University of Bahrain

College of Information Technology

Department of Network Engineering

Network Engineering and Design

ITCE418 Project:

Network Extension for SouqAl-Manama Business School

Submitted to: Dr. Mohammed A. Almeer

<u>Group A</u>

Done by:

Hesham Ahmed Ghulam – 202003472

Sayed Mahmood Alawi – 20194103

Ali Ahmed Ali –20193895

Yusuf Ali Hassan – 202006103

Submitted on: May 15, 2024

Contents

Introduction

The Souq Al-Manama Business School's network extension project is an important project that aims to improve the educational infrastructure to support the school's expansion plans. Four computer labs and two research rooms will be installed in the new building; therefore, a reliable and expandable network infrastructure is required. By expanding the current network to easily link the new building and provide high-speed, reliable, and secure connectivity for staff, teachers, and students, this project aims to meet this need.

Main Project Goal

The primary goal of the project is to establish a comprehensive network infrastructure that meets the evolving needs of Souq Al-Manama Business School's educational environment. This includes providing constant connectivity, facilitating access to digital resources, and supporting collaborative learning and research activities.

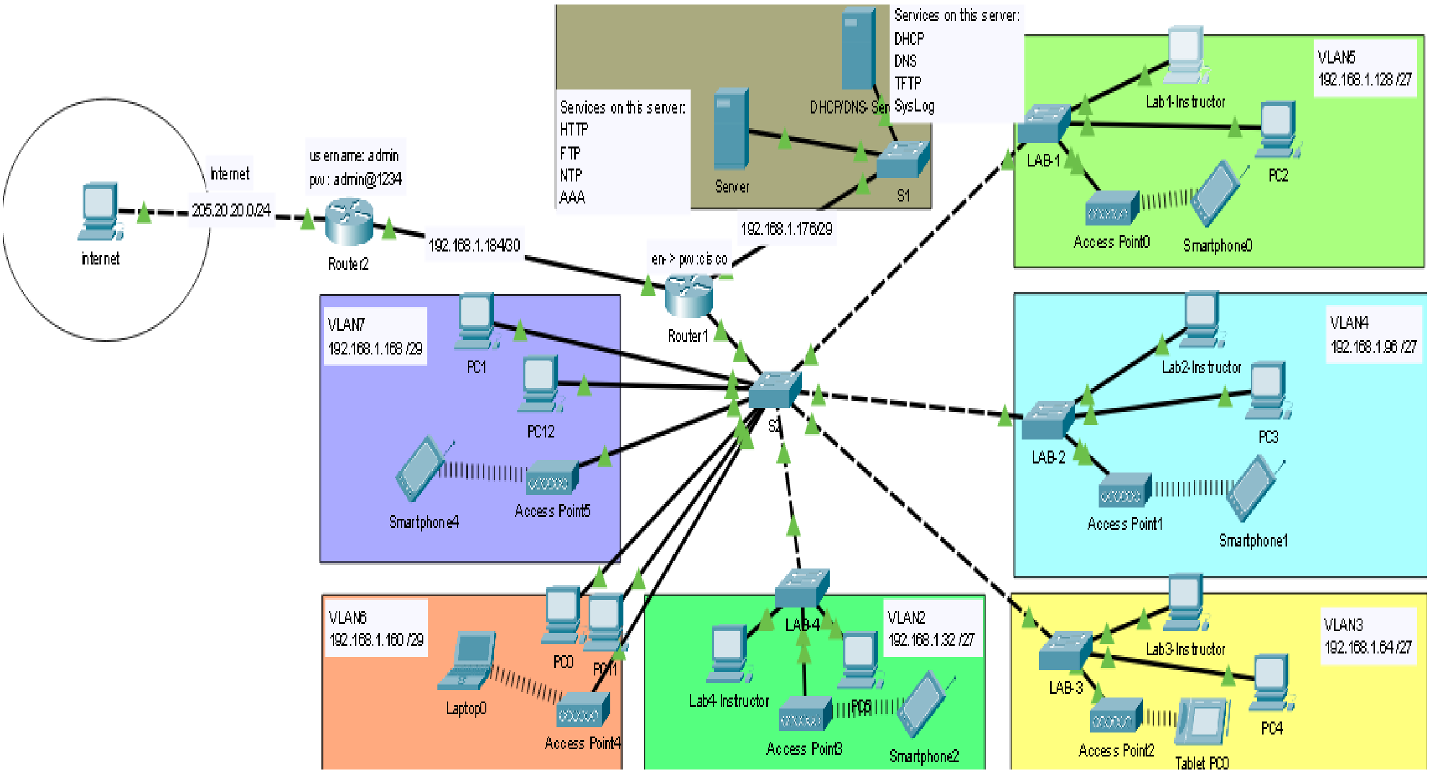
The Design Requirements section contains:

Business Goals	Technical Goals
Improve Academic Productivity: - The project aims to improve teacher and student productivity by providing easy access to digital learning platforms, educational resources, and collaborative tools.	**Enhanced Network Security:** - Sensitive administrative and academic data will be protected by the implementation of good security technologies and protocols.
Enhance Souq Al-Manama Business School's Competitiveness: - The network extension project aims to elevate the school's competitive edge by providing a technologically advanced learning environment.	**Optimized Network Performance:** - The project will focus to guarantee high-performance network operations by utilizing technologies and techniques.
Increase Student Enrollment and Retention: - A good and efficient network infrastructure will attract more students to Souq Al-Manama Business School by offering an engaging and interactive learning experience.	**Scalable Network Architecture:** - The network design will prioritize scalability and flexibility to accommodate future growth and technological advancements.
	User-Friendly Design and High Availability: - The network infrastructure will be designed to be always user-friendly and accessible.

Requirements and Architecture

We will install 20 high-performance student computers and one instructor computer in each lab, all connected to a secure local area network (LAN). Each research room will be equipped with four advanced computers, also connected to the LAN. Our solution guarantees high-speed internet access, with a Wi-Fi network capable of supporting 60+ users simultaneously. We propose a centralized network storage system that offers good space for data sharing and backups. The servers we install will be powerful enough to handle all computational tasks required by the labs and research rooms.

Network Diagram



Devic	Quantity	Vendor
Routers	2	Cisco
Switches	7	Cisco
Servers	2	Cisco
PC's	13	Cisco
AP	6	Cisco
Cables	2 types (Straight-Through & Cross-Over)	

Addressing Schema

Subnet Description	**# of IPs Needed**	**# of wasted IPs**	**Network Address/CIDR Subnet mask**	**Default Gateway**	**1st Usable Host Address**	**Broadcast Address**
Lab 4	21	9	192.168.1.32 /27 255.255.255.224	192.168.1.33	192.168.1.34	192.168.1.63
Lab 3	21	9	192.168.1.64 /27 255.255.255.224	192.168.1.65	192.168.1.66	192.168.1.95
Lab 2	21	9	192.168.1.96 /27 255.255.255.224	192.168.1.97	192.168.1.98	192.168.1.127
Lab 1	21	9	192.168.1.128 /27 255.255.255.224	192.168.1.129	192.168.1.130	192.168.1.159
Research Room 1	4	2	192.168.1.160 /29 255.255.255.248	192.168.1.161	192.168.1.162	192.168.1.167
Research Room 2	4	2	192.168.1.168 /29 255.255.255.248	192.168.1.169	192.168.1.170	192.168.1.179
IT (Server LAN)	2	4	192.168.1.176 /29 255.255.255.248	192.168.1.177	192.168.1.178	192.168.1.183

Notes:

- Selected IP address: 192.168.1.0/24
- We implemented VLSM to minimize the wasted IP addresses.

