to identifies the IP address of the DHCP server. There may be up to eight specified addresses. Requests from DHCP clients are sent to all specified server by the DHCP agent (a Hewlett Packard Enterprise Company, n.d.).

4.5 Routing Protocol

Hop count is a routing statistic used by the dynamic routing protocol known as Routing Information Protocol (RIP). This protocol is used to determine the optimum route or best route from a source network to a destination network with the number of routers connected within (GeeksforGeeks, 2022).

Since it is considered to be the best method to connect to a network, the routing table contains the route with the fewest hops. Furthermore, a hop count of 16 is regarded as exceeding the 15-hop RIP limit and being outside of the network's service area (GeeksforGeeks, 2022).

The High Dot Tech Network can regularly share updates due to RIP. Continuous updates will be made to the route data. The routing tables in this upgrade are complete. Routing information obtained from neighbouring routers is often used by routers. Routing on rumours is another name for it (GeeksforGeeks, 2022).

RIP version 2, incorporates subnet mask information in its routing update. The High Dot Tech network uses RIP version 2 on its routers. In its routing update, the "Classless Routing Protocol," or RIP version 2, includes subnet mask information (GeeksforGeeks, 2022).

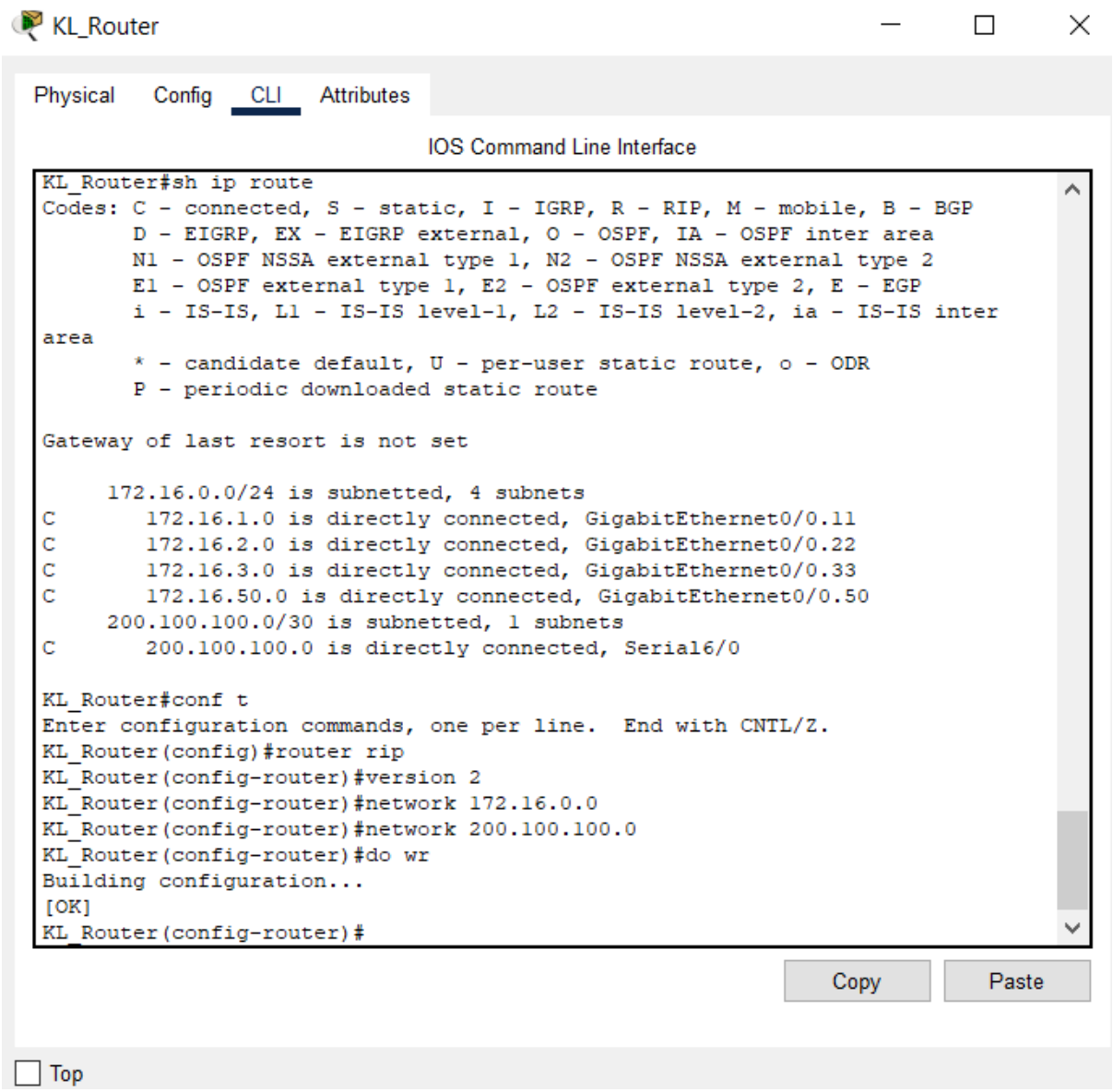

Figure 28 KL_Router

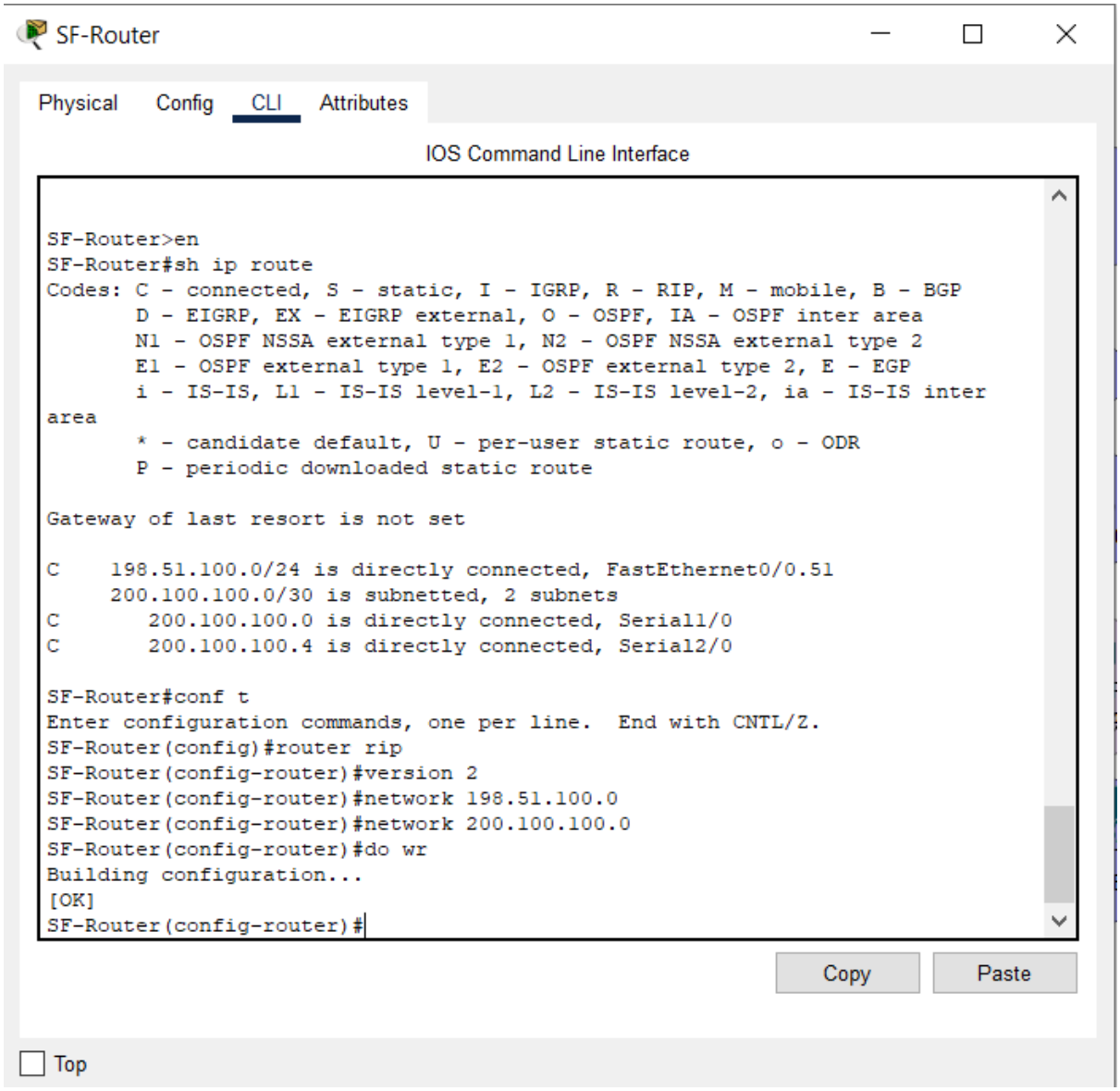

Figure 29 SF-Router

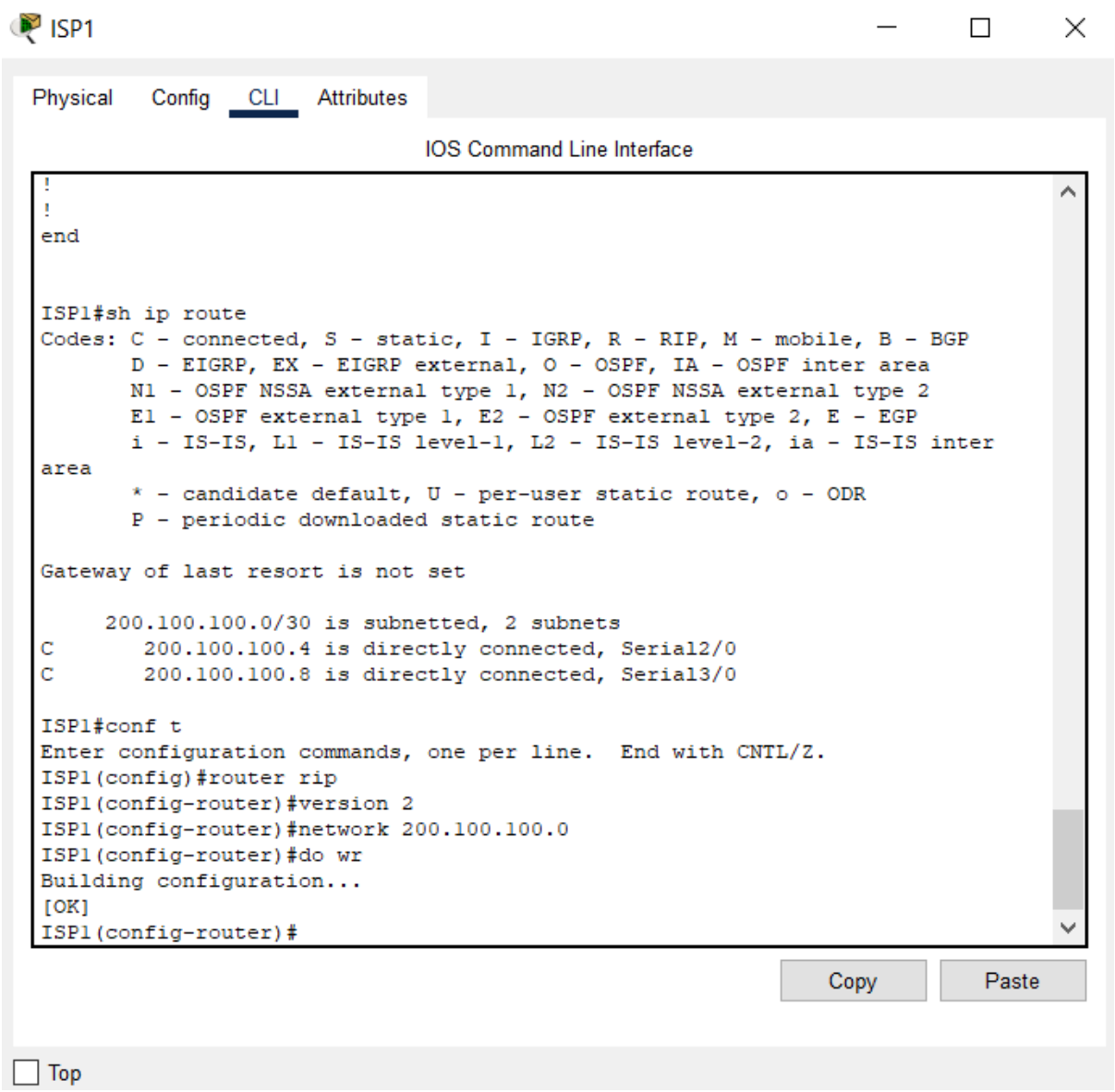

Figure 30 ISP1

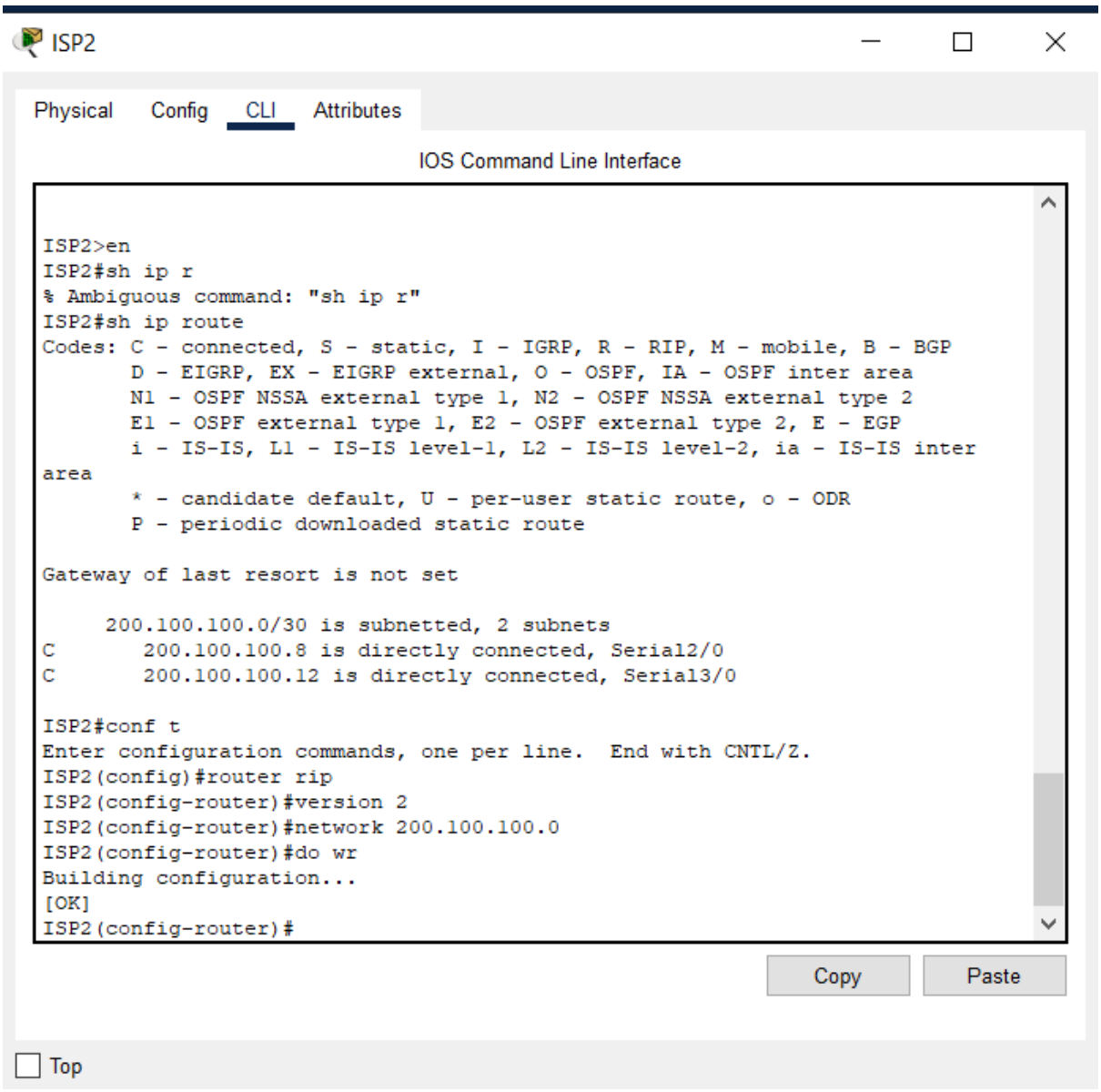

Figure 31 ISP2

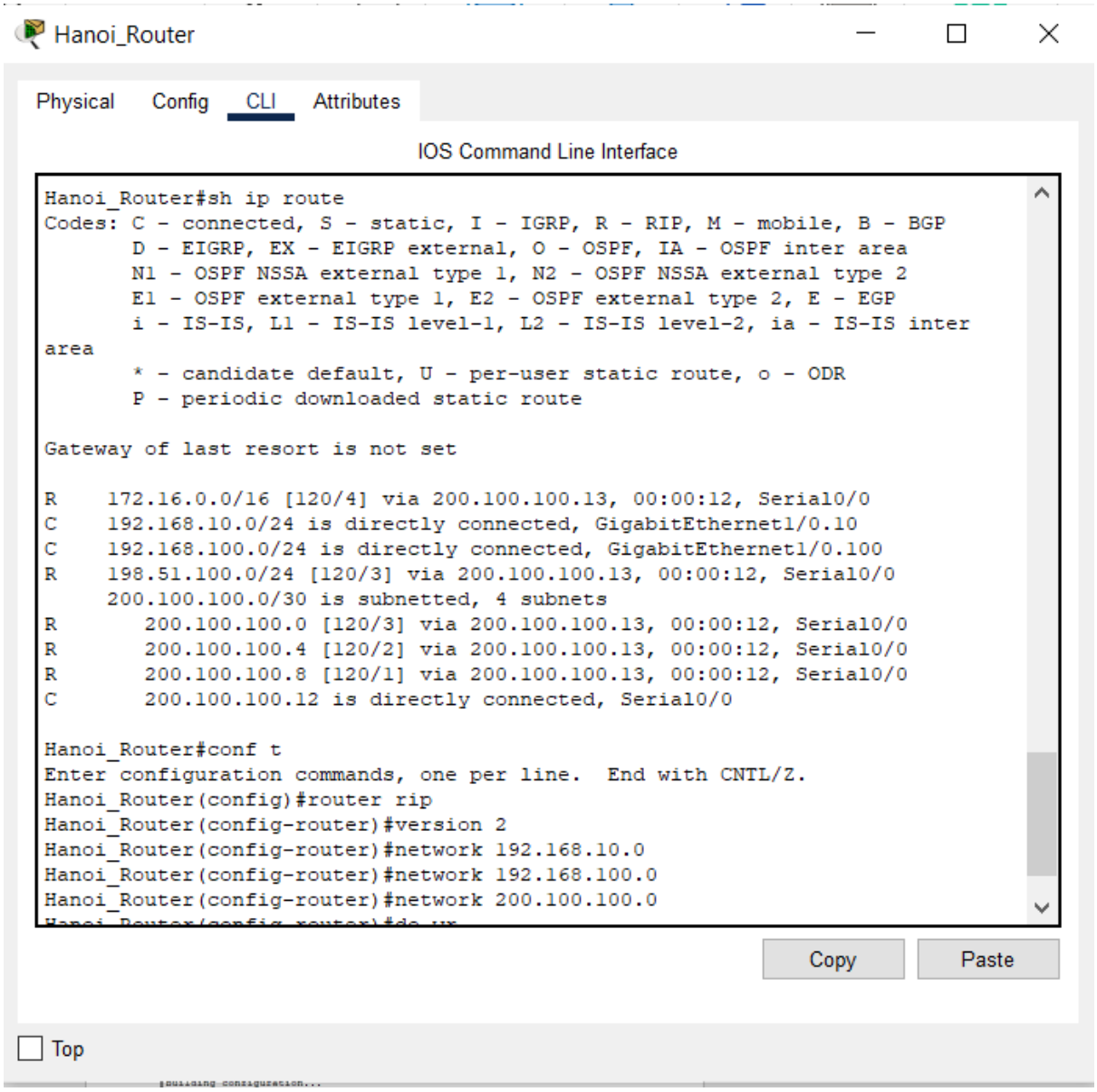

Figure 32 ISP2

The figures above demonstrate how to see connected networks using the "show ip route" command. The commands "router rip" and "version 2" make RIP version 2 available in the routers. The linked network that is shown in the "show ip route" command is configured.

4.6 VLAN

Breaking up High Dot Tech network into smaller network will make it simpler to manage High Dot Tech network. Virtual LANs (VLANs) provide High Dot Tech company flexibility and segmentation. A VLAN allows devices to interact with one another as if they were all connected by the same cable. Instead of using physical connections, VLANs rely on logical connections (Cisco, n.d.).

As shown in the Figure 1 Network Layout of High Dot Tech, users from different departments in High Dot Tech company such as HR, Management, Design, and Manufacture. These departments use VLANs to connect ot the same network regardless of the actual switch being used or where they located inside a LAN (Cisco, n.d.).

Without taking into account the actual physical location of the users or devices, VLANs enable network administrators to divide up their networks depending on the departments. Every VLAN is viewed as a unique logical network. VLANs may be connected to any switch port. Network executives like me may apply access and security controls to certain departments using VLANs (Cisco, n.d.).

Using VLANs in High Dot Tech network had successfully improved the network security. Users may only communicate with each other in the same VLAN. Without the help of the router, only user in the same VLAN can communicate. A security feature on the router, such as an access control list, may be used to limit communication across VLANs (Cisco, n.d.).

VLAN Creation

The figures below show the VLAN creation process in the switches of the High Dot Tech network. The number of VLAN and the name of VLAN is created based on the VLAN table above.

```
HR_SW(config)#vlan 50
HR_SW(config-vlan)#name Management
HR_SW(config-vlan)#vlan 11
HR_SW(config-vlan)#name HR
HR_SW(config-vlan)#do wr
Building configuration...
[OK]
```

```
Design_SW(config)#vlan 22
Design_SW(config-vlan)#name Design
Design_SW(config-vlan)#do wr
Building configuration...
[OK]
```

```
Manufacturer_SW(config)#vlan 33
Manufacturer_SW(config-vlan)#name Manufacturer
Manufacturer_SW(config-vlan)#do wr
Building configuration...
[OK]
```

```
SW_Distributed(config)#vlan 50
SW_Distributed(config-vlan)#name Management
SW_Distributed(config-vlan)#vlan 11
SW_Distributed(config-vlan)#name HR
SW_Distributed(config-vlan)#vlan 22
SW_Distributed(config-vlan)#name Design
SW_Distributed(config-vlan)#vlan 33
SW_Distributed(config-vlan)#name Manufacturer
SW_Distributed(config-vlan)#do wr
Building configuration...
[OK]
```

```
SF-SW(config)#vlan 51
SF-SW(config-vlan)#name ServerFarm
SF-SW(config-vlan)#do wr
