University of Europe for Applied Sciences

Software Engineering, BSc

PW24 — IT Platforms — Group B

Professor R. Kouatly

# “Simple Enterprise Network” Project

created by Ilnaza Saifutdinova, 60982580

# Table of Contents

# Brief Review

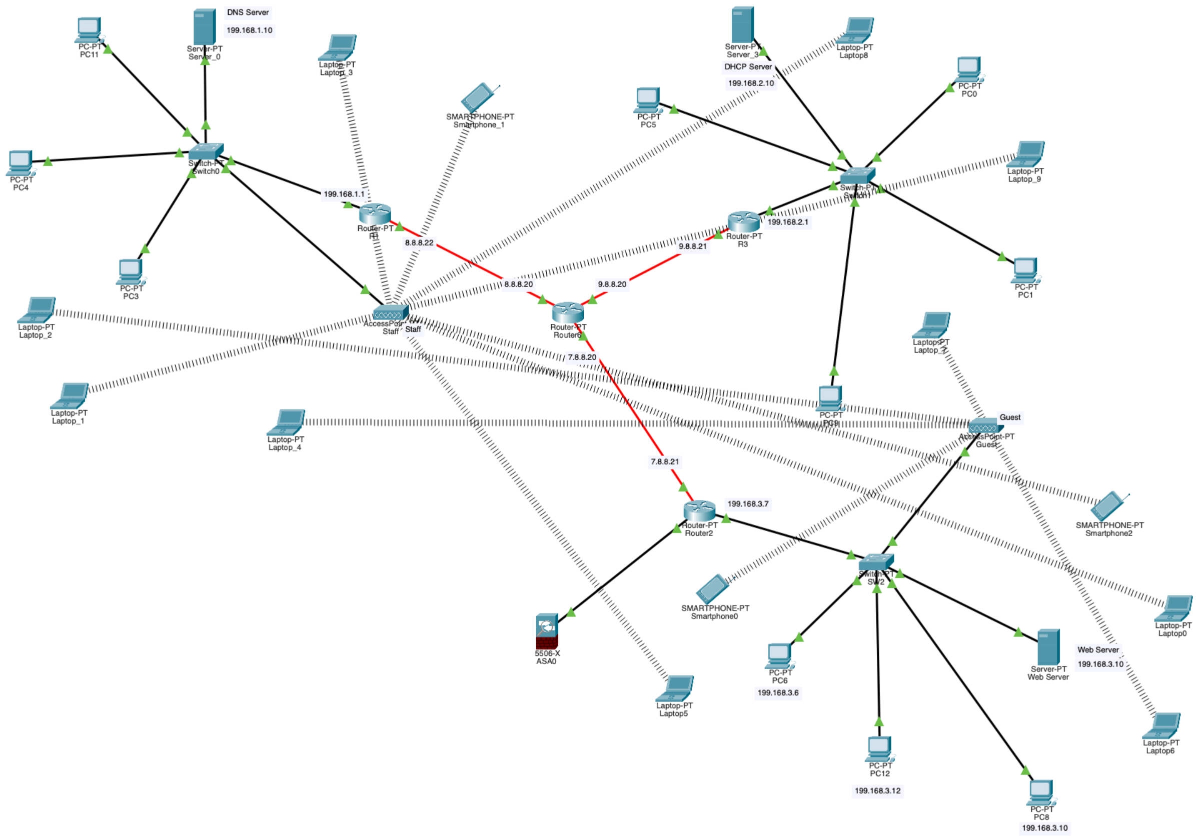
The goal of this report is to explain the design, setup, and testing of an enterprise network using Cisco Packet Tracer. It describes the network structure, which includes three subnets, routers, switches, servers (DNS, Web, and DHCP), and wireless devices. The report covers the use of Class A IP addresses for the WAN and Class C IP addresses for the internal network, along with the configuration of routers, switches, firewalls, and access points. It also looks at security measures, the wireless setup, and tests to ensure the network works correctly, including checking DNS, web server access, and DHCP.
Finally, the report evaluates the network's performance and identifies its strengths and areas that could be improved.

The enterprise network comprises three subnets, interconnected by routers and a central router ***Router-PT Router6*** linking the network to the ***WAN***. Each subnet is designed to serve specific functions, such as hosting DNS, Web, and DHCP services.
The task was to create a simulation of the enterprise computer network using ***Cisco Packet Tracer***
The network has the following equipments:

- 10 work stations,
- 3 Switches,
- 4 Routers,
- 3 Servers: 1 Web server, 1 DHCP Server, 1 DNS Server,
- Wireless Access points
- 3 Employees Mobile devices,
- 10 randomly distributed Laptops,
- 1 Firewall.

# Network Topology

The Enterprise Network Project involves designing and setting up a network with three subnets, each connected by routers and a central router that links to the WAN using a Class A IP address.
***Subnet 1*** includes 1 router (Router-PT R1), 1 switch (Switch-PT SW1), 1 DNS server (Server-PT Server_0), 3 workstations (PC-PT PC3, PC-PT PC11, PC-PT PC4), and 7 wireless devices (laptops and smartphones connected through AccessPoint-PT Staff).
***Subnet 2*** has 1 router (Router-PT R2), 1 switch (Switch-PT SW2), 1 web server (Server-PT WebServer), 3 workstations (PC-PT PC6, PC-PT PC12, PC-PT PC8), 5 wireless devices (laptops and smartphones connected through AccessPoint-PT Guest), and a firewall (5506-X ASA0).
***Subnet 3*** includes 1 router (Router-PT R3), 1 switch (Switch-PT SW3), 1 DHCP server (Server-PT Server_3), and 4 workstations (PC-PT PC5, PC-PT PC0, PC-PT PC1, PC-PT PC9).