For future growth we have left the following range of addresses in case the school is needed:

192.168.1.0 /27 **192.168.1.192 /27** **192.168.1.224 /27**

Interface Configurations

following subnetting. The IP addresses should be used to configure the router interfaces; interfaces from Router 1 and Router 2 are shown with their IP addresses in the tables below:

- Router 1

Table 1

Interface	Description	IP Address	VLAN
Gig0/0	-	-	Yes
Gig0/1	Connected to router 2	191.168.1.185/30	No
Gig0/2	Connected to servers LAN	192.168.1.177/29	No

```
Router(config)#inter gig0/1
Router(config-if)#ip add 192.168.1.185 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#inter gig0/2
Router(config-if)#ip add 192.168.1.177 255.255.255.248
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
```

Figure 1: Interface configuration on Router 1

```
Router(config)#inter gig0/0
Router(config-if)#no shut

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
```

Figure 2: Interface configuration on Router 1

- Router 2

Table 2

Interface	Description	IP Address	VLAN
Gig0/0	Connected to the internet	205.20.20.1/24	No
Gig0/1	Connected to router 1	191.168.1.186/30	No

```
Router(config)#inter gig0/1
Router(config-if)#ip add 192.168.1.186 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Figure 3: Interface configuration on Router 2

VLAN Configurations

- Switch 2

Here you can find the commands that we used to configure VLANs on Switch 2.
Note: Same commands are used for all VLANs.

```
Switch(config)#vlan 4
Switch(config-vlan)#name lab2
Switch(config-vlan)#exit
Switch(config)#int range fa0/3-4
Switch(config-if-range)#sw mode access
Switch(config-if-range)#sw access vlan 4
Switch(config-if-range)#exit
Switch(config)#
```

Figure 5: Ex: Labs VLAN configurations.

```
Switch(config)#vlan 6
Switch(config-vlan)#name research-room1
Switch(config-vlan)#exit
Switch(config)#int range fa0/9-14
Switch(config-if-range)#sw mode access
Switch(config-if-range)#sw access vlan 6
Switch(config-if-range)#exit
Switch(config)#
```

Figure 4: Ex: Research Room VLANs configurations.

```
Switch(config)#do sho vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    lab4                             active    Fa0/7, Fa0/8
3    lab3                             active    Fa0/5, Fa0/6
4    lab2                             active    Fa0/3, Fa0/4
5    lab1                             active    Fa0/1, Fa0/2
6    research-room1                   active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14
7    research-room2                   active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch(config)#
```

Figure 6: VLAN Verification on Switch 2.

Inter-VLAN Routing

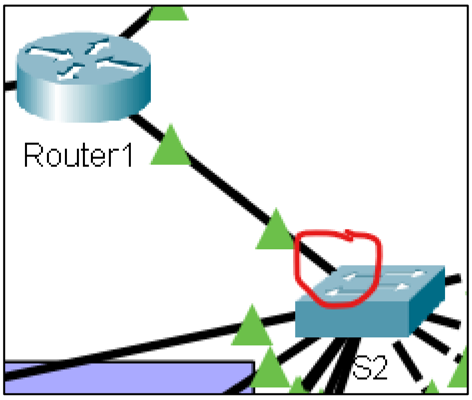


Figure 7: Trunk port (Fa0/22) on Switch 2.

```
Switch(config)#inter fa0/22
Switch(config-if)#sw mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up
```

Figure 8: Trunk port configuration on Switch 2.

We configured Router 1 by creating sub-interfaces for every VLAN so they can communicate with each other.

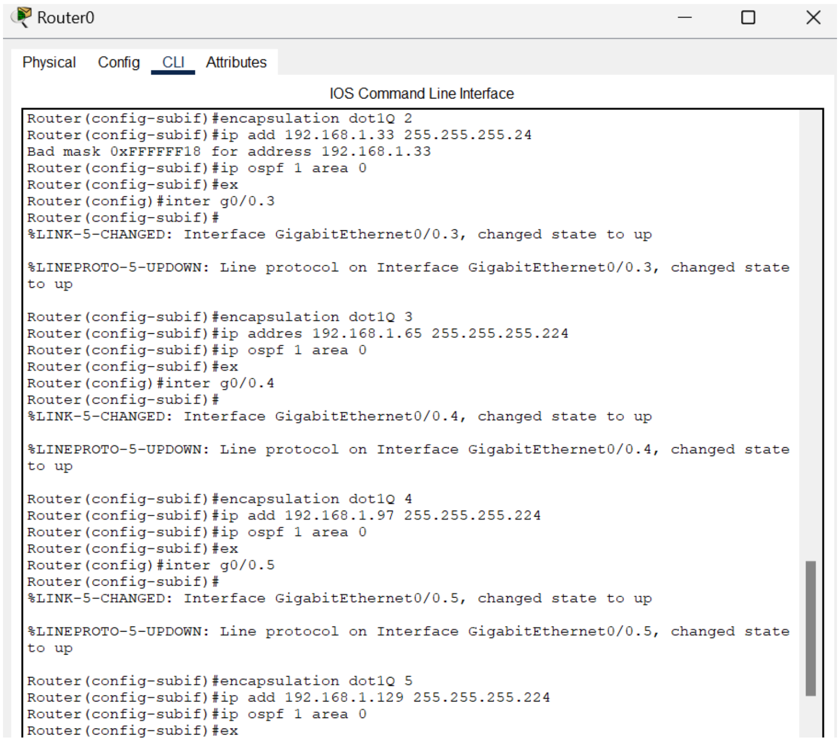


Figure 9: Sub-Interface configuration on Router 1.

Routing Protocol (OSPF)

```
Router(config)#inter gig0/1
Router(config-if)#ip ospf 1 area 0
Router(config-if)#inter gig0/2
Router(config-if)#ip ospf 1 area 0
Router(config-if)#exit
```

Figure 10: OSPF configuration on Router 1.

```
Router(config)#inter gig0/1
Router(config-if)#ip ospf 1 area 0
Router(config-if)#exit
```

Figure 11: OSPF configuration on Router 2.

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 14 subnets, 4 masks
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0.2
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0.2
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0.3
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0.3
C       192.168.1.96/27 is directly connected, GigabitEthernet0/0.4
L       192.168.1.97/32 is directly connected, GigabitEthernet0/0.4
C       192.168.1.160/29 is directly connected, GigabitEthernet0/0.6
L       192.168.1.161/32 is directly connected, GigabitEthernet0/0.6
C       192.168.1.168/29 is directly connected, GigabitEthernet0/0.7
L       192.168.1.169/32 is directly connected, GigabitEthernet0/0.7
C       192.168.1.176/29 is directly connected, GigabitEthernet0/2
L       192.168.1.177/32 is directly connected, GigabitEthernet0/2
C       192.168.1.184/30 is directly connected, GigabitEthernet0/1
L       192.168.1.185/32 is directly connected, GigabitEthernet0/1
     192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.169.1.128/27 is directly connected, GigabitEthernet0/0.5
L       192.169.1.129/32 is directly connected, GigabitEthernet0/0.5
```

Figure 12: OSPF verification on Router 1.