Building configuration...
[OK]
```

```
Hanoi-MLayerSW(config)#vlan 10
Hanoi-MLayerSW(config-vlan)#name R&D
Hanoi-MLayerSW(config-vlan)#vlan 100
Hanoi-MLayerSW(config-vlan)#name RBMgmt&Native
Hanoi-MLayerSW(config-vlan)#do wr
Building configuration...
[OK]
```

Create the VLANs of High Dot Tech network with the respective VLAN id. After creating the VLAN, the name of the VLAN is specified accordingly. For example, the VLAN n 10 is created, then the name of “R&D” is given to the VLAN.

VLAN Port Assignment

The figures below show how the switchport is assigned in the High Dot Tech network. The switchport mode assignment shown below will be the access mode follow by giving the VLAN number. The switchport which are configured with access mode can only be connected to one VLAN.

```
HR_SW(config)#int f0/3
HR_SW(config-if)#switchport mode access
HR_SW(config-if)#switchport access vlan 50
HR_SW(config-if)#ex
```

```
HR_SW(config)#int range f0/4-6
HR_SW(config-if-range)#switchport mode access
HR_SW(config-if-range)#switchport access vlan 11
HR_SW(config-if-range)#ex
```

```
Design_SW(config)#int range f0/4-6
Design_SW(config-if-range)#switchport mode access
Design_SW(config-if-range)#switchport access vlan 22
Design_SW(config-if-range)#ex
```

```
Manufacturer_SW(config)#int range f0/3-5
Manufacturer_SW(config-if-range)#switchport mode access
Manufacturer_SW(config-if-range)#switchport access vlan 33
Manufacturer_SW(config-if-range)#no shut
```

```
SF-SW(config)#int range f0/1-3
SF-SW(config-if-range)#switchport mode access
SF-SW(config-if-range)#switchport access vlan 51
SF-SW(config-if-range)#ex
```

```
Hanoi-MLayerSW(config)#int range f0/1-3
Hanoi-MLayerSW(config-if-range)#switchport mode access
Hanoi-MLayerSW(config-if-range)#switchport access vlan 10
Hanoi-MLayerSW(config-if-range)#ex
Hanoi-MLayerSW(config)#int range f0/4-5
Hanoi-MLayerSW(config-if-range)#switchport mode access
Hanoi-MLayerSW(config-if-range)#switchport access vlan 100
Hanoi-MLayerSW(config-if-range)#ex
```

VLAN configuration takes place on the switch port rather than the end device. VLAN-specific IP addresses and subnet masks are configured on switch ports for end devices. As shown in figures above, the VLAN is also specified in the interfaces. The ports that are not trunk and not shutdown will be configured with access mode. Also, the ports assigned must only connect to a vlan.

Results

The figures below show the lists of VLAN in the switches of High Dot Tech network. This is used to check if the created VLAN exist in the switch.

```
Password:
Hanoi-MLayerSW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
10   R&D                              active    Fa0/1, Fa0/2, Fa0/3
100  RBMgmt&Native                    active    Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
SW_Distributed#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- ---------
------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14,
Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18,
Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22,
Fa0/23
                                                Fa0/24, Gig0/2
11   HR                               active
22   Design                           active
33   Manufacturer                     active
50   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
HR_SW#sh vlan bri

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1,
Gig0/2
11   HR                                active    Fa0/4, Fa0/5, Fa0/6
50   Management                        active    Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
Design_SW#sh vlan bri

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1,
Gig0/2
22   Design                            active    Fa0/4, Fa0/5, Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
Manufacturer_SW#sh vlan bri

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24,
Gig0/1
                                                 Gig0/2
33   Manufacturer                      active    Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

SF-SW#sh vlan bri

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                 Gig0/1, Gig0/2
51   ServerFarm                        active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Trunk Configurations

The figures below show the trunk port assigned to the ports of the switches. Unlike access ports, the trunk ports in the switches can support more than one VLANs. By assigning trunk ports, the trunk native VLAN is also configured to VLAN 100.