The routers are connected by optical fiber for fast data transfer, and each subnet uses switches to manage the local traffic. Wireless access points in Subnet 1 and Subnet 2 allow mobility for up to 12 laptops and smartphones. The network uses Class A IP addresses for the WAN and Class C IP addresses for internal communication. Most devices get their IP addresses from the DHCP server, while servers and routers have static IPs. The firewall in Subnet 2 helps keep the network secure. The project was tested to check connectivity, domain name resolution, web server access, and DHCP function. The report ends with a summary of the project's results, pointing out the strengths and challenges.

# Class A and Class C IP Addresses

In networking, IP addresses are used to identify devices and allow them to communicate with each other. IP addresses are divided into different classes based on the size of the network they can support. Two of the most commonly used address classes are Class A and Class C, which are suitable for large and small networks.

— Class A IP Address: ***Class A IP addresses*** are designed for large networks and can support a large number of devices. They range from ***1.0.0.0*** to ***127.255.255.255***. Class A networks can handle millions of devices, making them ideal for large enterprise networks or Wide Area Networks (WANs). In this project, ***Class A IP addresses*** are used for the ***WAN*** network, specifically from ***7.8.8.20*** to ***9.8.8.50***. This range provides flexibility and scalability as the network grows and connects multiple subnets.

— Class C IP Address: ***Class C IP addresses*** are typically used for smaller networks, such as Local Area Networks (LANs), where fewer devices are connected. They range from

***192.0.0.0*** to ***223.255.255.255***, supporting up to 254 devices. Class C networks are ideal for internal networks. In this project, ***Class C IP addresses*** are used for the ***local networks (subnets)***, with the range from ***199.168.1.1*** to ***199.168.3.254***, which accommodates the devices across the three subnets.
By using ***Class A*** for the WAN and ***Class C*** for the local networks, this design ensures that the network is scalable for external connections while efficiently managing internal communication between devices.

## Subnet Design & Components

Certainly! Here's a brief paragraph for each subnet, explaining the purpose of each subnet and how the servers are integrated:

### **Subnet 1**:

This subnet is designed to host the primary internal devices, including workstations and mobile devices. It features ***Server_0***, which acts as the ***DNS Server*** for the network. The DNS server is crucial for translating domain names into IP addresses, enabling communication between devices using hostnames instead of IP addresses. Devices in this subnet, such as ***PCs***, ***Laptops***, and ***Smartphones***, are dynamically assigned IP addresses via ***DHCP***, allowing for easy management and configuration. The ***AccessPoint-PT Staff*** provides wireless connectivity, ensuring that employees can access the network without the need for physical connections.

| Device Type | Device Type | Connected to | Connection Type |
|---|---|---|---|
| Router-PT R1 | Router | Switch-PT Switch0,<br>***Router-PT R6*** | Ethernet,<br>***Optical Fiber*** |
| Switch-PT Switch0 | Switch | DNS Server, PCs | Ethernet |
| Server-PT Server_0 | DNS Server | Switch-PT Switch0 | Ethernet |
| PC-PT PC3 | Workstation | Switch-PT Switch0 | Ethernet |
| PC-PT PC4 | Workstation | Switch-PT Switch0 | Ethernet |
| PC-PT PC11 | Workstation | Switch-PT Switch0 | Ethernet |
| AccessPoint-PT Staff | Wireless AP | Switch-PT Switch0 | Ethernet |
| Laptop-PT Laptop_1 | Laptop | AccessPoint-PT Staff | Wireless |
| Laptop-PT Laptop_3 | Laptop | AccessPoint-PT Staff | Wireless |

| | | | |
|---|---|---|---|
| Laptop-PT Laptop_5 | Laptop | AccessPoint-PT Staff | Wireless |
| Laptop-PT Laptop_9 | Laptop | AccessPoint-PT Staff | Wireless |
| Smartphone-PT Smartphone_1 | Mobile Device | AccessPoint-PT Staff | Wireless |
| Smartphone-PT Smartphone_2 | Mobile Device | AccessPoint-PT Staff | Wireless |