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 8 subnets, 4 masks
O       192.168.1.32/27 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
O       192.168.1.64/27 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
O       192.168.1.96/27 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
O       192.168.1.160/29 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
O       192.168.1.168/29 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
O       192.168.1.176/29 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
C       192.168.1.184/30 is directly connected, GigabitEthernet0/1
L       192.168.1.186/32 is directly connected, GigabitEthernet0/1
     192.169.1.0/27 is subnetted, 1 subnets
O       192.169.1.128/27 [110/2] via 192.168.1.185, 00:00:30, GigabitEthernet0/1
```

Figure 13: OSPF verification on Router 2.

DHCP Server

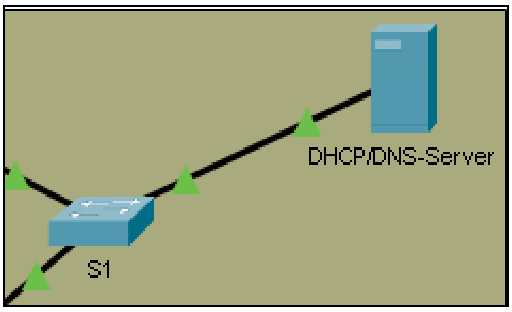


Figure 14: DHCP server connected to Switch 1 with static IP address (192.168.1.178).

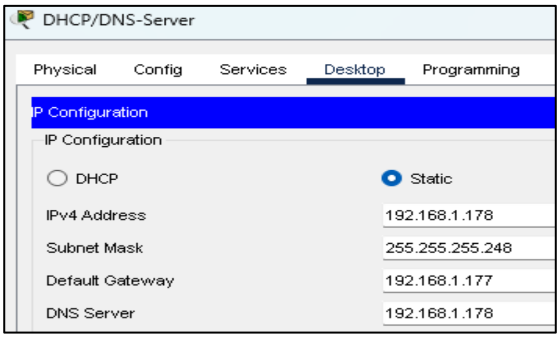


Figure 15: Assign static IP address to the DHCP server.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WL(Addre
Lab1Pool	192.168....	192.168....	192.168....	255.255....	30	0.0.0.0	0.0.0.0
Lab2Pool	192.168....	192.168....	192.168....	255.255....	30	0.0.0.0	0.0.0.0
Lab3Pool	192.168....	192.168....	192.168....	255.255....	30	0.0.0.0	0.0.0.0
Lab4Pool	192.168....	192.168....	192.168....	255.255....	30	0.0.0.0	0.0.0.0
researRoom1Pool	192.168....	192.168....	192.168....	255.255....	6	0.0.0.0	0.0.0.0
researRoom2Pool	192.168....	192.168....	192.168....	255.255....	6	0.0.0.0	0.0.0.0

Figure 16: DHCP pools creation on the server.