```
HR_SW(config)#int range f0/1-2
HR_SW(config-if-range)#switchport mode trunk
HR_SW(config-if-range)#switchport trunk native vlan 100
```

```
Design_SW(config)#int range fa0/1-3
Design_SW(config-if-range)#switchport mode trunk
Design_SW(config-if-range)#switchport trunk native vlan 100
Design_SW(config-if-range)#do wr
Building configuration...
[OK]
```

```
Manufacturer_SW(config)#int range f0/1-2
Manufacturer_SW(config-if-range)#
Manufacturer_SW(config-if-range)#switchport mode trunk

Manufacturer_SW(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

Manufacturer_SW(config-if-range)#switchport trunk native vlan 100
Manufacturer_SW(config-if-range)#
```

```
SW_Distributed(config)#int range f0/1-3, g0/1
SW_Distributed(config-if-range)#switchport mode trunk
SW_Distributed(config-if-range)#switchport trunk native vlan 100
SW_Distributed(config-if-range)#do wr
Building configuration...
[OK]
```

```
SF-SW(config)#int f0/4
SF-SW(config-if)#switchport mode trunk

SF-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up

SF-SW(config-if)#switchport trunk native vlan 100
SF-SW(config-if)#ex
SF-SW(config)#ex
```

```
Hanoi-MLayerSW(config)#int range g0/1-2
Hanoi-MLayerSW(config-if-range)#switchport trunk encapsulation dot1Q
Hanoi-MLayerSW(config-if-range)#switchport mode trunk
Hanoi-MLayerSW(config-if-range)#switchport trunk native vlan 100
Hanoi-MLayerSW(config-if-range)#ex
```

A Layer 2 connection between two switches known as a "VLAN trunk", delivers traffic for all VLANs. In the interface, the port will be configured as trunk port. VLAN 100 is now the native VLAN. The Cisco Catalyst 2960 switches are used by every switch in the High Dot Tech network, and they all feature 802.1Q encapsulation on trunk lines. Due to the fact that the 802.1Q encapsulation on trunk connections is not automatic, the Multilayer Switch's "switchport trunk encapsulation dot1Q" has to be specified.

Results

```
SW_Distributed#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100
Fa0/3       on           802.1q         trunking      100
Gig0/1      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,11,22,33,50
Fa0/2       1,11,22,33,50
Fa0/3       1,11,22,33,50
Gig0/1      1,11,22,33,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,11,22,33,50
Fa0/2       11,22,33,50
Fa0/3       1,11,22,33,50
Gig0/1      1,11,22,33,50
```

```
HR_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,11,50
Fa0/2       1,11,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       11,50
Fa0/2       1,11,50
```

```
Design_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100
Fa0/3       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,22
Fa0/2       1,22
Fa0/3       1,22

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,22
Fa0/2       1,22
Fa0/3       1,22
```

```
Manufacturer_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,33
Fa0/2       1,33

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,33
Fa0/2       1,33
```

```
Hanoi-MLayerSW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      100
Gig0/2      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,100
Gig0/2      1,10,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,100
Gig0/2      1,10,100

SF-SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/4       1,51

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       1,51
```

4.7 Inter VLAN Routing

Switched Layer 2 networks of High Dot Tech company are segmented using VLANs to separate the departments. Without a router or Layer 3 switch to offer routing services, hosts in one VLAN are unable to connect with those in another VLAN. Network traffic may be sent from one VLAN to another via inter-VLAN routing.

Router-on-a-Stick

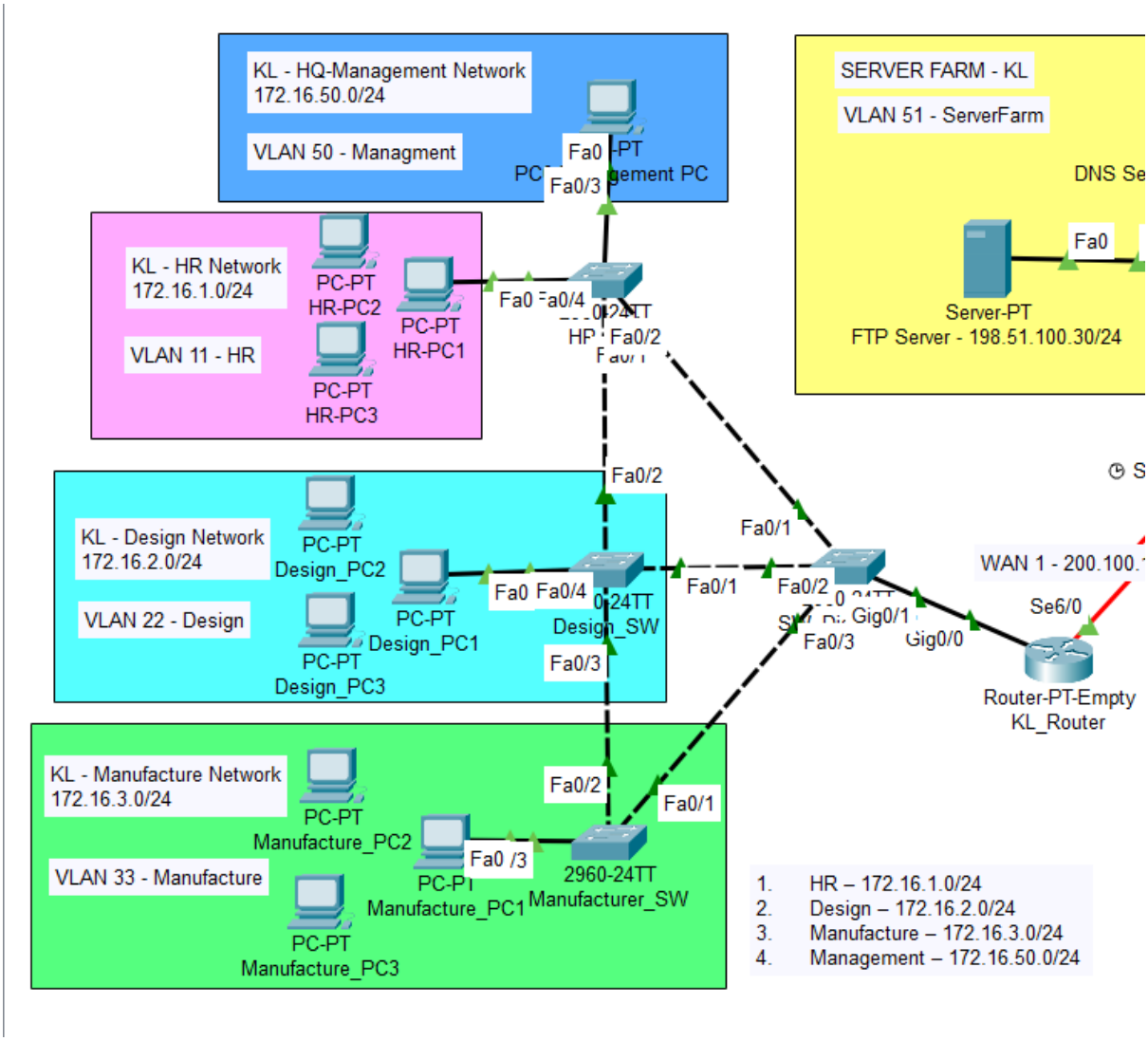

Figure 33 Router-on-a-stick

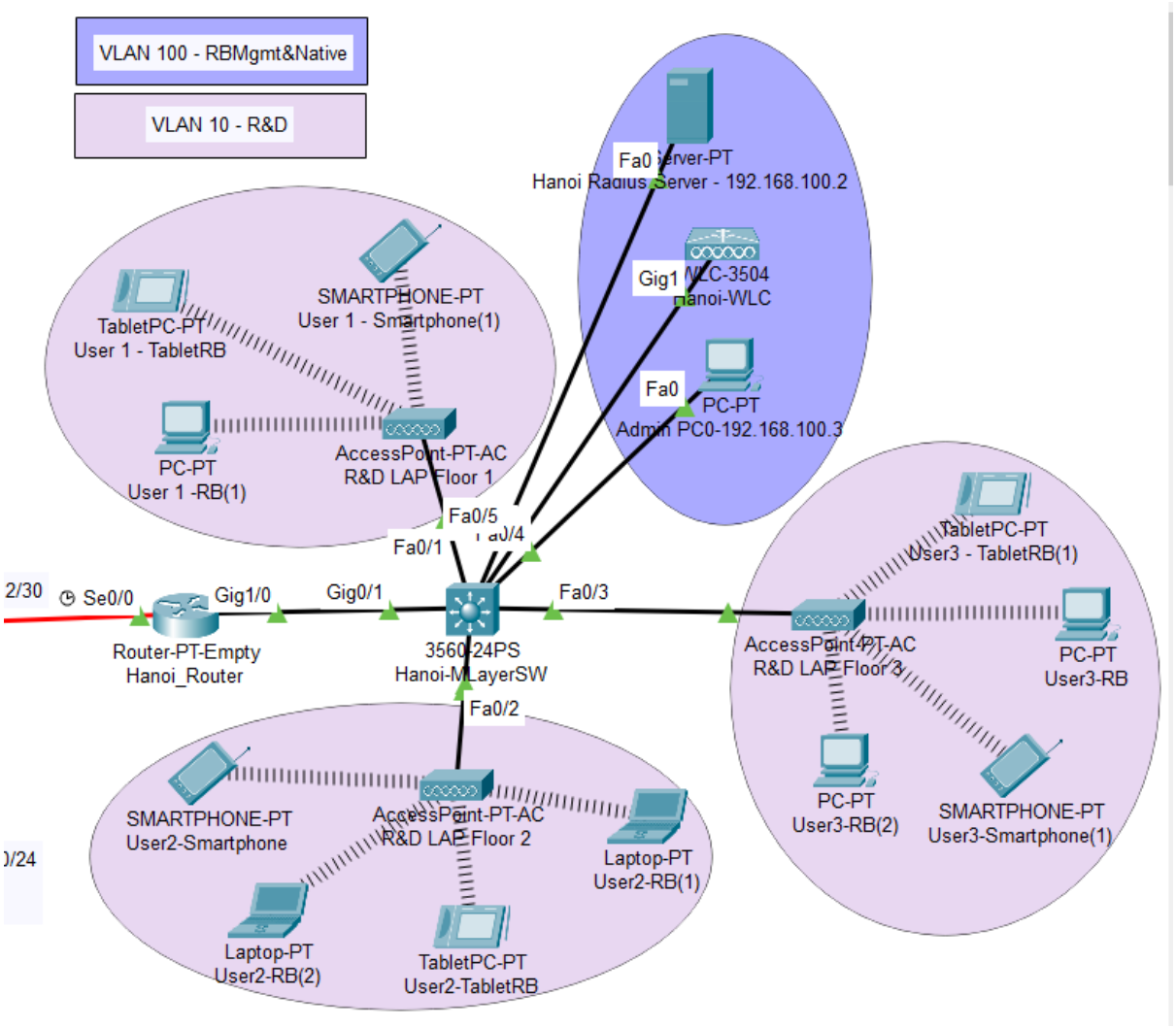

Figure 34 Router-on-a-stick

The KL network and Hanoi network of the High Dot Tech company employs Router-on-a-Stick inter-VLAN routing. The disadvantages of the prior inter-VLAN routing method is removed by the "router-on-a-stick" inter-VLAN routing strategy (Cisco, n.d.).

A Cisco IOS router is connected to a Layer 2 switch's trunk port and has its Ethernet interface set up as an 802.1Q trunk for the High Dot Tech network. To distinguish routable VLANs, subinterfaces are specially established on the router interface. The Ethernet interface of a Cisco IOS router is configured as an 802.1Q trunk for the High Dot Tech network and is attached to a Layer 2 switch's trunk port. Subinterfaces are specifically formed on the router interface to identify routable VLANs (Cisco, n.d.).

Software-based interfaces make up the virtual interfaces that have been set up. Each one has been given a single physical Ethernet port. Subinterface configuration is made possible by a router's software. A distinct VLAN designation and IP address are given to each

subinterface. According to each subnet's assigned VLAN, subinterfaces are set up for that subnet. This facilitates logical routing (Cisco, n.d.).

Traffic with a VLAN tag is received by the VLAN subinterface and sent to the router interface. After deciding on a routing path with the destination IP network address given, the router would chooses the exit interface for the traffic. The data are transmitted back out the physical interface while being VLAN-tagged with the new VLAN if the exit interface is configured as an 802.Q subinterface (Cisco, n.d.).

Router Sub interface Configuration

The figures below show the step to configure subinterfaces in routers of the High Dot Tech network. For example, “g0/0” is an interface and “g0/0.50”, “g0/0.11”, “g0/0.22”, and “g0/0.33” are the sub interfaces.

KL_Router

Physical Config CLI Attributes

```
Enter configuration commands, one per line.  End with CNTL/Z.
KL_Router(config)#int g0/0
KL_Router(config-if)#no shut

KL_Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

KL_Router(config-if)#int g0/0.50
KL_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

KL_Router(config-subif)#encapsulation dot1Q 50
KL_Router(config-subif)#ip address 172.16.50.1 255.255.255.0
KL_Router(config-subif)#ex
KL_Router(config)#int g0/0.11
KL_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.11, changed state to up

KL_Router(config-subif)#encapsulation dot1Q 11
KL_Router(config-subif)#ip address 172.16.1.1 255.255.255.0
KL_Router(config-subif)#int g0/0.22
KL_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.22, changed state to up

KL_Router(config-subif)#encapsulation dot1Q 22
KL_Router(config-subif)#ip address 172.16.2.1 255.255.255.0
KL_Router(config-subif)#int g0/0.33
KL_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.33, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.33, changed state to up

KL_Router(config-subif)#encapsulation dot1Q 33
KL_Router(config-subif)#ip address 172.16.3.1 255.255.255.0
KL_Router(config-subif)#ex
KL_Router(config)#ex
KL_Router#
%SYS-5-CONFIG_I: Configured from console by console

KL_Router#cop r st
Destination filename [startup-config]?
Building configuration...
[OK]
KL_Router#
```

Top

Figure 35 KL_Router

```
Hanoi_Router(config)#int g1/0
Hanoi_Router(config-if)#no shut

Hanoi_Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

Hanoi_Router(config-if)#int g1/0.10
Hanoi_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.10, changed state to up

Hanoi_Router(config-subif)#encapsulation dot1Q 10
Hanoi_Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Hanoi_Router(config-subif)#ex
Hanoi_Router(config)#int g1/0.100
Hanoi_Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.100, changed state to up

Hanoi_Router(config-subif)#encapsulation dot1Q 100 native
Hanoi_Router(config-subif)#ip address 192.168.100.1 255.255.255.0
Hanoi_Router(config-subif)#ex
Hanoi_Router(config)#ex
```

Figure 36 Hanoi_Router

```
Hanoi_Router#cop r st
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
SF-Router(config)#int f0/0
SF-Router(config-if)#no shut
SF-Router(config-if)#int f0/0.51
SF-Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.51, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.51, changed
state to up

SF-Router(config-subif)#encapsulation dot1Q 51
SF-Router(config-subif)#ip address 198.51.100.1 255.255.255.0
SF-Router(config-subif)#ex
SF-Router(config)#ex
SF-Router#
%SYS-5-CONFIG_I: Configured from console by console

SF-Router#cop r st
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 37 SF-Router

IP address, subnet mask, dot1Q encapsulation, and VLAN are all specified on the router sub interface. After that, the management interface needs to be created which is VLAN 100. Then, the access ports and trunk ports is configured.