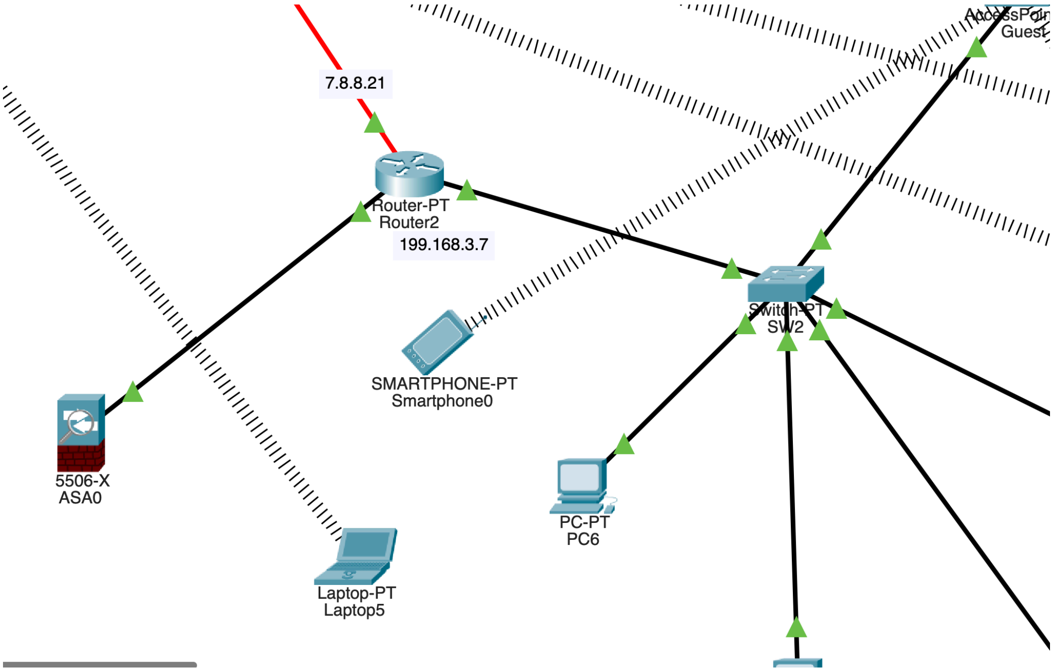
## **Subnet 2**:

Subnet 2 is primarily designed for web services and guest access. It includes ***WebServer***, which hosts the company's website and other web services that can be accessed externally or internally. Devices in this subnet, including ***PCs***, ***Laptops***, and ***Smartphones***, are also dynamically assigned IP addresses. The ***AccessPoint-PT Guest*** provides wireless connectivity to guest devices, keeping them isolated from the main internal network while still offering access to the internet and other necessary services. This subnet's design ensures that external and internal services are separated, maintaining security and performance.

| Device Type | Device Type | Connected to | Connection Type |
|---|---|---|---|
| Web Server | Web Server | Switch-PT SW2 | Ethernet |
| PC6 | Workstation | Switch-PT SW2 | Ethernet |
| PC8 | Workstation | Switch-PT SW2 | Ethernet |
| PC12 | Workstation | Switch-PT SW2 | Ethernet |
| AccessPoint-PT Guest | Wireless AP | Switch-PT SW1 | Ethernet |
| Laptop-PT Laptop_2 | Laptop | AccessPoint-PT Guest | Wireless |
| Laptop-PT Laptop_4 | Laptop | AccessPoint-PT Guest | Wireless |
| Laptop-PT Laptop_6 | Laptop | AccessPoint-PT Guest | Wireless |
| Laptop-PT Laptop_7 | Laptop | AccessPoint-PT Guest | Wireless |
| Smartphone-PT | Mobile Device | AccessPoint-PT | Wireless |

| | | | |
|---|---|---|---|
| Smartphone_0 | | Guest | |
| 5506-X ASA0 | Firewall | Switch-PT SW2 | Wireless |
| Router-PT R2 | Router | Switch-PT SW2,<br>***Router-PT R6*** | Wireless,<br>***Optical Fiber*** |

**Subnet 2**: Firewall



The **5506-X ASA0** firewall in this network helps protect it from outside threats. It checks all the data coming into and going out of the network to make sure nothing harmful, like viruses or hackers, can get through. It also controls who can access different parts of the network, making sure only trusted devices and users can connect. This helps keep the network safe and secure.

## **Subnet 3**:

Subnet 3 is dedicated to managing ***DHCP*** services within the network. The ***Server_3*** is configured as the ***DHCP Server***, responsible for assigning dynamic IP addresses to devices in this subnet and potentially other subnets. Devices such as ***PCs*** and ***Laptops*** within this subnet receive their IP addresses from this server, allowing them to connect seamlessly to the network. This subnet helps reduce the administrative burden of manually assigning static IP addresses, ensuring devices can quickly connect to the network. The ***Switch-PT Switch1*** facilitates communication between all devices in this subnet.

| Device Type | Device Type | Connected to | Connection Type |
|---|---|---|---|
| Server-PT Server1 | DHCP Server | Switch-PT Switch1 | Ethernet |
| PC0 | Workstation | Switch-PT Switch1 | Ethernet |

| | | | |
|---|---|---|---|
| PC1 | Workstation | Switch-PT Switch1 | Ethernet |
| PC5 | Workstation | Switch-PT Switch1 | Ethernet |
| PC9 | Workstation | Switch-PT Switch1 | Ethernet |
| Switch-PT Switch1 | Switch | Router-PT R3,<br>***Router-PT R6*** | Ethernet,<br>***Optical Fiber*** |

Each subnet is logically separated to handle different network tasks, ensuring that internal services like DNS, web hosting, and DHCP are efficiently managed while maintaining security and scalability across the network.