```
Router(config)#inter gig0/0.5
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#inter gig0/0.4
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#inter gig0/0.3
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#inter gig0/0.2
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#inter gig0/0.6
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#inter gig0/0.7
Router(config-subif)#ip helper-address 192.168.1.178
Router(config-subif)#exit
Router(config)#do wr
```

Figure 17: IP-helper configuration on Router 1.

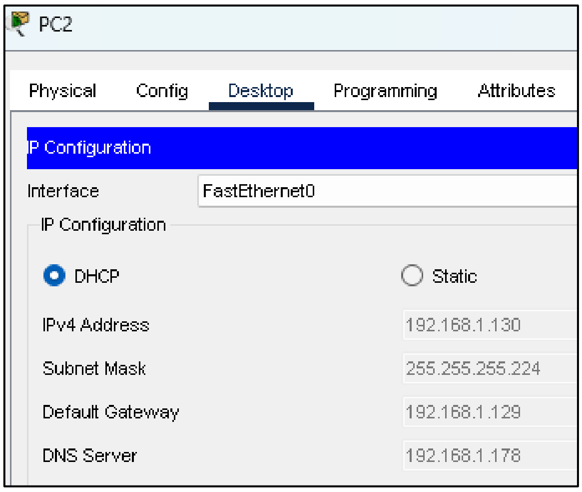


Figure 18: Assign dynamic IP address to PC’s.

DNS Server

We are using the DNS server to match IP-Address of the website with the URL.

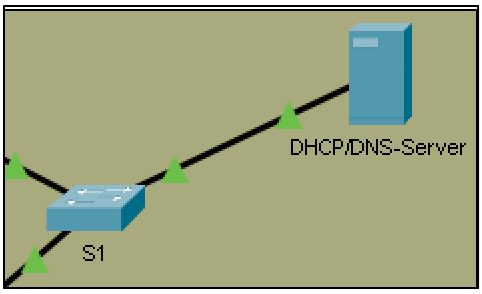


Figure 19: DNS server connected to Switch 1 with static IP address (192.168.1.178).

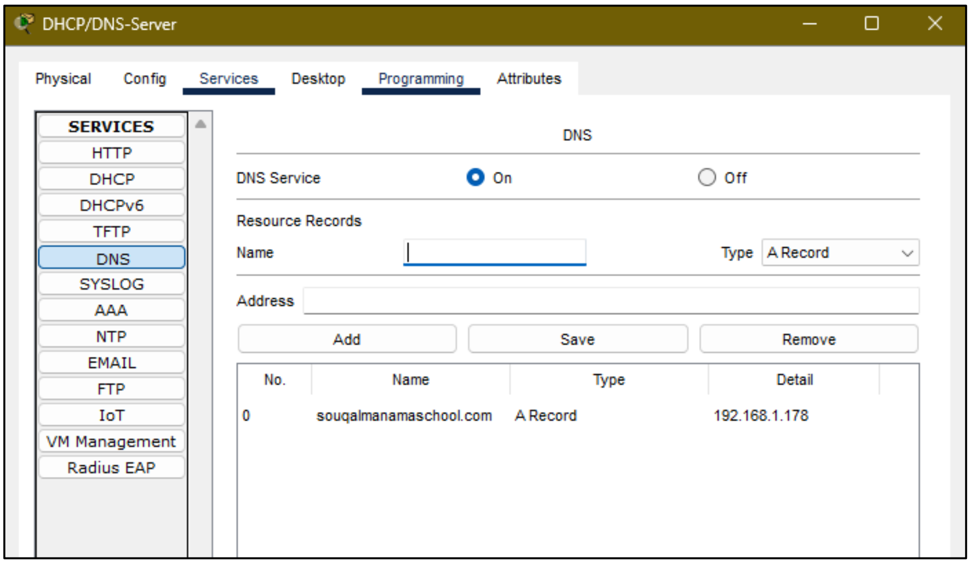


Figure 20: DNS settings and configuration.

HTTP Server:

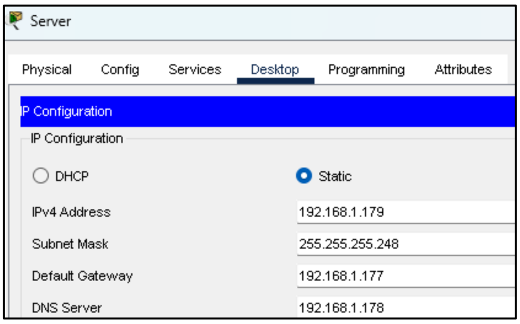


Figure 21: Assign static IP address to the Web server.

We created a website for the school using the HTTP server.

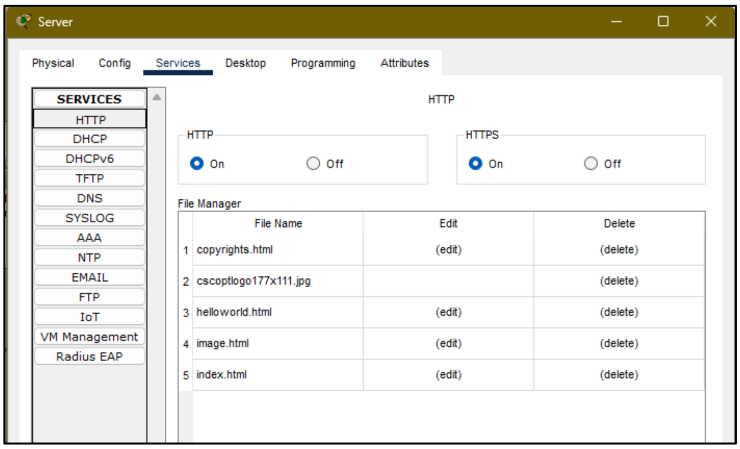


Figure 22: Web server settings and configurations.

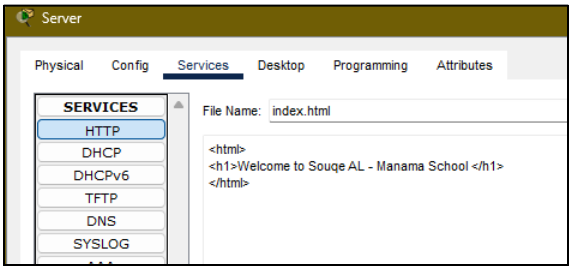


Figure 23: Web server file (HTML, CSS, and PHP …)

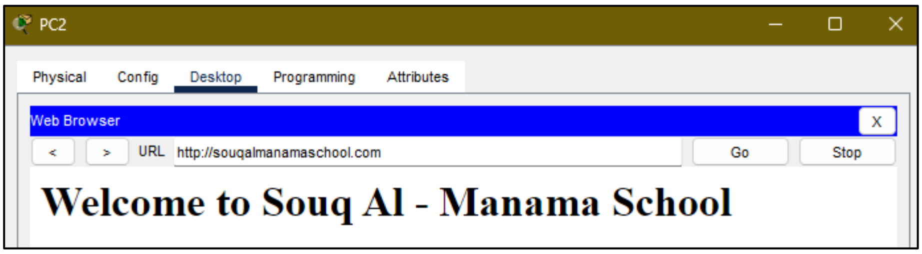


Figure 24: Web server verification using domain name.

FTP Server

Using File Transfer Protocol (FTP), users can transmit and receive files from a server that manages and saves all the data. This is a crucial service since lots of businesses have multiple employees working on the same documents, so having a way to share them is important.

Here we created a user for lab instructors, and they will have read and write permissions.

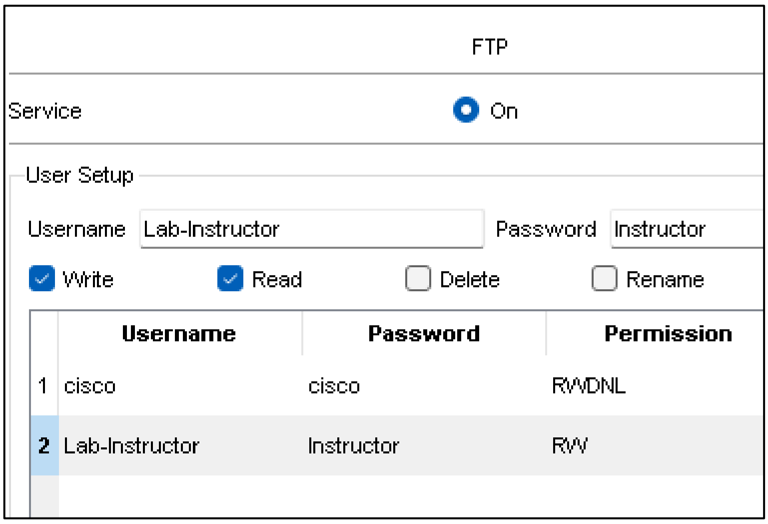


Figure 25: FTP server settings and configurations.

As you can the lab instructor can access the ftp server.

Figure 26: FTP server verification.

Host-Based Firewall

Here as you can see, we configured the host-based firewall on the server to allow all lab instructors to access the FTP service. Deny any other users from using the FTP service. We Enabled HTTP service (should be accessible from inside and outside users).

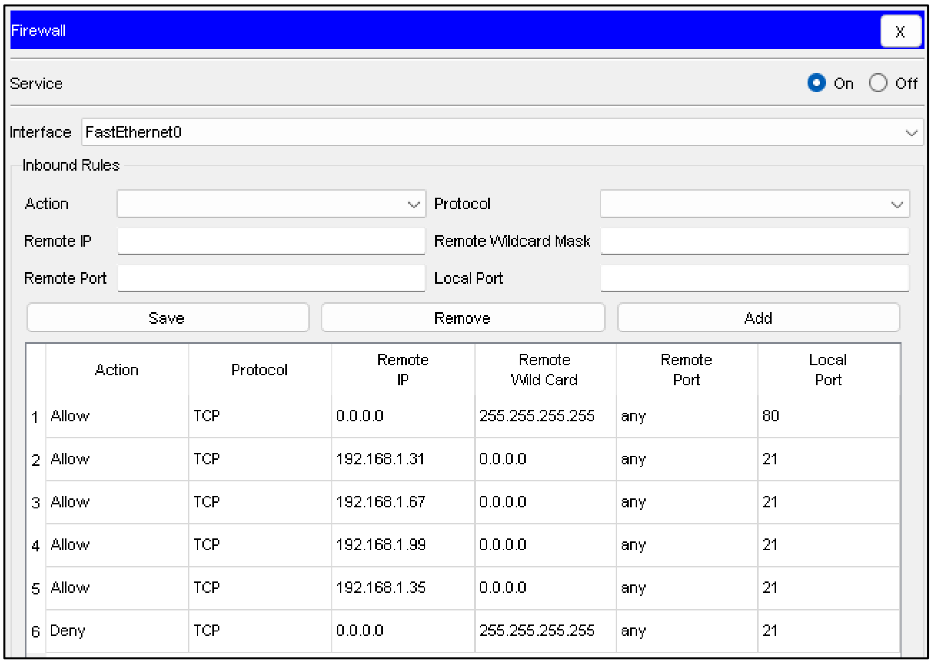


Figure 27: Server settings and configurations.

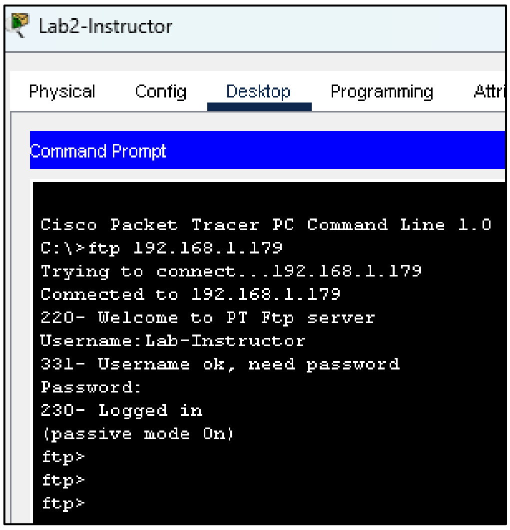


Figure 28: Verification (Allowing lab instructor to access).

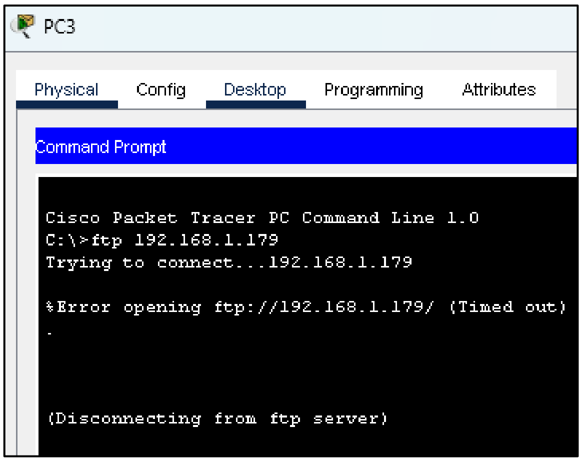


Figure 29: Verification (Denying other users from access).

Network-Based Firewall

As you can see anyone can access the internal website (http server) from the internet. So, now to avoid threats from the internet we will configure a firewall on Router 2 which is connecting the internal LAN to the internet.

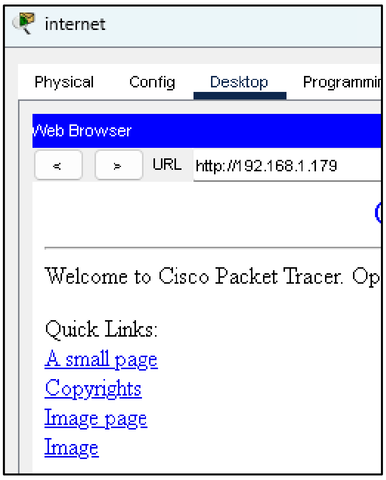
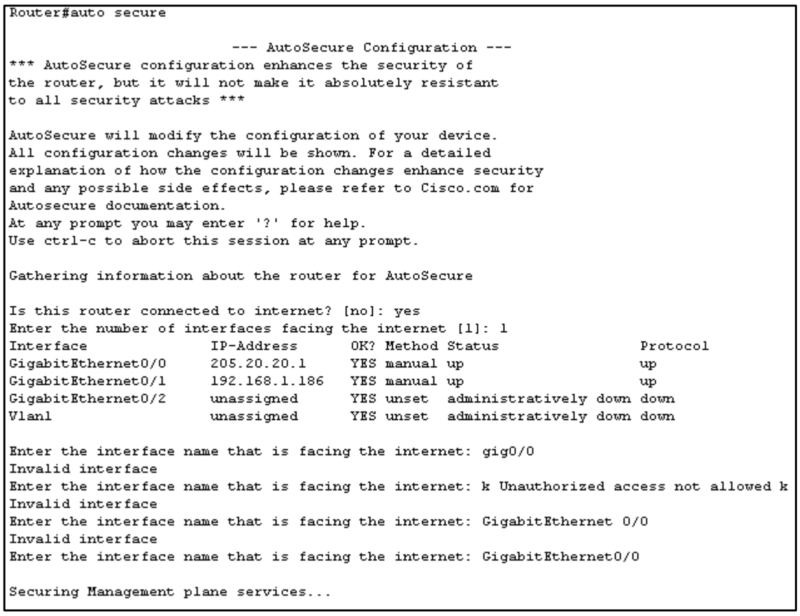


Figure 30: User from the internet accessing the web server.