Verification

The figures below show the configured result of the VLAN and Inter-VLAN routing.

```
KL_Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.1.0 is directly connected, GigabitEthernet0/0.11
C       172.16.2.0 is directly connected, GigabitEthernet0/0.22
C       172.16.3.0 is directly connected, GigabitEthernet0/0.33
C       172.16.50.0 is directly connected, GigabitEthernet0/0.50
R    192.168.10.0/24 [120/4] via 200.100.100.2, 00:00:25, Serial6/0
R    192.168.100.0/24 [120/4] via 200.100.100.2, 00:00:25, Serial6/0
R    198.51.100.0/24 [120/1] via 200.100.100.2, 00:00:25, Serial6/0
     200.100.100.0/30 is subnetted, 4 subnets
C       200.100.100.0 is directly connected, Serial6/0
R       200.100.100.4 [120/1] via 200.100.100.2, 00:00:25, Serial6/0
R       200.100.100.8 [120/2] via 200.100.100.2, 00:00:25, Serial6/0
R       200.100.100.12 [120/3] via 200.100.100.2, 00:00:25, Serial6/0

KL_Router#sh ip int bri
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.11  172.16.1.1      YES manual up                    up
GigabitEthernet0/0.22  172.16.2.1      YES manual up                    up
GigabitEthernet0/0.33  172.16.3.1      YES manual up                    up
GigabitEthernet0/0.50  172.16.50.1     YES manual up                    up
Serial6/0              200.100.100.1   YES manual up                    up
Serial7/0              unassigned      YES unset  administratively down down
```

Figure 38 KL-Router

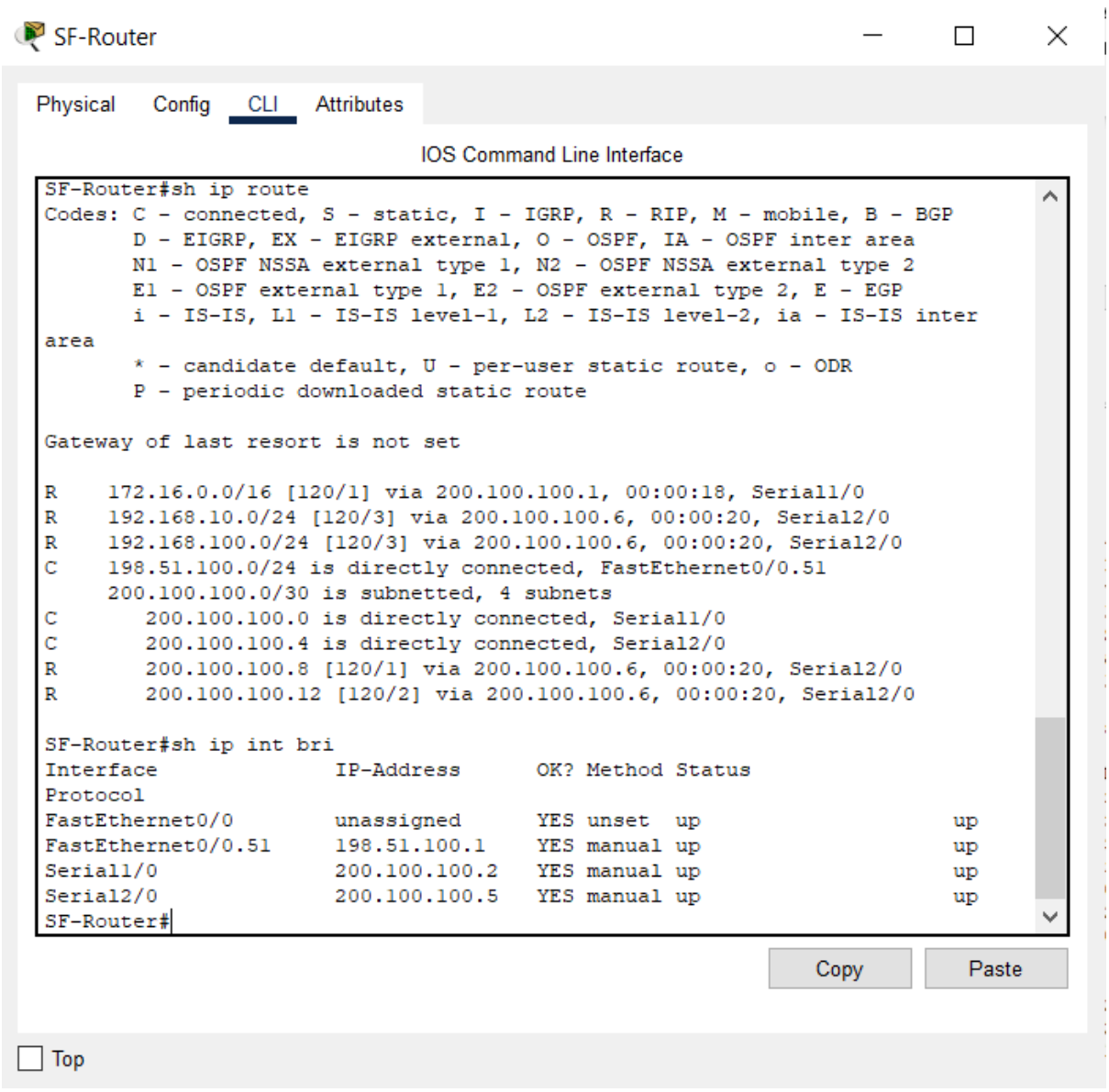

Figure 39 SF-Router

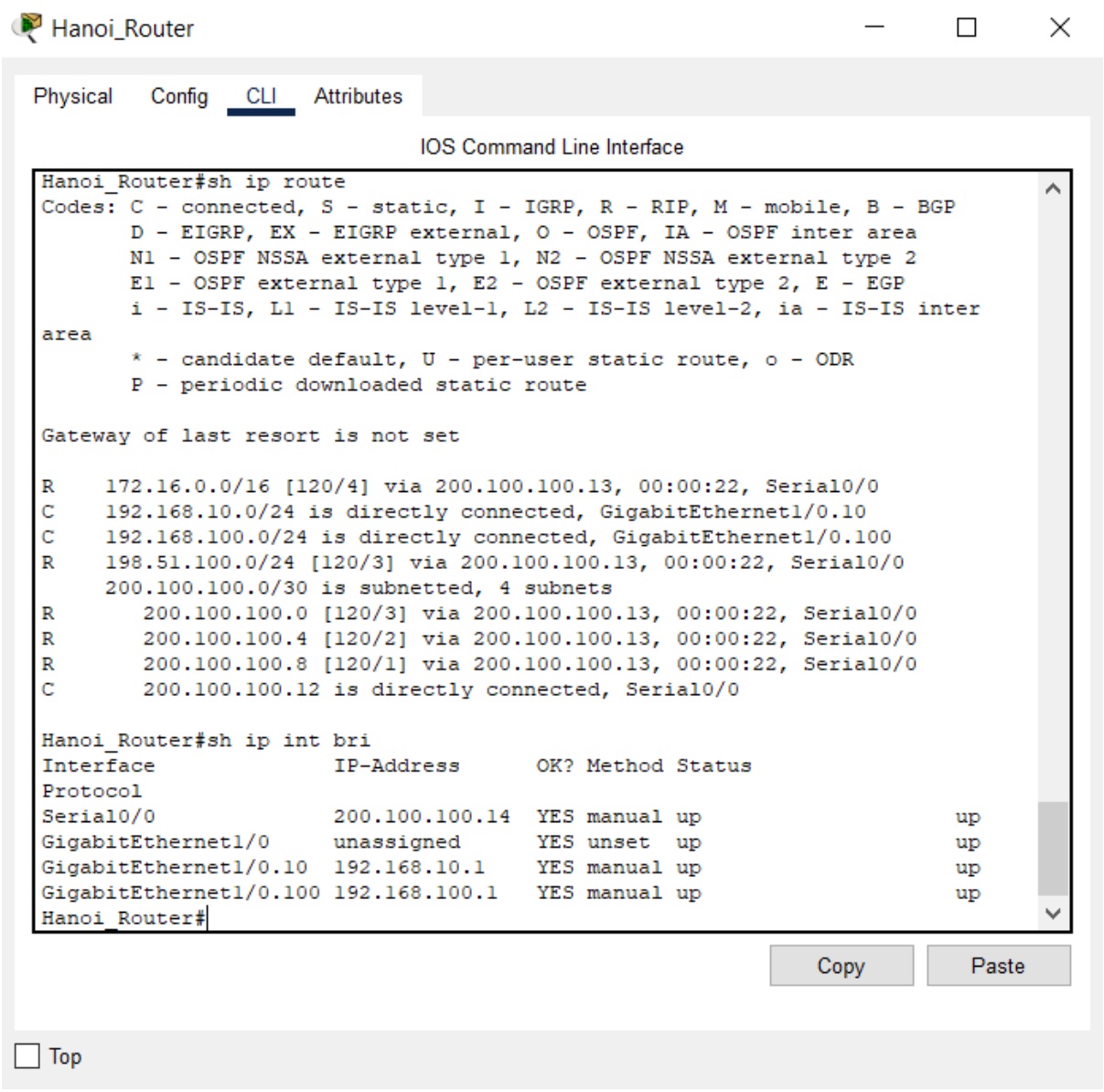

Figure 40 Hanoi_Router

5.0 Layer 2 Security Mechanisms Deployment in configuration.

To enhance the security of the Layer 2 of High Dot Tech network. The port security and secure shell is enabled in the High Dot Tech network.

5.1 Port Security

The figures below show how the port security is enabled in the High Dot Tech network. The port security will be enabled on the switch access ports.