# Router Configurations

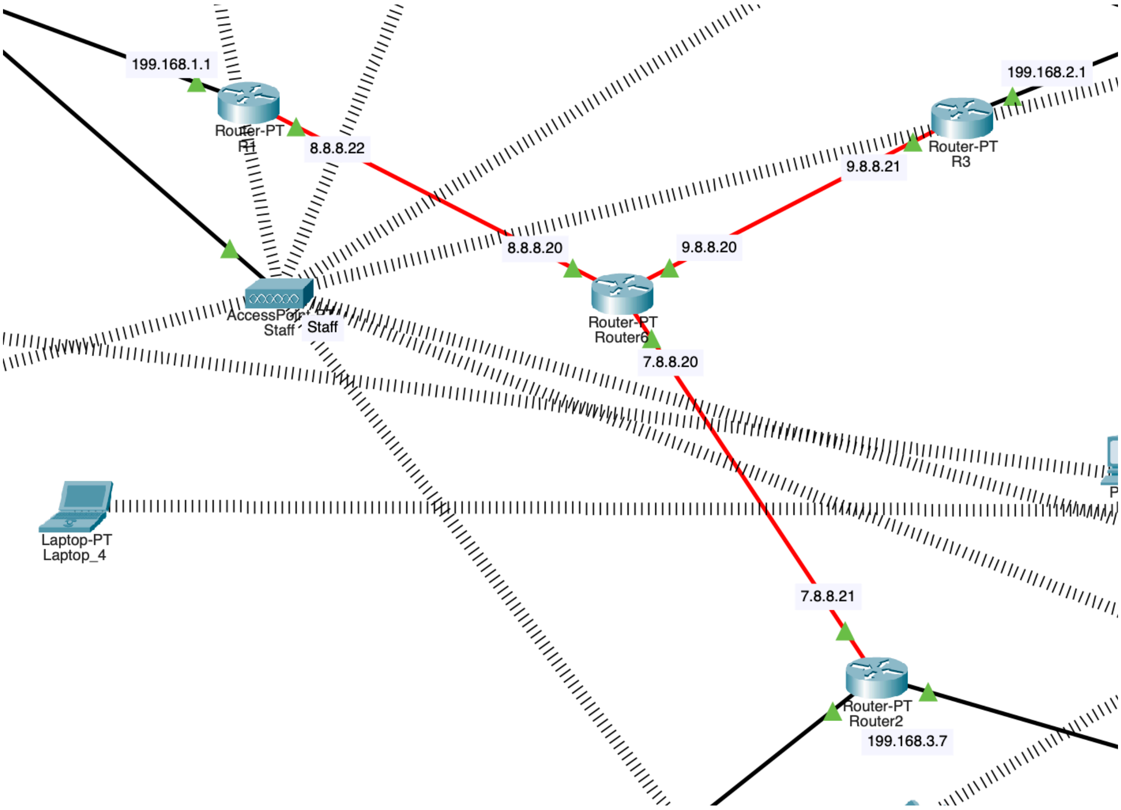
Connection Details:

Router6 is the ***core router*** that connects the internal network to the ***WAN***. It is connected directly to Router R1, Router R2, and Router R3 through FastEthernet interfaces (Fa4/0, Fa5/0, Fa6/0), each with a unique ***Class A IP address*** (from 7.8.8.20 to 9.8.8.21). This ensures proper communication between the routers and the network.

Router R1 connects **Subnet 1** to the network. Its Fa0/0 interface is connected to ***Switch0*** (199.168.1.1), allowing devices in this subnet to communicate and access resources. Router2 manages ***Subnet 2***, with its Fa0/0 interface using IP ***199.168.3.7***, and Router R3 manages ***Subnet 3***, with IP ***199.168.2.1*** on its Fa4/0 interface. These routers are connected to their respective switches (***SW2*** and ***Switch1***), which help manage communication within the local subnets.

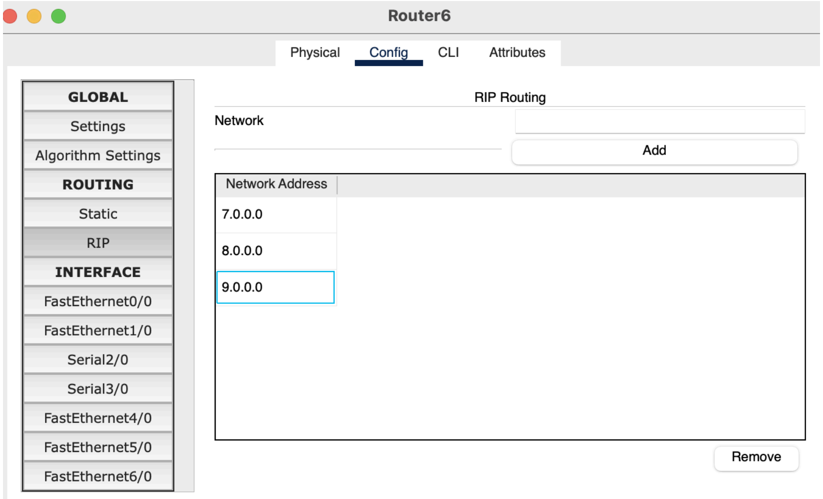
The routers in this network use ***RIP (Routing Information Protocol)*** for dynamic routing between subnets, ensuring smooth communication between devices in different subnets. The ***core router (Router6)*** connects the network to the WAN using ***Class A IP addresses***, while ***Router R1, Router2, and R3*** manage their local subnets with ***Class C IP addresses***. ***Optical fiber*** links provide high-speed connections between the routers, and ***FastEthernet*** interfaces connect the routers to the local switches, supporting communication within and between the subnets.