```
Router#auto secure

                        --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     205.20.20.1     YES manual up                    up
GigabitEthernet0/1     192.168.1.186   YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down

Enter the interface name that is facing the internet: gig0/0
Invalid interface
Enter the interface name that is facing the internet: k Unauthorized access not allowed k
Invalid interface
Enter the interface name that is facing the internet: GigabitEthernet 0/0
Invalid interface
Enter the interface name that is facing the internet: GigabitEthernet0/0

Securing Management plane services...
```

Figure 31: Firewall configurations on Router 2.

Table 3: Network-Based Firewall configurations on Router.

Router terminal	Settings
Is this router connected to the internet? [no]:	yes
Enter the number of interfaces facing the internet [1]:	1
Enter the interface name that is facing the internet:	FastEthernet1/0
Enter the security banner {Put the banner between k and k, where k is any character}:	k (use user student ID) k
Enable secret is either not configured or is the same as enable password, Enter the new enable secret:	cisco
Confirm the enable secret:	cisco
Enter the new enable password:	cisco1
Confirm the enable password:	cisco1
Configuration of local user database, Enter the username:	admin
Enter the password:	admin@1234
Confirm the password:	admin@1234
Blocking Period when Login Attack detected:	3
Maximum Login failures with the device:	3
Maximum time period for crossing the failed login attempts:	3

Configure SSH server? [yes]:	Yes
Enter the host name:	R1
Enter the domain-name:	Class.com
Configure CBAC Firewall feature? [yes/no]:	Yes
Apply this configuration to running-config? [yes]:	yes

Now as you can see here someone is trying to access the web server, but our network-based router is not letting him access.

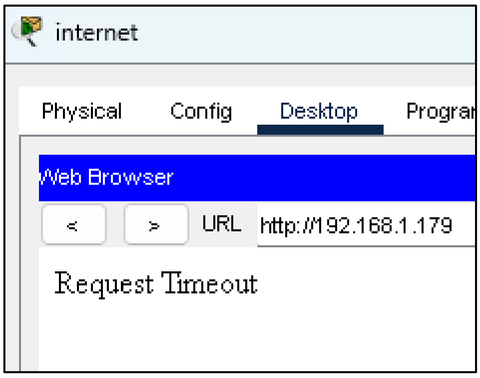


Figure 32: No one from the internet can access.

NTP Server

The NTP service is necessary for the network to synchronize the clocks of the devices and to facilitate troubleshooting and potential problem solving.

The correct date and time are then set as indicated on the server after the NTP service has been toggled to "on" in the server.

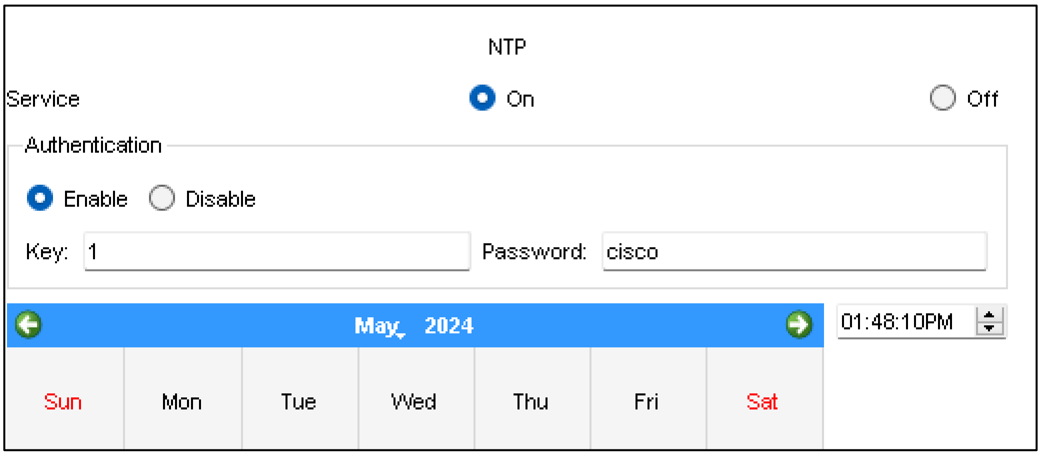


Figure 33: NTP Server settings and configurations.