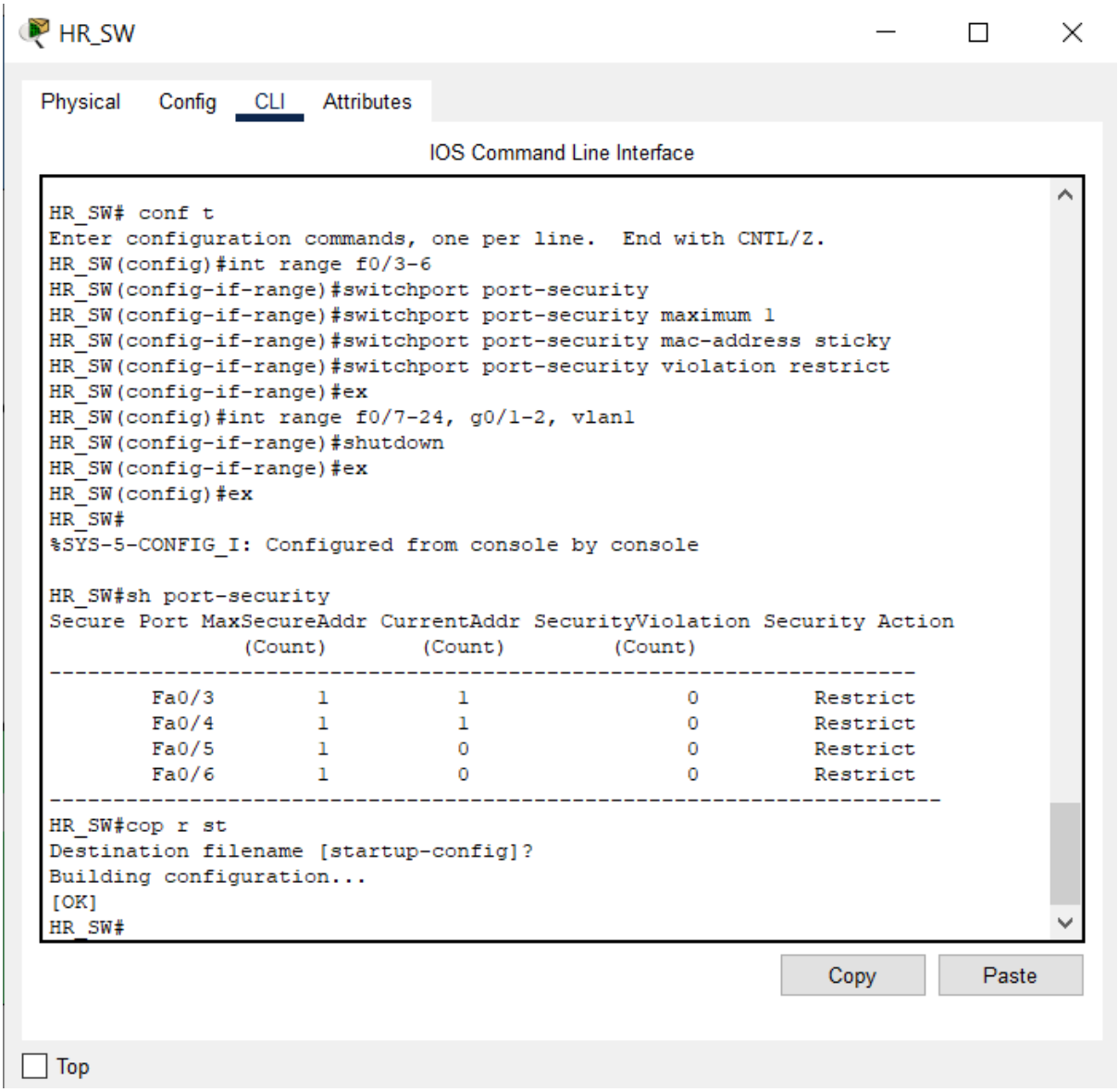

Figure 41 HR-SW

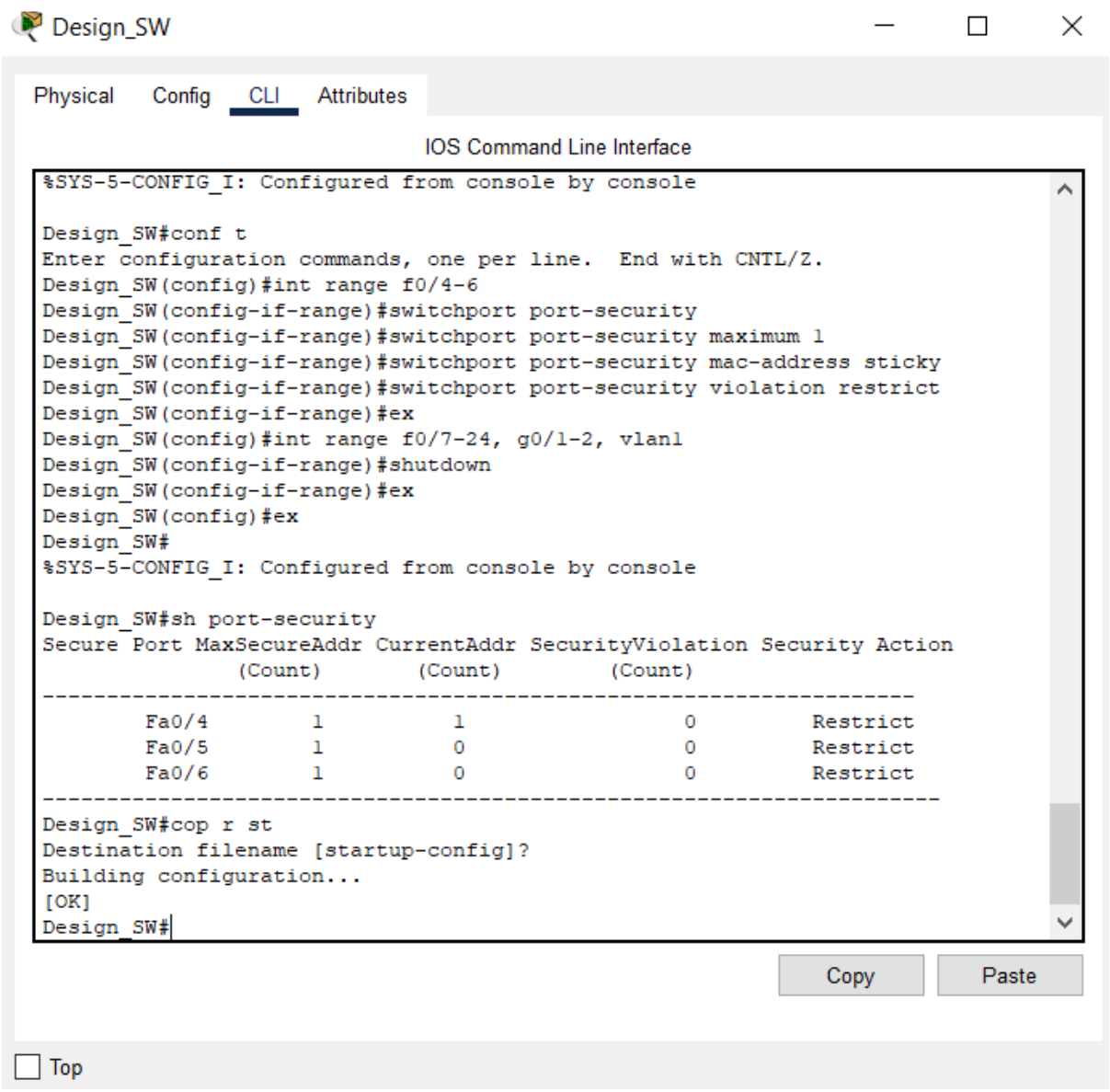

Figure 42 Design-SW

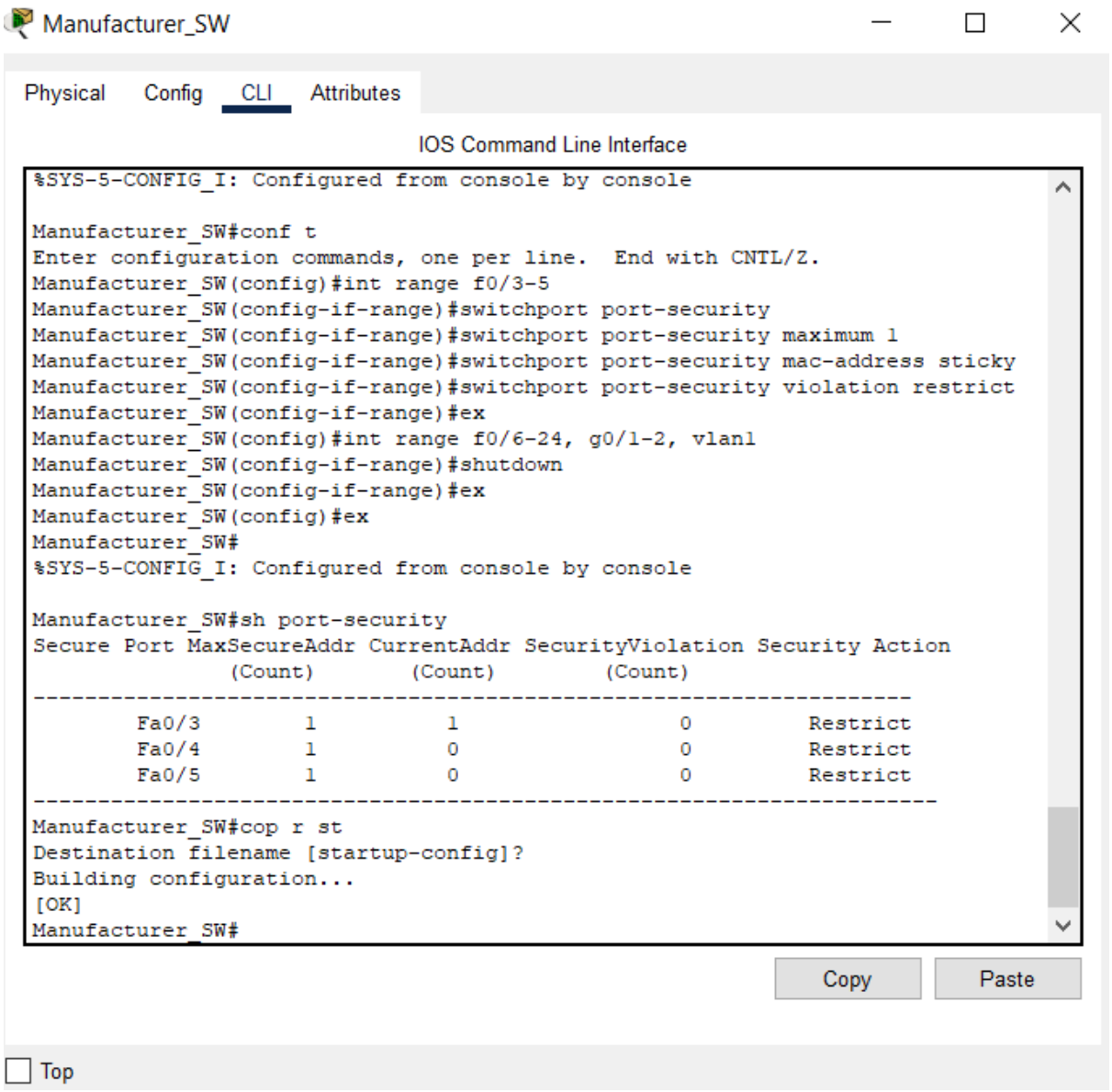

Figure 43 Manufacture-SW

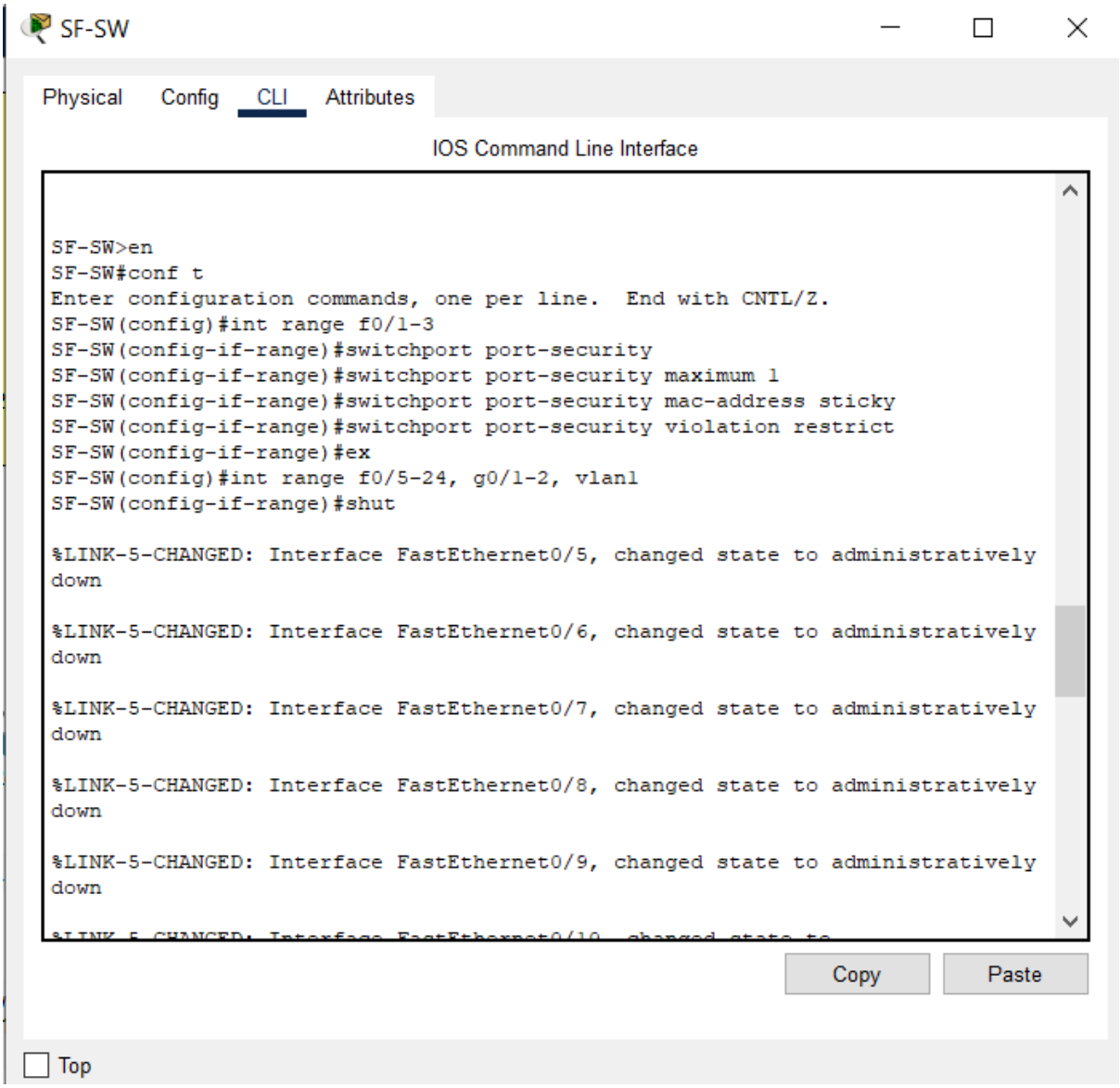

Figure 44 SF-SW

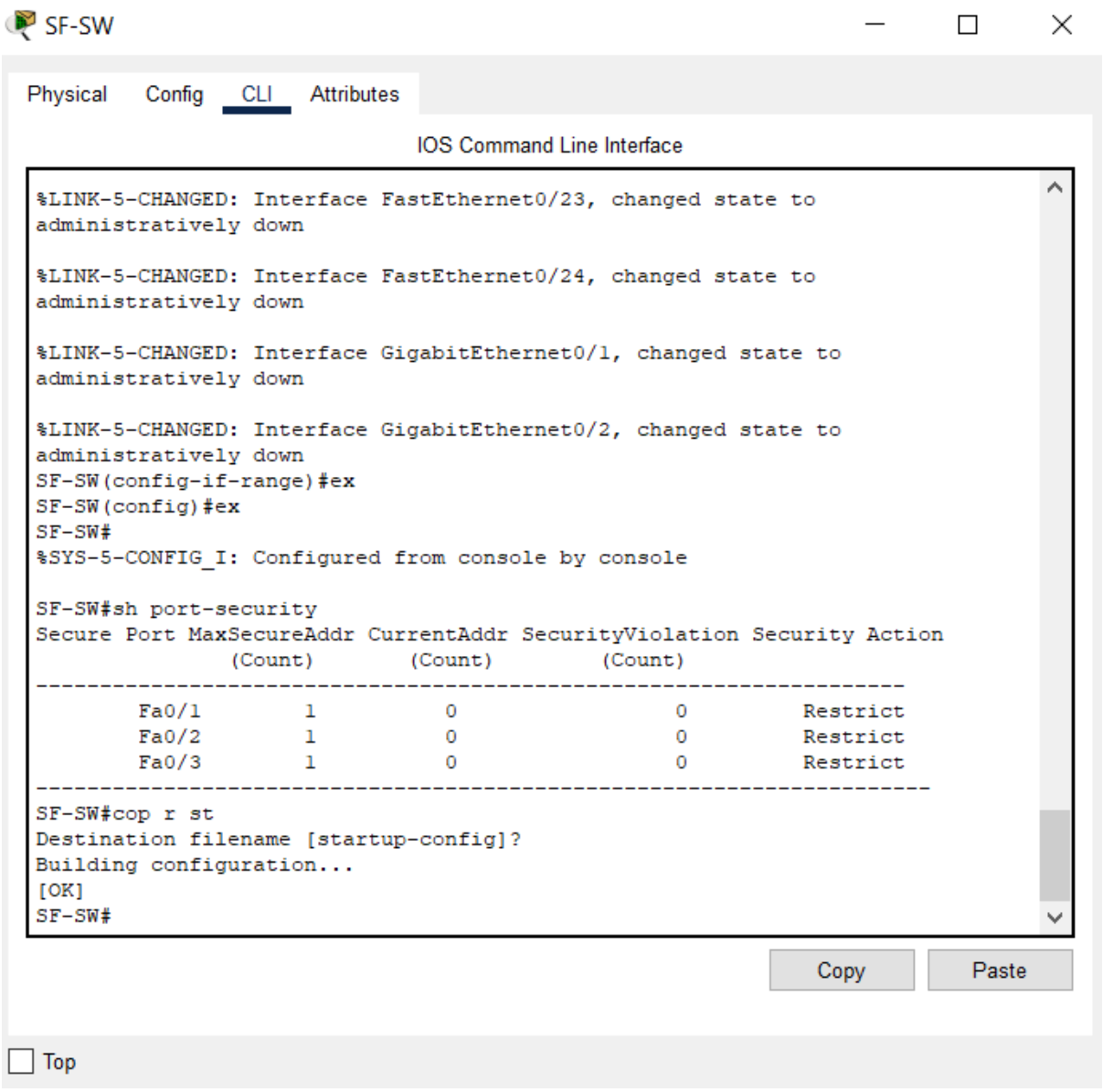

Figure 45 SF-SW

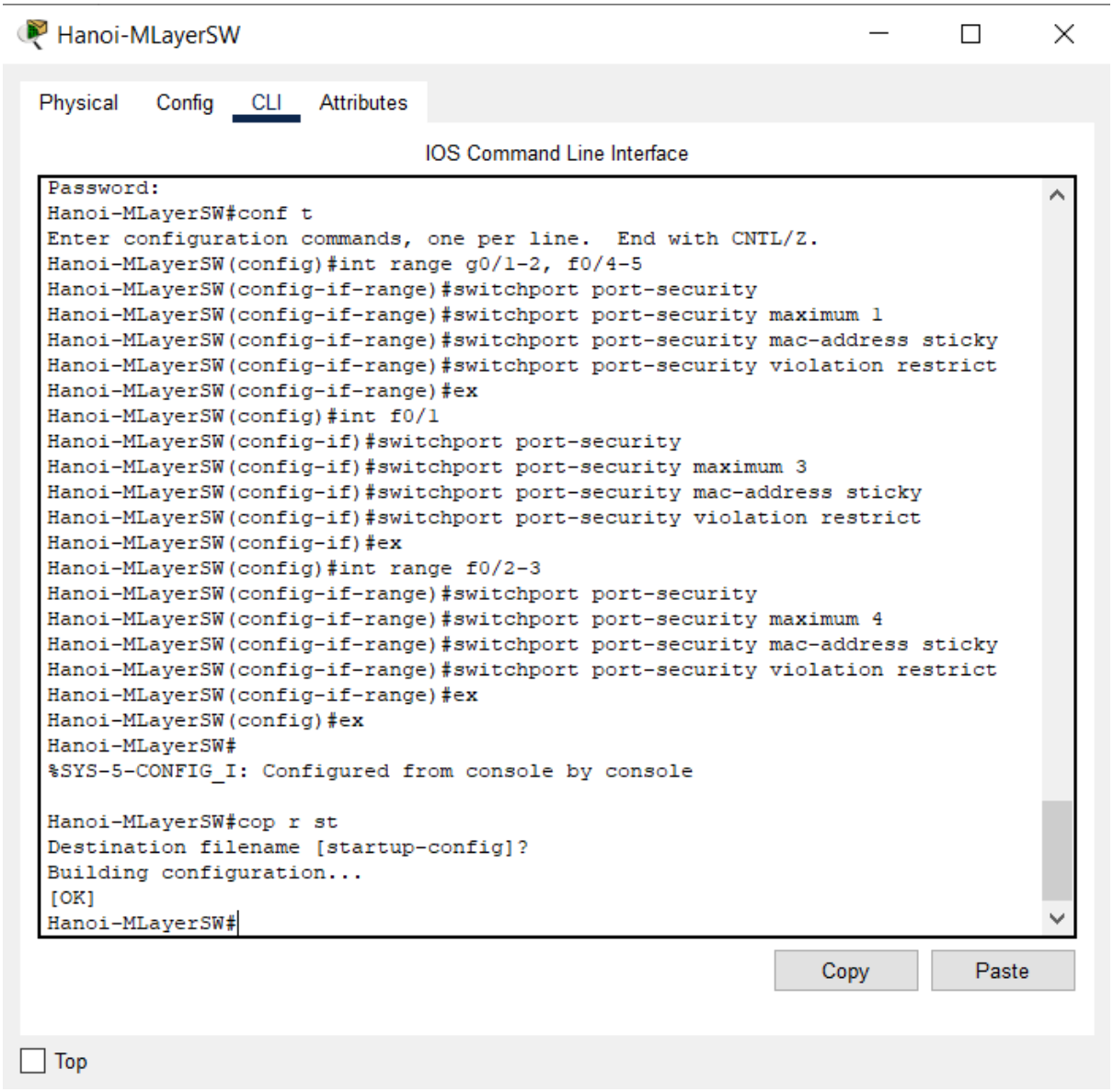

Figure 46 Hanoi-MLayerSW

The port security is enabled on the switch ports with switchport mode access. There may be a maximum number of secure mac addresses set as the required mac-address of the network. For example, the Hanoi-MLayerSw has different amount of maximum mac-address due to the wireless LAN includes the end devices. The mac-address is configured to stick to the current configuration since its mode is set to sticky. After the maximum number of mac-addresses is achieved, the violation mode is configured to restrict where mac-address will not be learned. The unused ports will all be closed.

As shown in the figure above, the number of maximum mac-address needs to be focus as wrong maximum number of mac-address assigned will cause issues. Especially for the end devices

which connects to the access points, the number maximum mac-address should be equal or bigger than the number of the end devices that are connected to the access points.

Verification

The figures below show the interfaces of the Hanoi-MLayerSW switch. This switch is configured with the respective switchport mode. The ports which only connects to one VLAN will be assigned as access ports. Other ports that connects to different VLANs will be assigned as trunk ports.

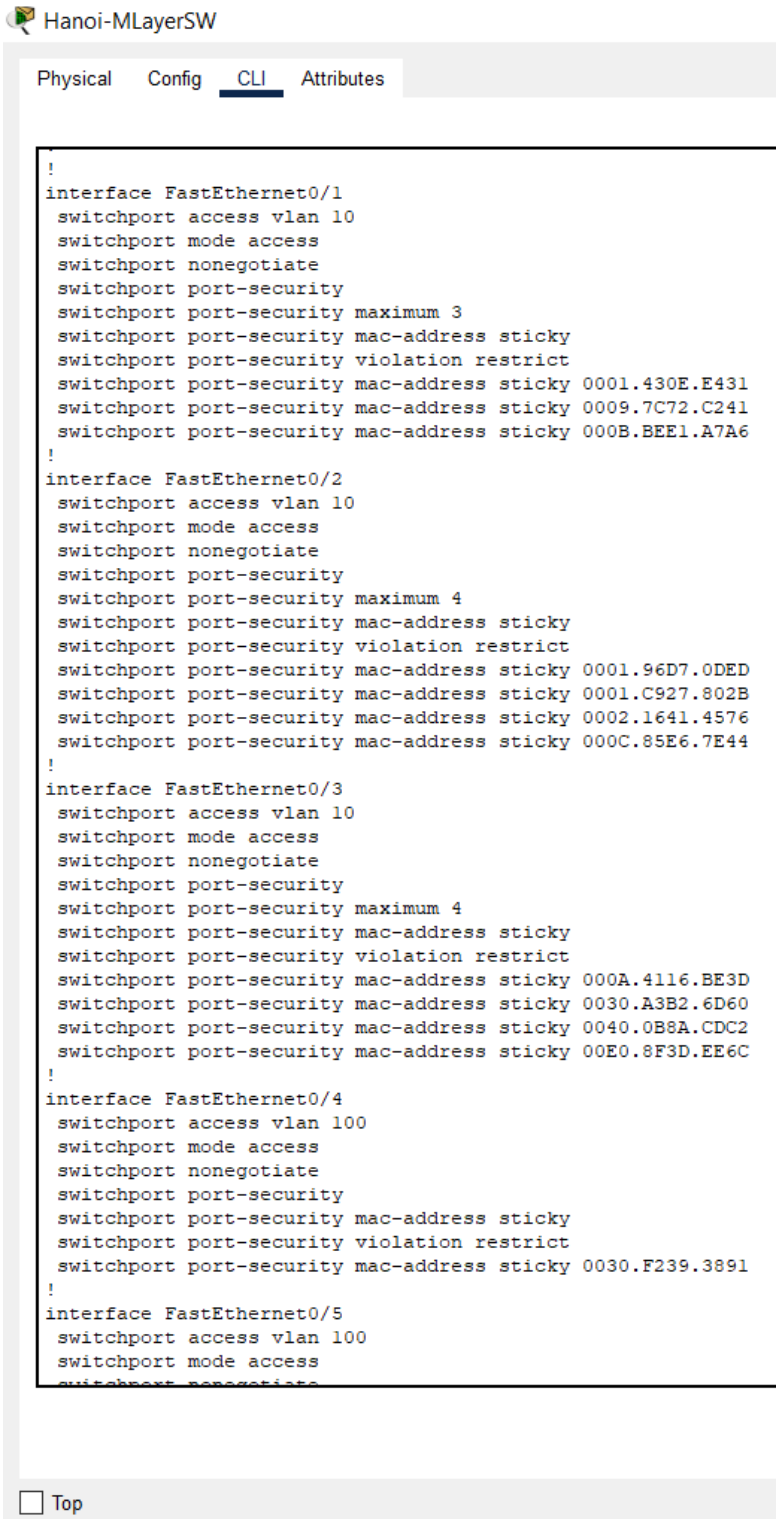