The picture of four routers connected together:



“The Core Router Router6 — Subnets’ Routers” Configuration

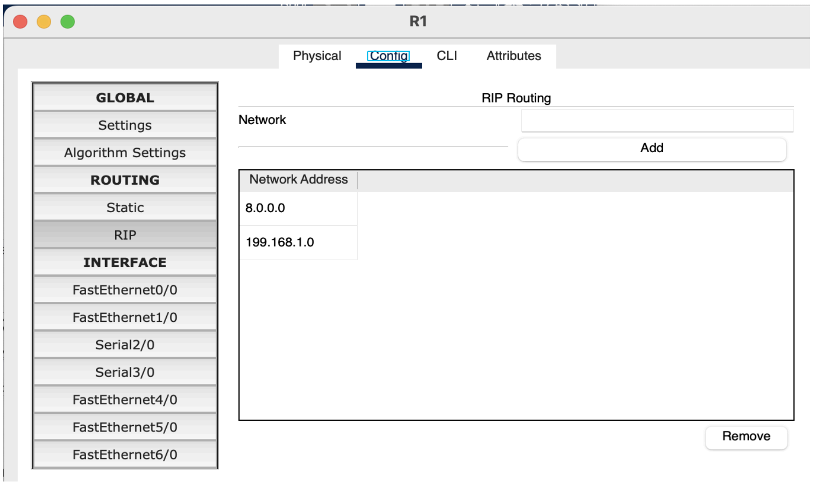
<table>
<tr><td>Router name</td><td>Interface</td><td>IP Address</td></tr>
<tr><td>Router6</td><td>Fa4/0</td><td>8.8.8.20</td></tr>
<tr><td colspan="3">This interface connects Router6 to Router R1 (Fa4/0) with IP Address 8.8.8.22</td></tr>
<tr><td>Router6</td><td>Fa5/0</td><td>9.8.8.20</td></tr>
<tr><td colspan="3">This interface connects Router6 to Router R1 (Fa4/0) with IP Address 9.8.8.21</td></tr>
<tr><td>Router6</td><td>Fa6/0</td><td>7.8.8.20</td></tr>
<tr><td colspan="3">This interface connects Router6 to Router R1 (Fa4/0) with IP Address 7.8.8.21.</td></tr>
</table>



| Network Address |
|---|
| 7.0.0.0 |
| 8.0.0.0 |
| 9.0.0.0 |

## “Router-PT Router R1 — Switch-PT Switch0” Configuration

| Router name | Interface | IP Address |
|---|---|---|
| Router R1 | Fa0/0 | 199.168.1.1 |
| This interface connects Router R1 to Switch0 within Subnet 1 (the local network), allowing communication between devices in this subnet | | |

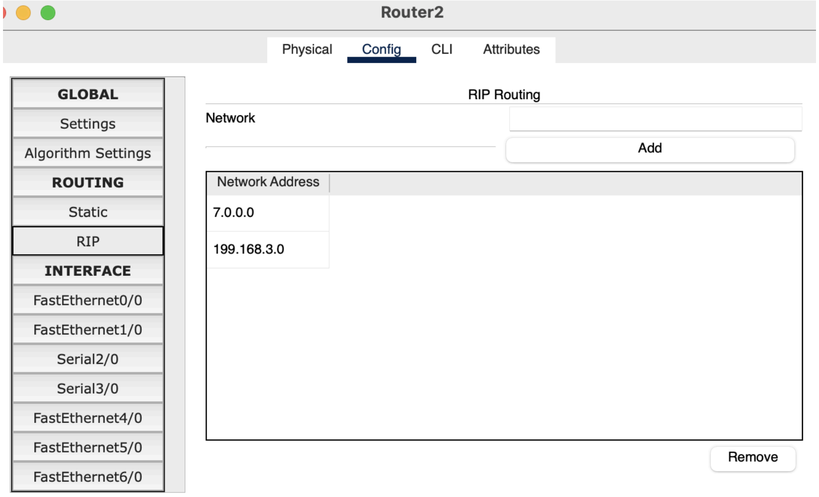


| Network Address |
|---|
| 8.0.0.0 |
| 199.168.1.0 |

## “Router-PT Router2 — Switch-PT Switch SW2” Configuration

| Router name | Interface | IP Address |
|---|---|---|
| Router Router2 | Fa0/0 | 199.168.3.7 |

This interface connects Router2 to Switch SW2 within Subnet 2. Devices in Subnet 2 will use this router for routing traffic

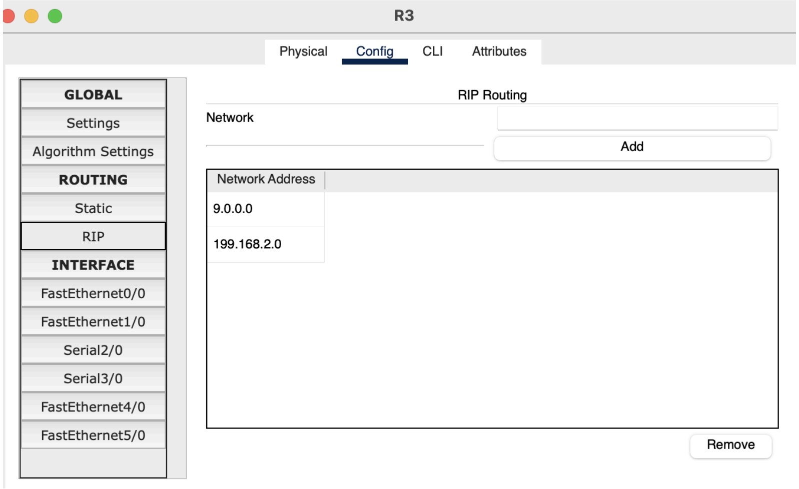


| Network Address |
|---|
| 7.0.0.0 |
| 199.168.3.0 |

## “Router-PT Router R3 — Switch-PT Switch1” Configuration

| Router name | Interface | IP Address |
|---|---|---|
| Router R3 | Fa4/0 | 199.168.2.1 |