```
Router(config)#ntp authentication-key 1 md5 cisco
Router(config)#ntp authenticate
Router(config)#ntp trusted-key 1
Router(config)#ntp server 192.168.1.179 ket 1
                                          ^
% Invalid input detected at '^' marker.

Router(config)#ntp server 192.168.1.179 key 1
Router(config)#ntp update-calendar
```

Figure 34: NTP Server configurations on Router 1

```
Router#show clock
23:55:31.780 UTC Mon May 13 2024
```

Figure 35: NTP Server verification on Router 1.

Syslog Server

A network service called Syslog is set up to gather log messages from devices connected to the network, together with dates and timestamps. These logs and data are used thereafter if troubleshooting is required to determine the root cause of a network disturbance. For this reason, Syslog is a necessary tool and service for each network administrator in a business.

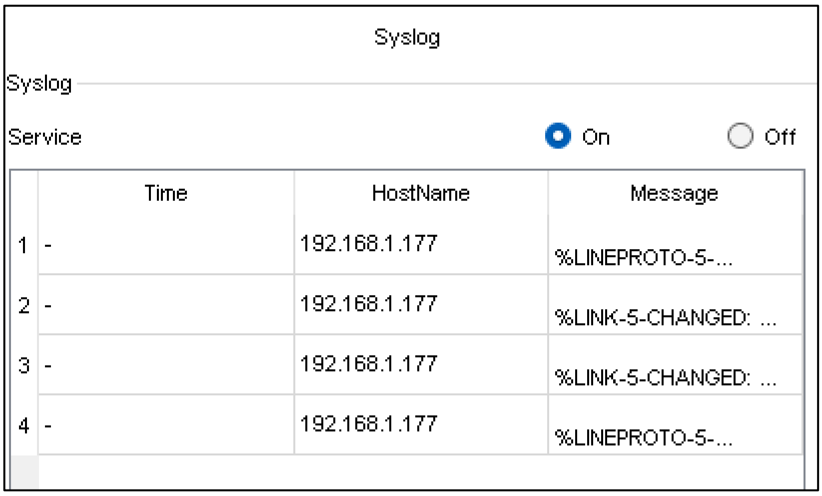


Figure 36: Syslog settings and configurations on the server.

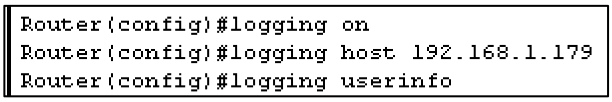


Figure 37: Syslog configurations on Router 1.

SNMP

Simple Network Management Protocol. It's like a language that helps devices like computers, routers, and switches talk to each other and share important information about how they're doing. Think of it as a way for these devices to report on their health and performance.

So, SNMP helps network administrators keep track of what's happening in their network and make sure everything is running smoothly.