Figure 47 Hanoi-MLayerSW

Figure 48 Hanoi-MLayerSW

Hanoi-MLayerSW

Physical Config CLI Attributes

```
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0004.9AAA.75DA
!
interface GigabitEthernet0/2
 switchport trunk native vlan 100
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

Top

Figure 49 Hanoi-MLayerSW

5.2 Secure Shell (SSH)

Secure Shell (SSH) protocol offers a safe and encrypted connection for administration to a distant device. Telnets need to be replaced by SSH for administration connections. By encrypting data transferred between communication devices and when a device is approved, SSH provides security for distant connections. The switches and routers that connect to the LAN in the High Dot Tech network will be configured with a username and password (Cisco, n.d.). The SSH is configured on all the switches and routers that are connected with the LAN in High Dot Tech network.

```
KL_Router(config)#ip domain-name highdottech.com
```

Figure 50 IP domain name

All Ip domain name is configured as “highdottech.com” with the command shown above.

```
KL_Router(config)#crypto key generate rsa
The name for the keys will be: KL_Router.highdottech.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Figure 51 Generate RSA

The command above is used to generate the RSA key. Then the SSH, will be enables in the router or switch configured. The bit of the modulus is set to 1024.

```
KL_Router(config)#username admin password cisco
*Mar 1 3:12:35.664: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Figure 52 Authentication

The username and password is created in the switches or routers configured.