This interface connects Router R3 to Switch1 in Subnet 3, managing internal communication within Subnet 3



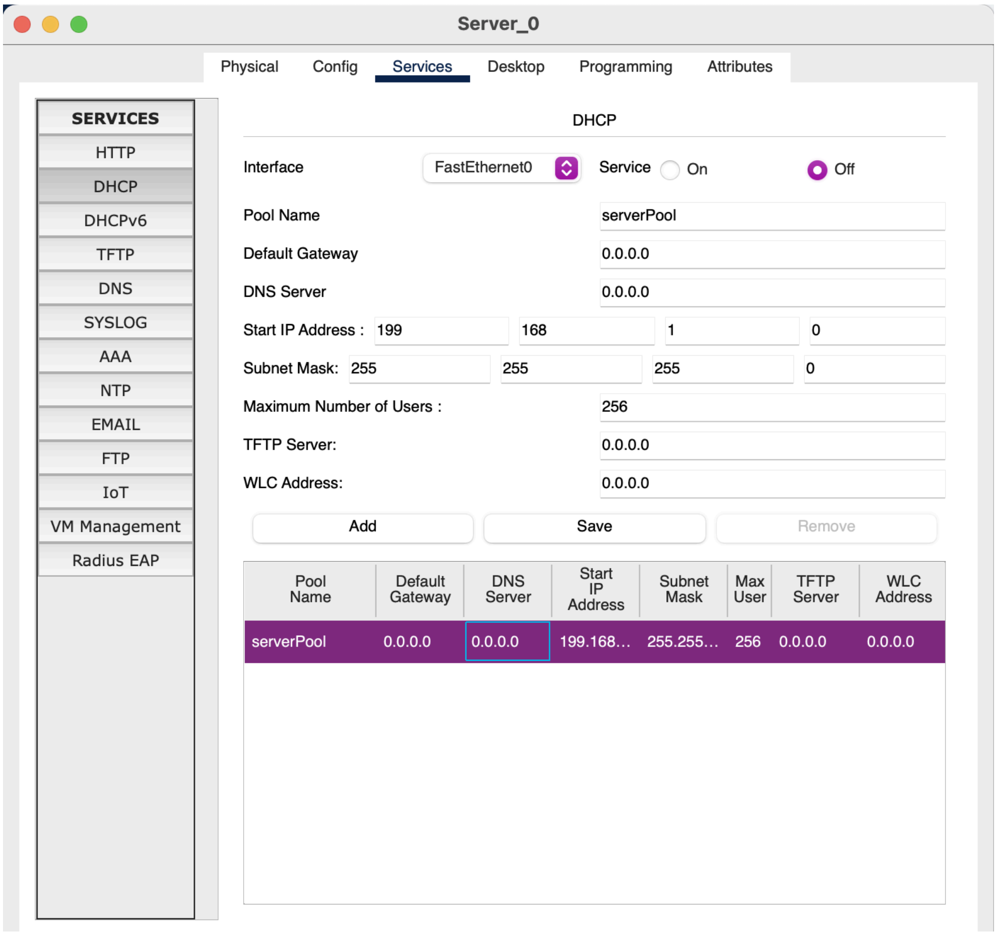
| Network Address |
|---|
| 9.0.0.0 |
| 199.168.2.0 |

# Server Configurations

In this network design, three key servers play a crucial role in providing essential services to the network: the ***DNS Server***, ***DHCP Server***, and ***Web Server***. These servers are connected to the network through routers and switches, and they are responsible for ensuring smooth communication, address allocation, and access to internal and external resources.

1. DNS Server (Server_0):

The ***DNS Server*** is responsible for resolving domain names to IP addresses within the network. It helps ensure that devices can access websites and services using domain names instead of IP addresses. In this network, the DNS Server is connected to ***Router R1*** through its Ethernet interface. Devices within the network, such as ***PCs*** and ***Laptops***, are configured to use this DNS server to resolve domain names. The connection between the devices and the server is made through switches (***Switch0, Switch1, SW2***) and ***Routers***.