```
Router(config)#snmp-server community public ro
%SNMP-5-WARMSTART: SNMP agent on host Router is undergoing a warm start
Router(config)#snmp-server community private rw
```

Figure 38: SNMP configurations on Router 1.

As you can see here by MIB tree the administrator can manage the network device with help of SNMP protocol.

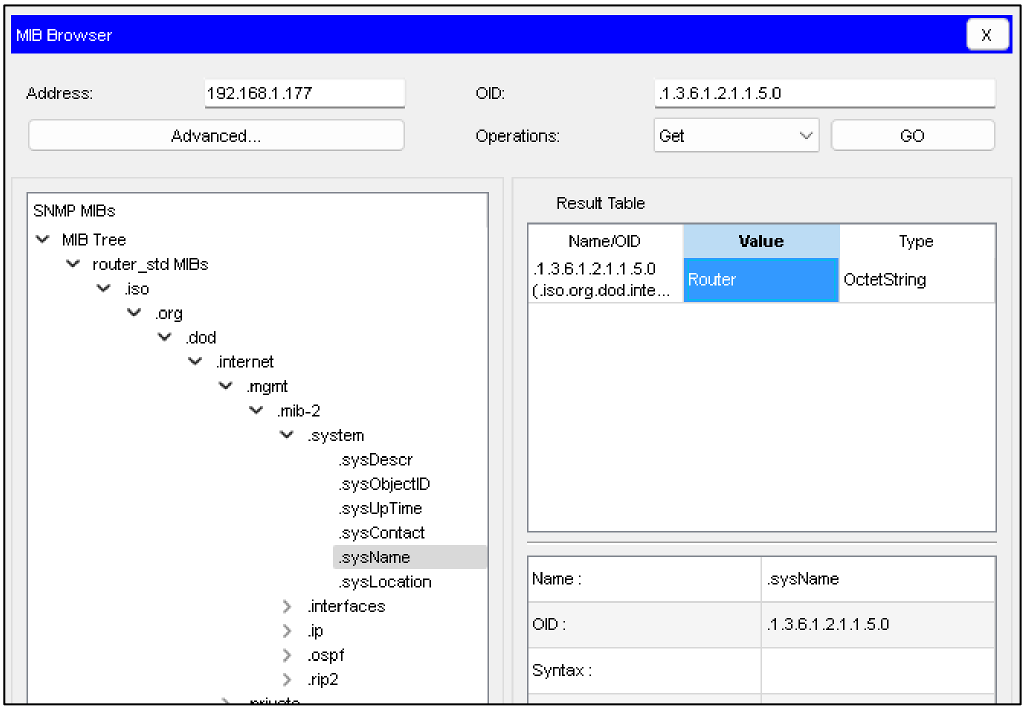


Figure 39: SNMP verification (Ex: Getting Router name).

AAA

AAA stands for Authentication, Authorization, and Accounting. It's like a three-step process that helps control who can access a computer network and what they can do once they're in.

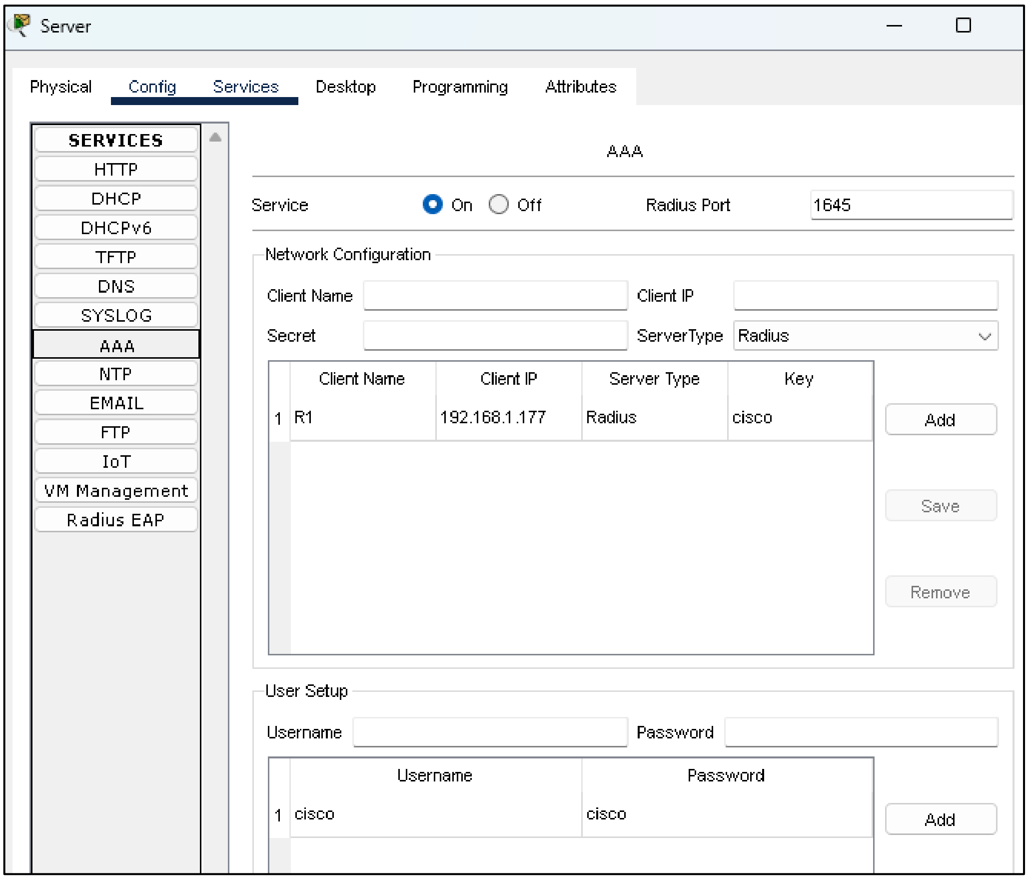


Figure 40: AAA settings and configurations on the server.

Now, here when we enter (en) mode it will check the radius first if it exists then we must enter the password that we set (Ex: cisco).

```
Router>en
Password:
Router#
Router#
```

Figure 41: AAA verification.

TFTP Server

TFTP server is used for sending and receiving files between computers on a network. TFTP is often used for things like updating software on network devices, like routers or switches, or for booting computers over the network. It's a quick and easy way to transfer files between computers without a lot of fuss.

We will use TFTP for saving a backup configuration on the TFTP server.

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.178
Destination filename [Router-confg]?

Writing running-config...!!
[OK - 2345 bytes]

2345 bytes copied in 0.018 secs (130277 bytes/sec)
Router#
```

Figure 42: Copying the running configuration to the TFTP server.

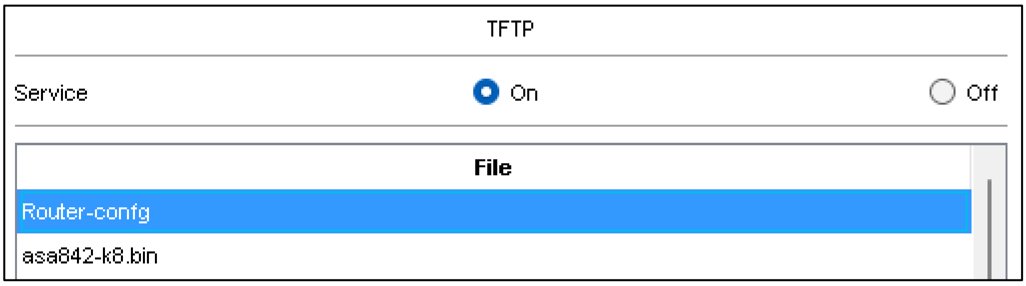


Figure 43: TFTP verification. The configurations are saved in the server.

By saving a backup configuration on a TFTP server, we have a secure and easily accessible copy of the device's settings that can be used for restoring configurations in case of emergencies, such as hardware failures or accidental changes.

WLAN (Access Points)

We will deploy APs to provide wireless connectivity to the entire business.

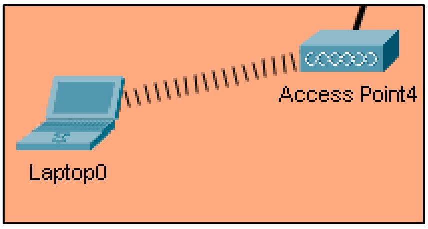


Figure 44: Cisco Access Points are deployed.

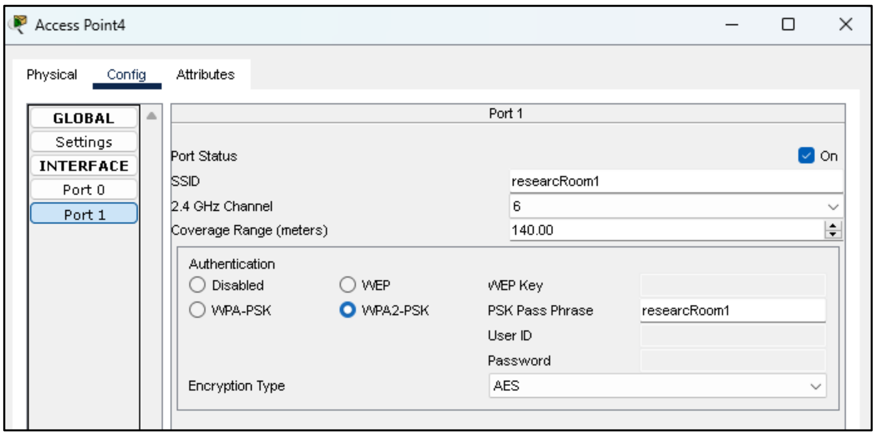


Figure 45: AP settings and configurations.