```
SW_Distributed(config)#line vty 0 15
SW_Distributed(config-line)#transport input ssh
SW_Distributed(config-line)#login local
SW_Distributed(config-line)#exit
```

Figure 53 vty lines

The vty lines from 0 to 15 is configured so the SSH is also enabled in the vty lines. The router or switches are also configured to require authentication.

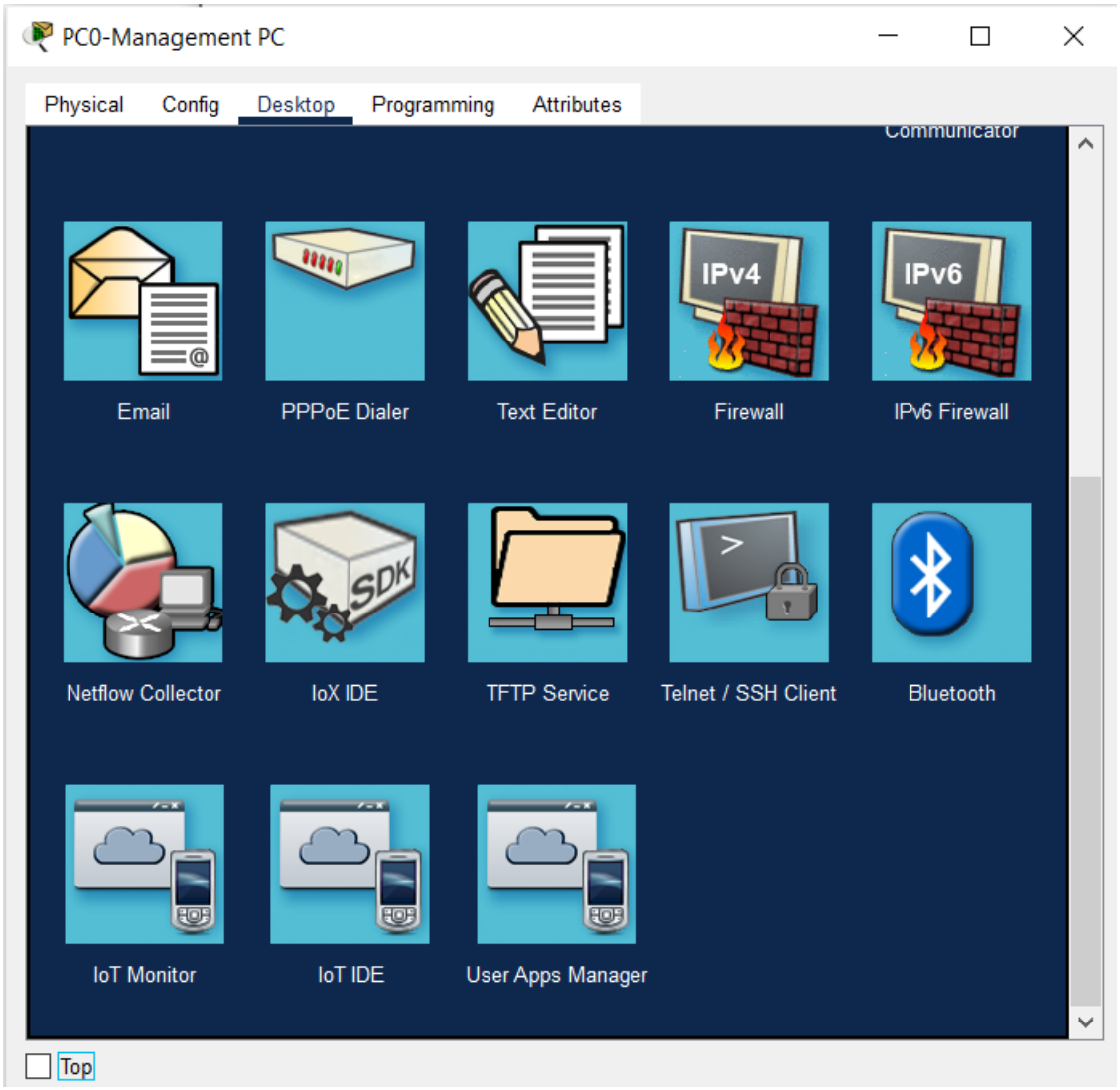

Figure 54 Telnet/SSH Client

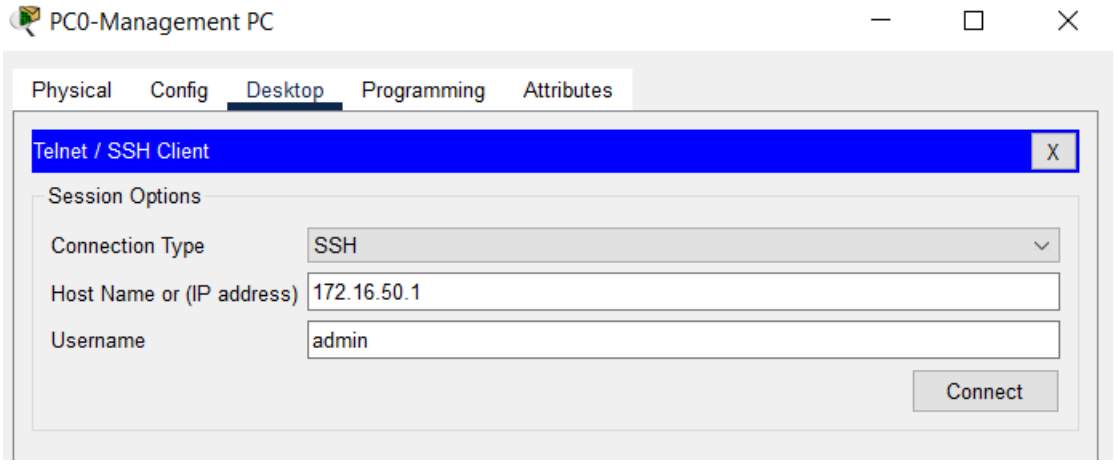

Figure 55 Telnet/SSH Client

The “Telnet/SSH Client” is chosen in the Desktop tab and the figures above shows the step to connect SSH by giving the gateway IP and the username configured.

SSH Client

After clicking on “Connect” button, enter the correct password and the router can be accessed. As shown in the figure below, the hostname is the hostname of the router which indicates the router is connected.

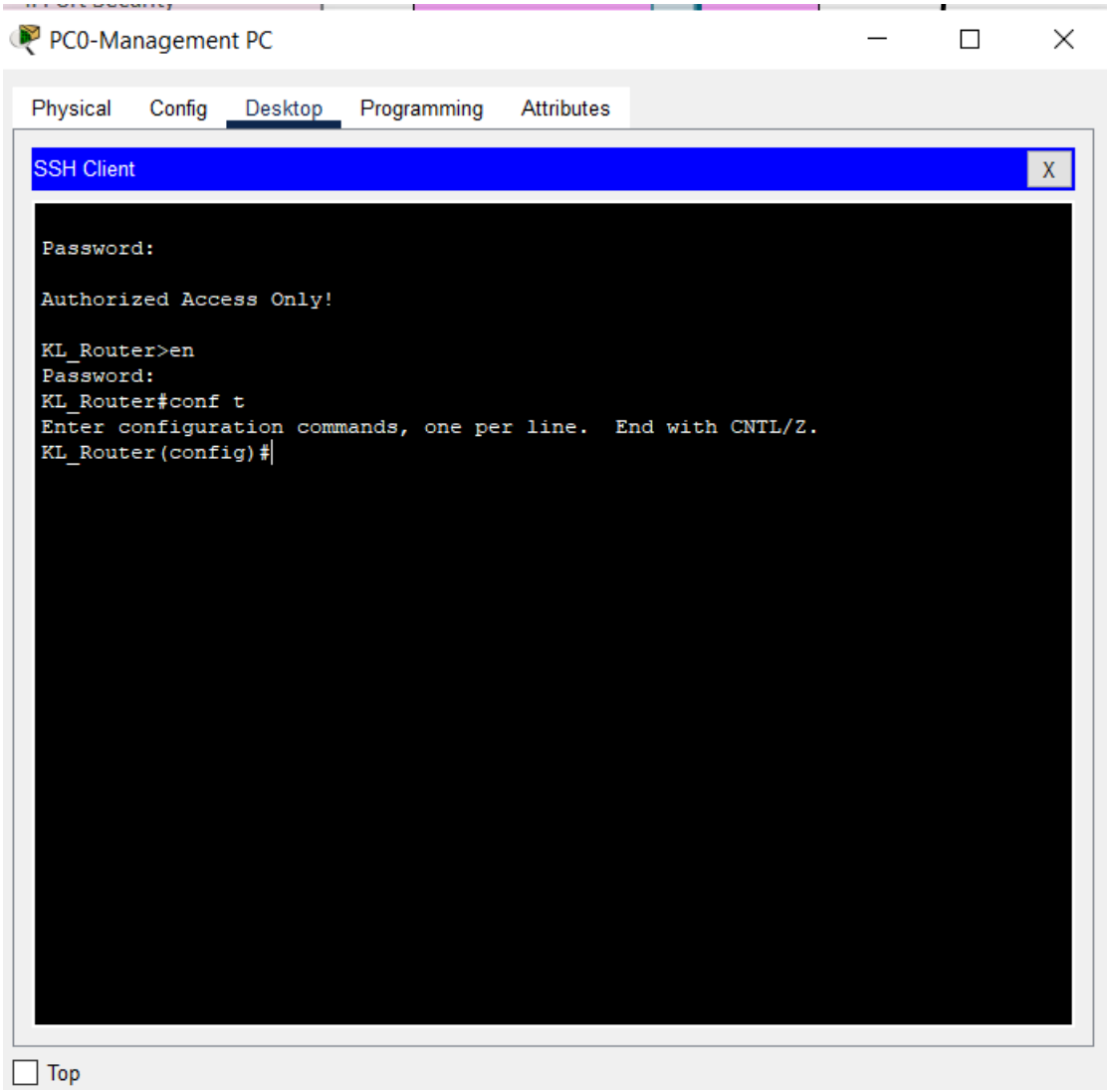

Figure 56 PC0-Managment PC

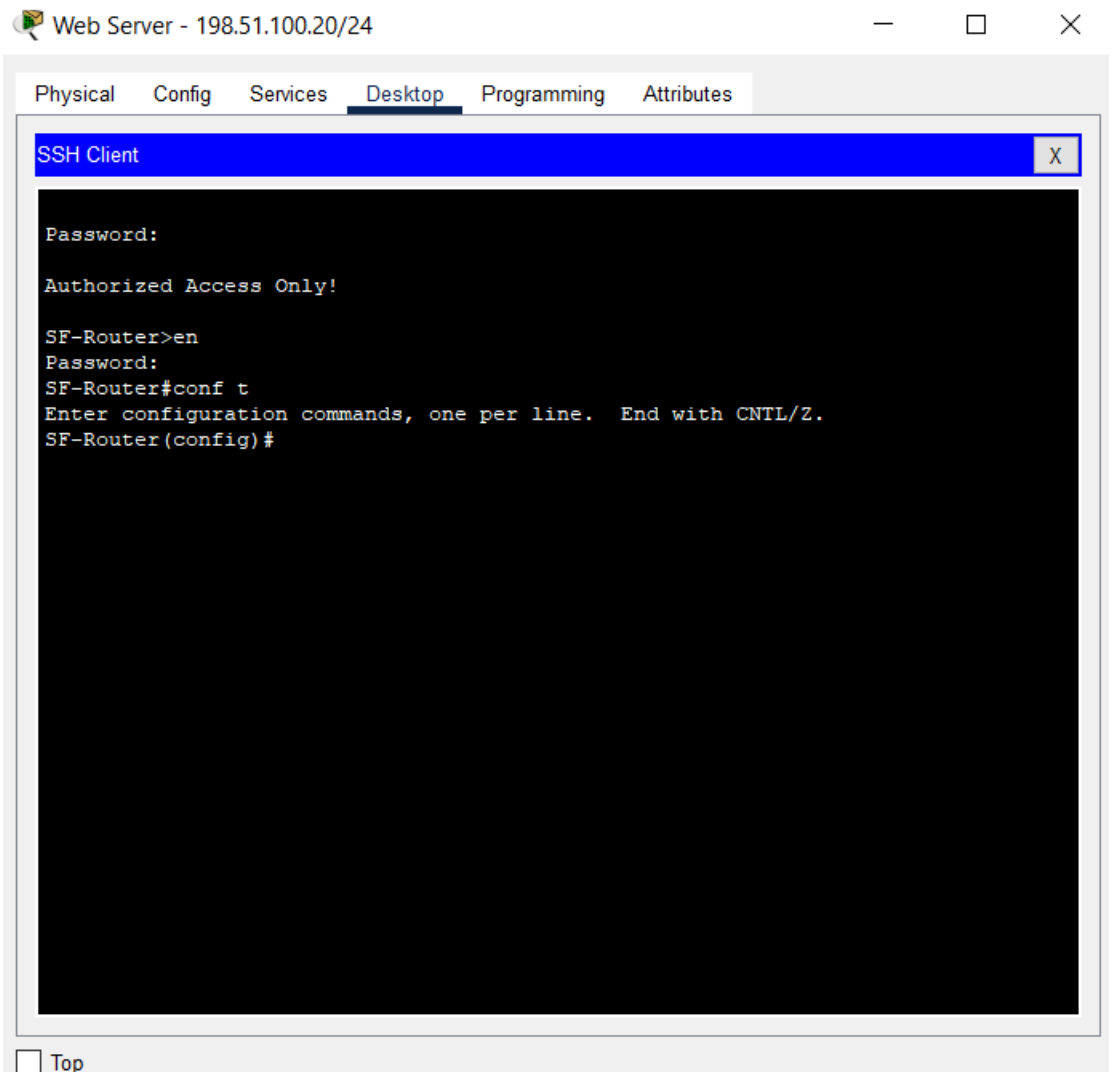

Figure 57 Web Server

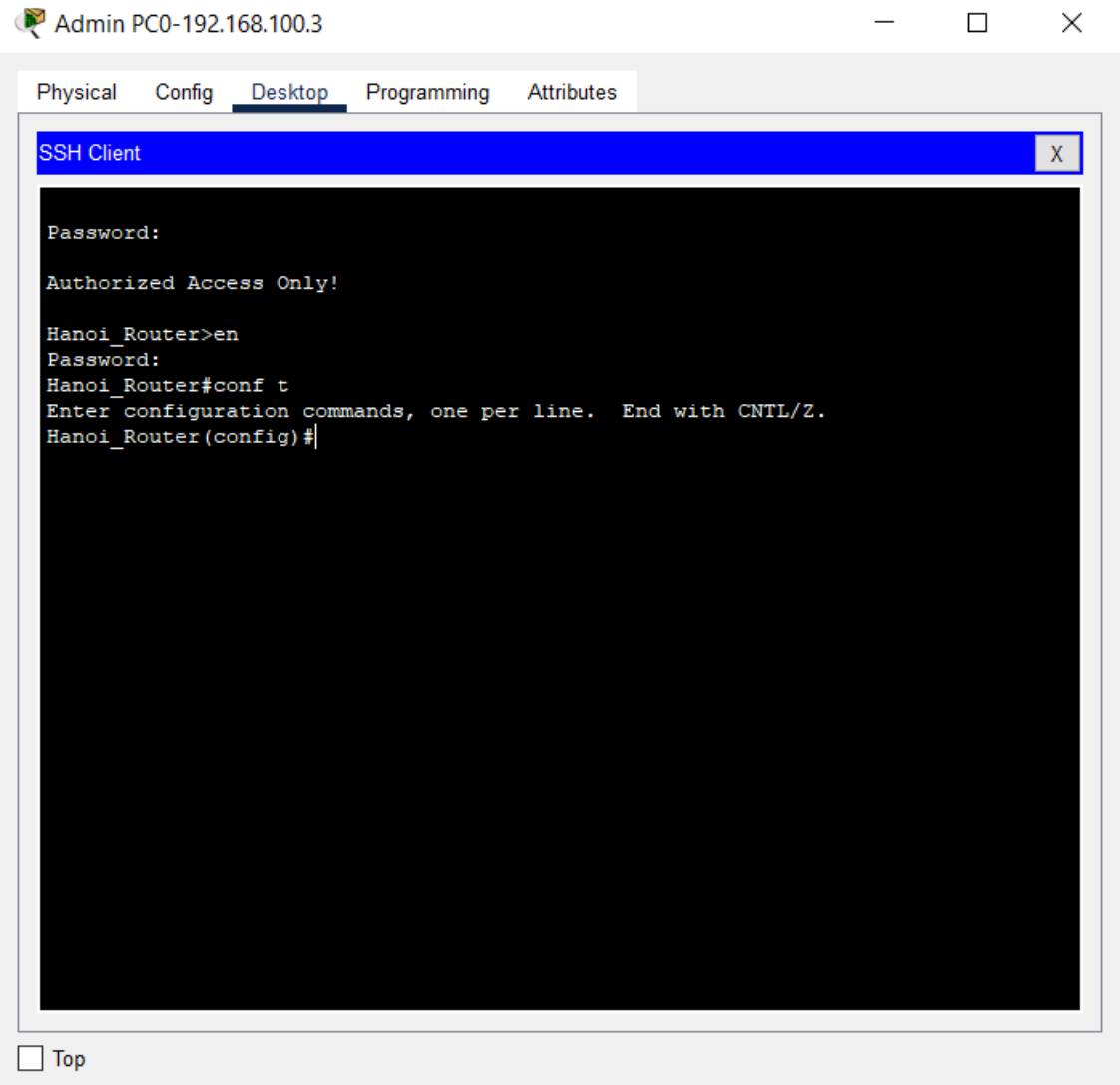

Figure 58 Admin PC0

Command Prompt

The figures below shows that the routers can also be accessed through the command prompt by entering accurate username and Ip address. As shown in the figures below, I have entered the password accurately and I am able to enter. This action is done on the LANs to check the SSH.

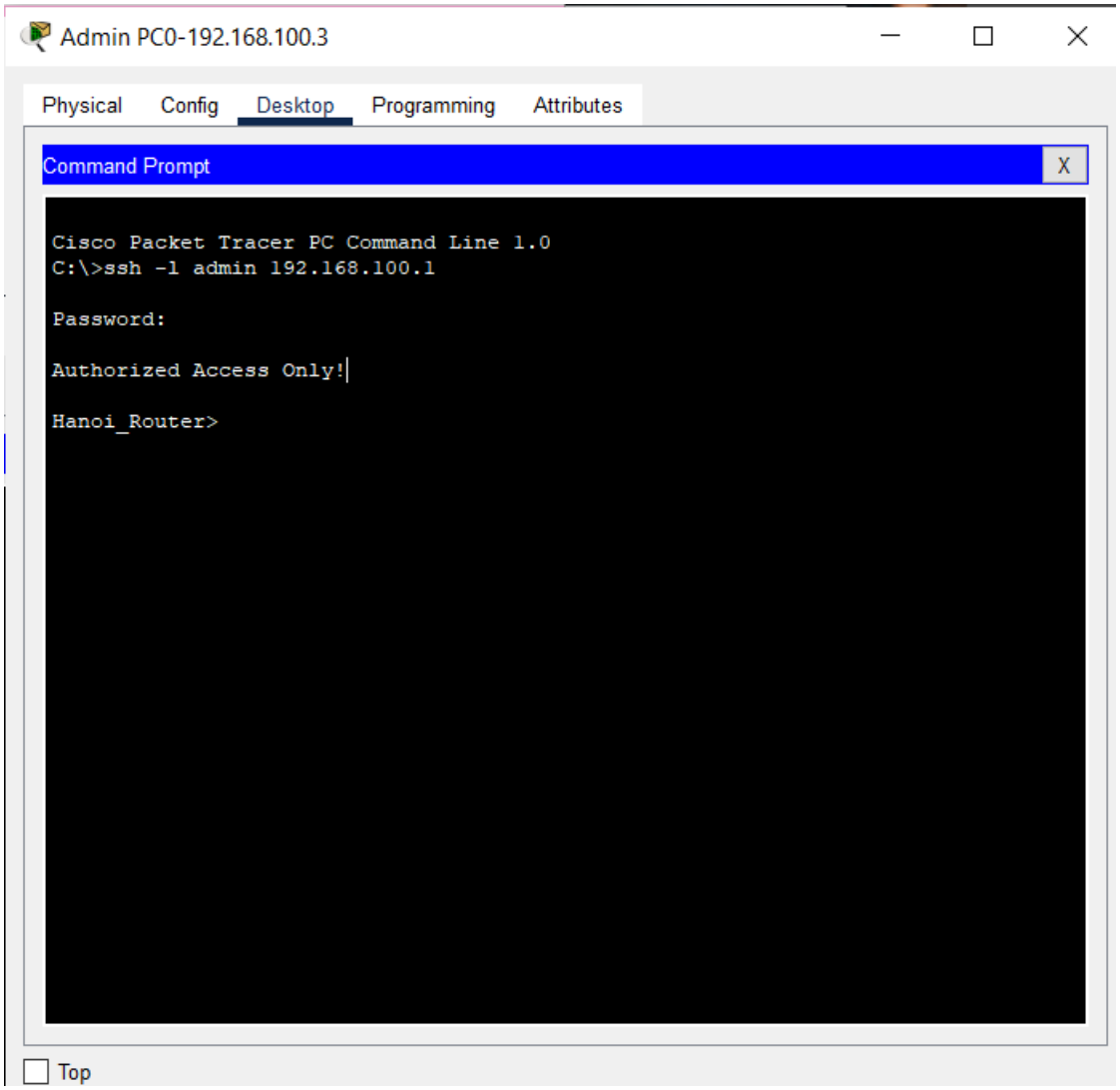

Figure 59 Admin PC0

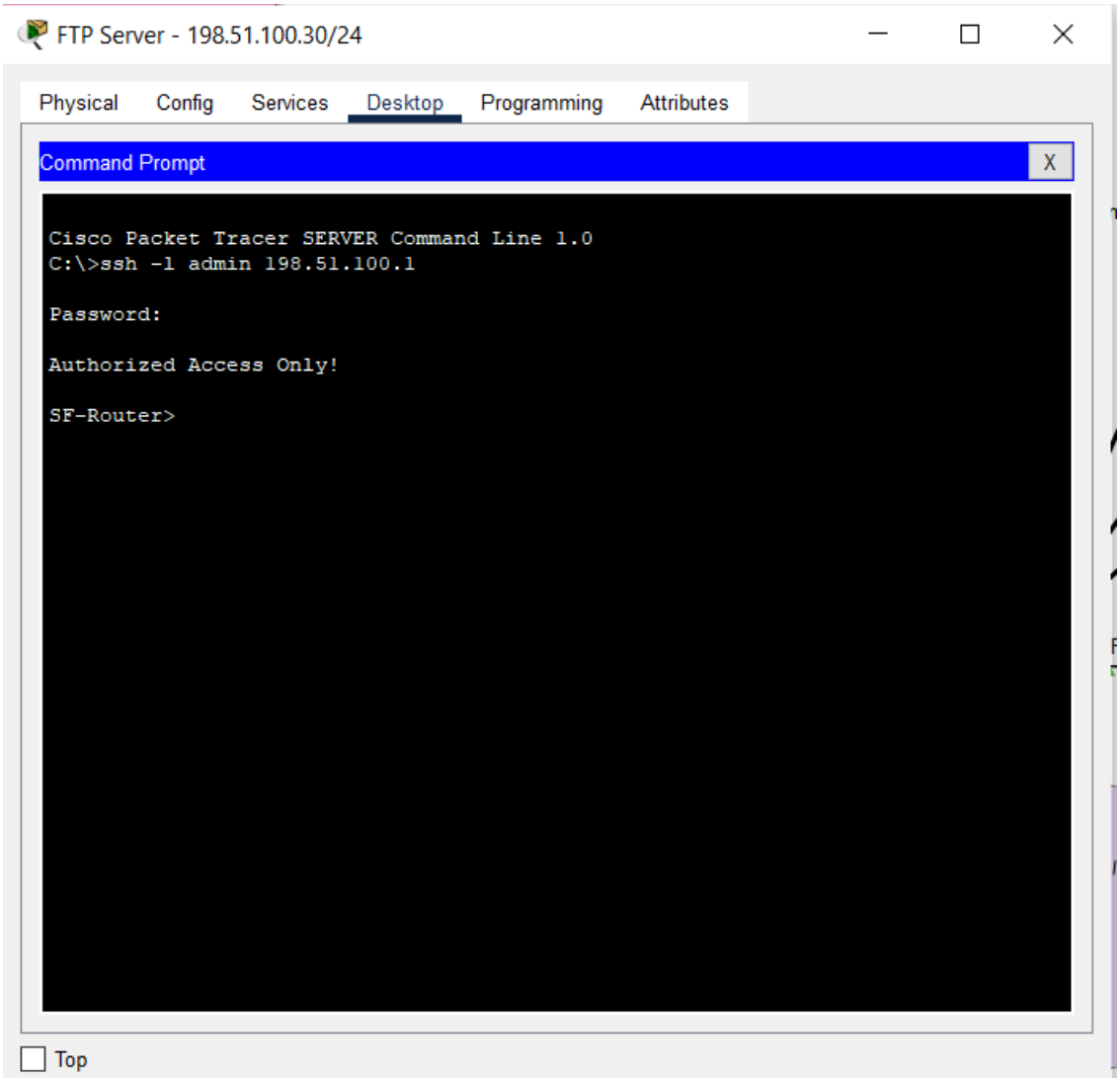

Figure 60 FTP Server

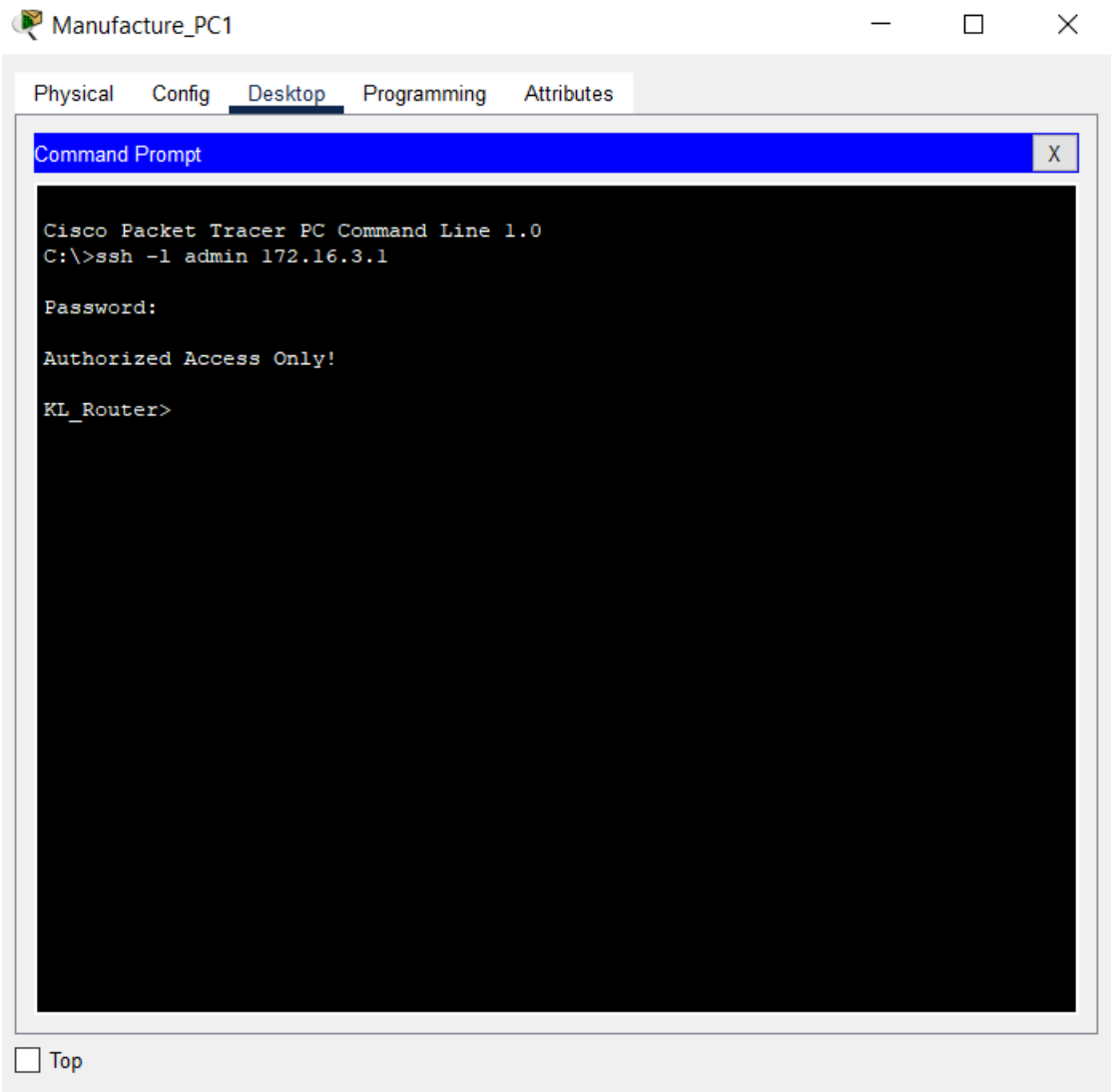

Figure 61 Manufacture_PC1

6.0 Conclusion

Through this task to design and create prototype, I have learnt how to configure the servers, access points, VLANs, inter-VLANs, Routing Interface Protocol (RIP), Ip routing, Ip helper-address and basic configurations of switch and routers. Other than that, I also learn how to do IP Addressing tables in detail where VLAN and Inter-VLAN is included. Each network is listed separately. The High Dot Tech network can be managed more easily, and the issues will be identified faster. Lastly, the overall security of the High Dot Tech network is also enhanced with the VLAN, and Port Security configured.

The content that had been discussed previously in the Section A will be the WLAN architecture of the High Dot Tech network. Furthermore, the layer 2 security attacks that might happens on the High Dot Tech network are also discussed. Moreover, the security deployment on layer 2 to mitigate the attacks is also discussed as well.

For section B of this assignment, a brief introduction about the content is given. The passwords of the packet tracer is also included. As for the IP Addressing Table section, I have included a subnet table to identify the usable IP of the LANs and WANs. This will reduce mistakes and make the process of getting IP address faster. The IP addressing table for WAN and LAN is listed separately. Some Ip addresses that are assigned automatically will be stated as “DHCP Assigned” in the table. To ease the process of configuring and make things clear, a VLAN table, port assignments table and router subinterfaces table is listed. These three tables had helped me a lot while I configure the VLAN and inter-VLAN of High Dot Tech network. As for the entire network layout, the types of topologies used in the High Dot Tech network is discussed. The advantages and disadvantages of topology is also discussed.