DHCP

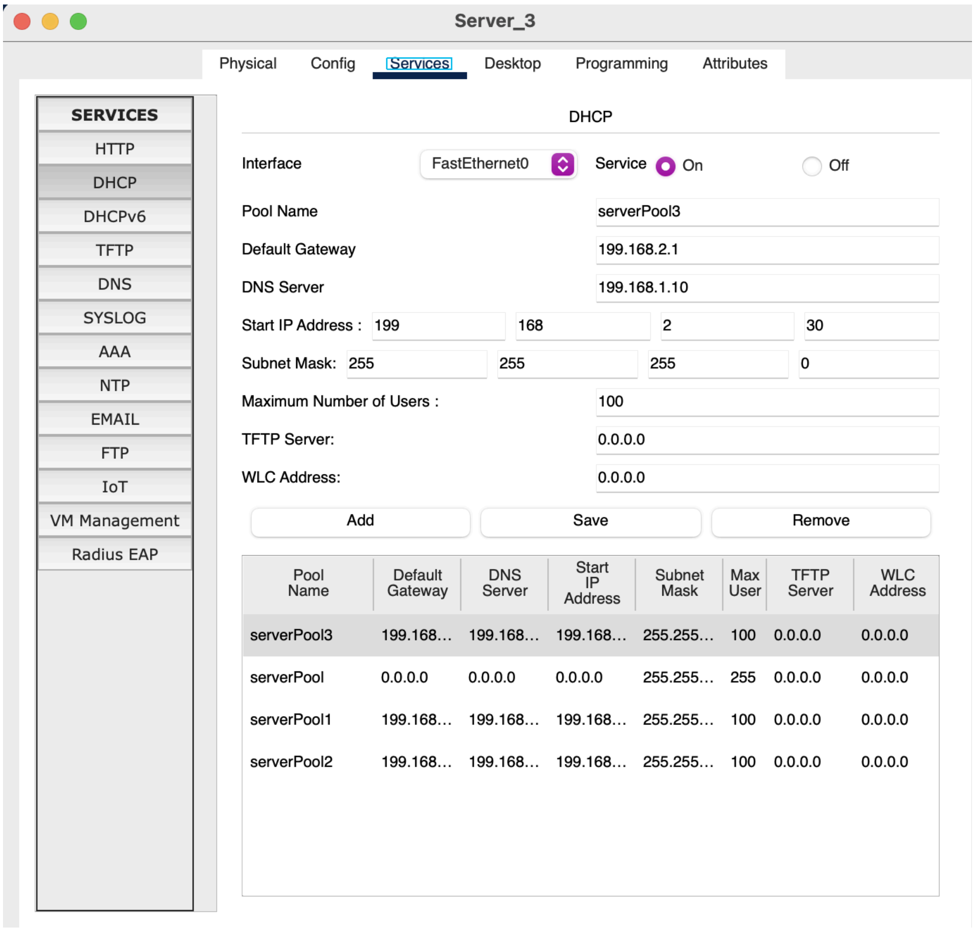
Interface: FastEthernet0
Service ○ On ● Off

Pool Name: serverPool
Default Gateway: 0.0.0.0
DNS Server: 0.0.0.0
Start IP Address : 199 168 1 0
Subnet Mask: 255 255 255 0
Maximum Number of Users : 256
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|---|---|---|---|---|---|---|---|
| serverPool | 0.0.0.0 | 0.0.0.0 | 199.168… | 255.255… | 256 | 0.0.0.0 | 0.0.0.0 |

2. DHCP Server (Server_3):

The ***DHCP Server*** dynamically assigns IP addresses to devices within the network. This eliminates the need for manual IP address configuration on each device. In this setup, the DHCP server is connected to ***Router R3***, with the router's interface providing access to ***Subnet 3***. ***Laptops, PCs, Smartphones***, and other devices are connected to the network via ***wired connections*** (through ***Switches***) or ***wirelessly*** (via ***Access Points***). When a device joins the network, it sends a DHCP request, and the server assigns an available IP address from the configured range. This ensures that all devices receive proper IP addressing, enabling them to communicate with each other and the internet.