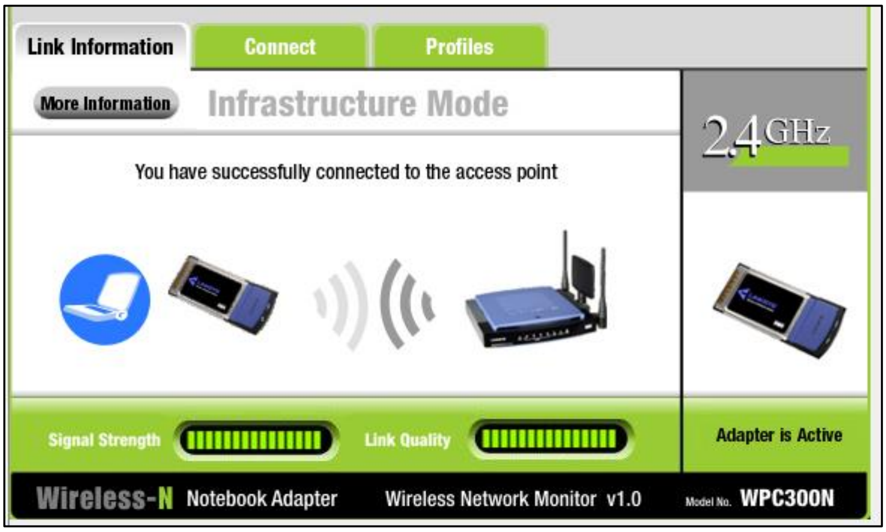


Figure 46: Verification (Wireless device successfully connected).

Testing the Connectivity of the network

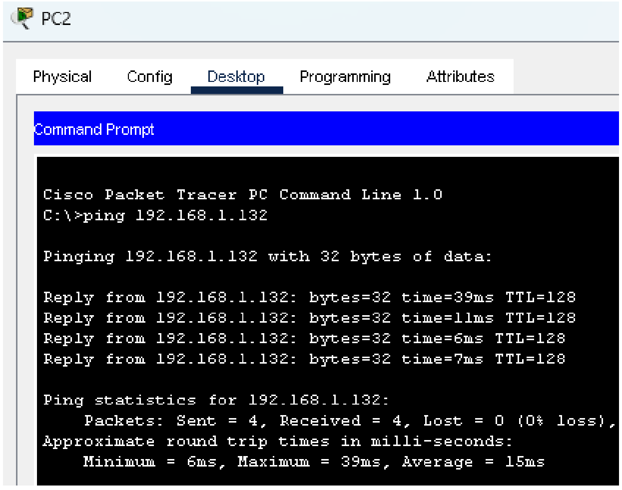


Figure 48: Same VLAN

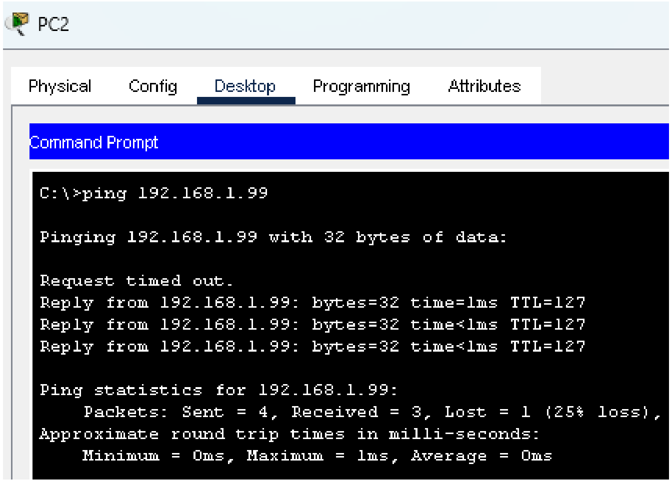


Figure 47: Different VLANs

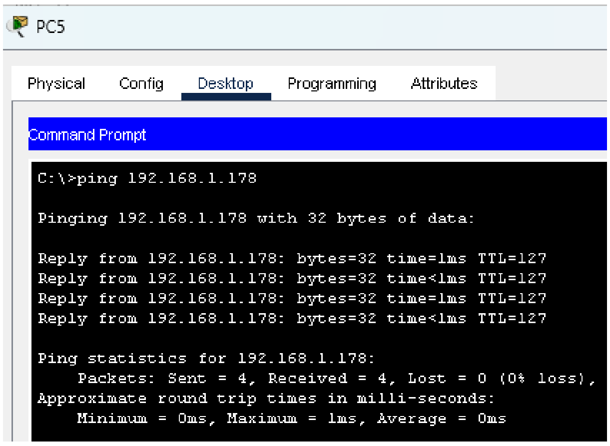


Figure 49: Pinging the DHCP server.

Note: If you want to check the other services like HTTP, NTP, FTP, etc. Please check them from the PCs not by pinging, due to software-based firewall you are not able to ping them.

Design Analysis

Table 4

Requirement	Met (Yes/No)	Fulfilled by
Implement Company Structure	Yes	Cisco Packet Tracer Simulation
Multiple Switches and VLANs	Yes	Utilization of Switches and VLANs
Routing Between VLANs/Branches	Yes	Router-on-Stick Architecture and OSPF Routing
Firewall Implementation	Yes	Integration of Host-Based Firewall and Network-Based Firewall
Network Management	Yes	Integration of SNMP, Syslog, TFTP, NTP, AAA
Network Connectivity Verification	Yes	Successful execution of ping, show IP route, and show VLAN brief commands

This summary table provides an overview of how each project requirement has been addressed in the design. It indicates whether the requirement has been met and specifies which aspect of the design fulfills this requirement. This allows for a clear and good evaluation of the design's alignment with project requirements.

Conclusion

Through the design and implementation of the network infrastructure using Cisco Packet Tracer, we've built a strong and safe network setup that meets the project goals. We've used Cisco Packet Tracer to make it happen. The network has switches and different sections called VLANs to organize things neatly. We've also made sure computers in different areas can talk to each other using routers and a smart routing system called OSPF.

We've added a Host-Based Firewall and Network-Based Firewall to keep the network safe from bad stuff on the internet. And we've set up tools like SNMP, Syslog, TFTP, NTP, and AAA to help manage and secure the network better.

Trade-Offs

While the implemented design successfully meets the project requirements, there are some trade-offs to consider. The use of VLANs and routing protocols adds complexity to the network configuration, requiring careful planning and management.

Network Future

Looking forward to the fact that we can keep improving the network. We might upgrade the hardware to handle more traffic, add extra security measures like IPS, and try out new tech like SDN to make things easier to manage. With some upkeep and staying on top of new tech, the network will keep supporting the school's needs and growing along with it.

References

[1] “What Is a Network Firewall?,” Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-network-firewall

[2] “Single DHCP server for multiple VLANs (packet tracer),” Network Engineering Stack Exchange. https://networkengineering.stackexchange.com/questions/54252/single-dhcp-server-for-multiple-vlans-packet-tracer

[3] “SNMP Configuration Guide - Configuring SNMP Support [Cisco ASR 1000 Series Aggregation Services Routers],” Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book/nm-snmp-cfg-snmp-support.html

[4] T. Fisher, “What You Need to Know About Network DNS Servers,” Lifewire, Jul. 18, 2022. https://www.lifewire.com/what-is-a-dns-server-2625854