Furthermore, for the LAN and WAN configuration part, the basic configurations on all routers and switches is shown and explain. As for the Server configurations, the changes are made on the Graphic User Interface (GUI) of servers. So, the screenshots of the server configurations are attached. There are also the steps for configuring all the servers in High Dot Tech network. Effort to achieve static and dynamic ip addressing is also shown along with explanation. Dynamic Ip addressing needs the help of the IP helper address. To make routers connect with each other, RIP version 2 is implemented in the WAN of High Dot Tech network. There are also some explanation and demonstrations of VLAN configurations shown. Inter-VLAN is also discussed.

For the security mechanism deployment in configuration of High Dot Tech network, I have chosen two which I can implement them. When configuring the port security at first, I

have faced difficulties that I found out after the port security is configured, the DHCP is not working anymore. To solve this, I set the maximum mac-address to be learn according to the number of the end devices. The following security mechanism deployed in High Dot Tech network will be the SSH. The SSH is configured in the routers and switches that connects to LAN. After SSH configured, the data transmitted will be encrypted which provide the business more security and protection. The SSH can be accessed through the SSH Client and the command prompt of the LAN devices.

7.0 References

Cisco. (n.d.). *Inter-VLAN Routing Operation*. Switching, Routing, and Wireless Essentials. Retrieved November 28, 2022, from https://contenthub.netacad.com/srwe-dl/4.1.3

Cisco. (n.d.). *Overview of VLANs*. Switching, Routing, and Wireless Essentials. Retrieved November 28, 2022, from https://contenthub.netacad.com/srwe-dl/3.1.5

Cisco. (n.d.). *Secure Remote Access*. Switching, Routing, and Wireless Essentials. Retrieved November 30, 2022, from https://contenthub.netacad.com/srwe-dl/1.3.2

a Hewlett Packard Enterprise Company. (n.d.). *IP helper-address*. aruba. Retrieved November 28, 2022, from https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7837/Content/Chp_DHCP/DHCPv4_relay_cmds/ip-hel-add-10.htm#:~:text=Defines%20the%20address%20of%20a,requests%20to%20all%20defined%20servers.

Indeed. (2022, April 2). *7 network topology types (plus definitions and key features)*. Indeed. Retrieved November 27, 2022, from https://www.indeed.com/career-advice/starting-new-job/network-topology-types

Routing information protocol (RIP). GeeksforGeeks. (2022, June 28). Retrieved November 28, 2022, from https://www.geeksforgeeks.org/routing-information-protocol-rip/

WatchGuard. (n.d.). *Static and Dynamic IP Addresses*. Help Centre. Retrieved November 28, 2022, from https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/overview/networksecurity/ip_address_static_dyn_c.html#:~:text=A%20dynamic%20IP%20address%20is,using%20either%20DHCP%20or%20PPPoE.

What is network topology? best guide to types & diagrams. DNSstuff. (2022, October 20). Retrieved November 28, 2022, from https://www.dnsstuff.com/what-is-network-topology#hybrid-topology