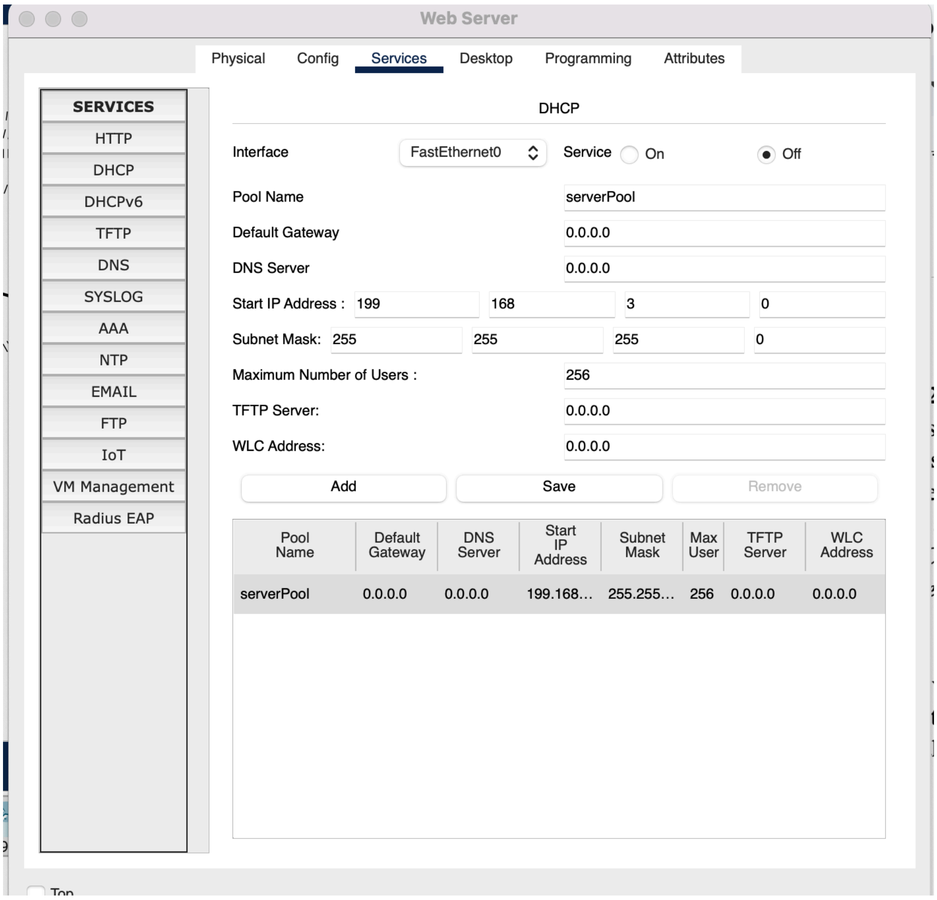


| | |
|---|---|
| Interface | FastEthernet0 |
| Service | ● On ○ Off |
| Pool Name | serverPool3 |
| Default Gateway | 199.168.2.1 |
| DNS Server | 199.168.1.10 |
| Start IP Address : | 199 168 2 30 |
| Subnet Mask: | 255 255 255 0 |
| Maximum Number of Users : | 100 |
| TFTP Server: | 0.0.0.0 |
| WLC Address: | 0.0.0.0 |

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|---|---|---|---|---|---|---|---|
| serverPool3 | 199.168... | 199.168... | 199.168... | 255.255... | 100 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 255.255... | 255 | 0.0.0.0 | 0.0.0.0 |
| serverPool1 | 199.168... | 199.168... | 199.168... | 255.255... | 100 | 0.0.0.0 | 0.0.0.0 |
| serverPool2 | 199.168... | 199.168... | 199.168... | 255.255... | 100 | 0.0.0.0 | 0.0.0.0 |

3. Web Server (WebServer):

The ***Web Server**** hosts the website and is connected to ***Router R2***, which links it to ***Subnet 2***. Devices within ***Subnet 2*** and other subnets can access the web server through the internal network or via the ***WAN***, depending on the routing and firewall rules in place. The web server is used for hosting and delivering web content to users. In this case, the ***Web Server*** is set up to serve internal websites or applications, ensuring that users can access resources via their browsers. Devices that need access to the web server, such as ***PCs*** and ***Laptops***, are either connected directly through wired connections or wirelessly via ***Access Points***.



DHCP

Interface FastEthernet0 Service ○ On ● Off

Pool Name serverPool

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Start IP Address : 199 168 3 0

Subnet Mask: 255 255 255 0

Maximum Number of Users : 256

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|---|---|---|---|---|---|---|---|
| serverPool | 0.0.0.0 | 0.0.0.0 | 199.168… | 255.255… | 256 | 0.0.0.0 | 0.0.0.0 |

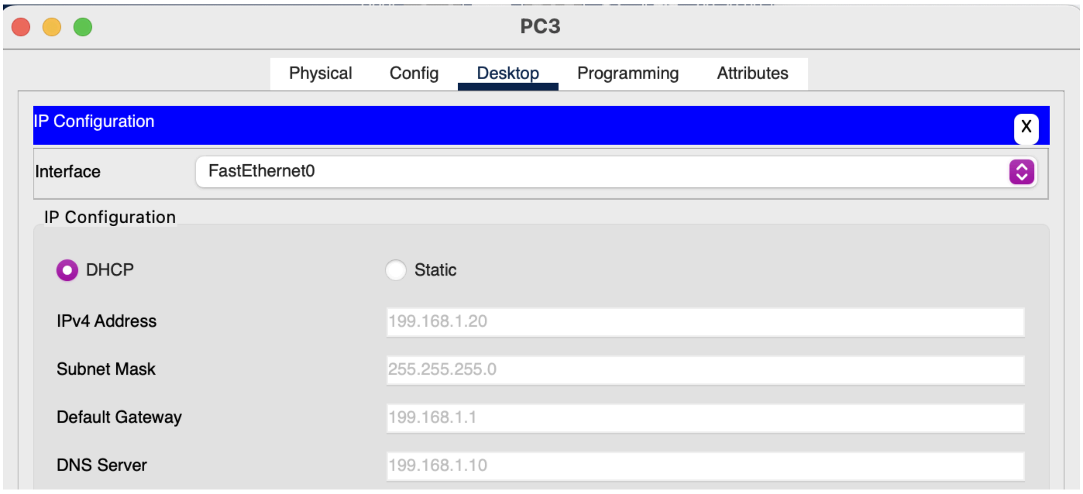
4. Connecting Devices to the DHCP Server: In this network, all devices, including ***Laptops***, ***PCs, Smartphones***, and other networked devices, are connected to the ***DHCP Server*** for automatic IP address assignment.

## The devices can connect in several ways:

## Wired and Wireless Configuration:

5. Wired Connections: Devices like ***PCs*** are connected to the network through ***Switches*** (Switch0, SW1, SW2). These switches provide connectivity between the devices and the ***DHCP Server***, ensuring that each device is assigned a unique IP address in the range specified by the server.

IP Address for PC3:



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 199.168.1.20

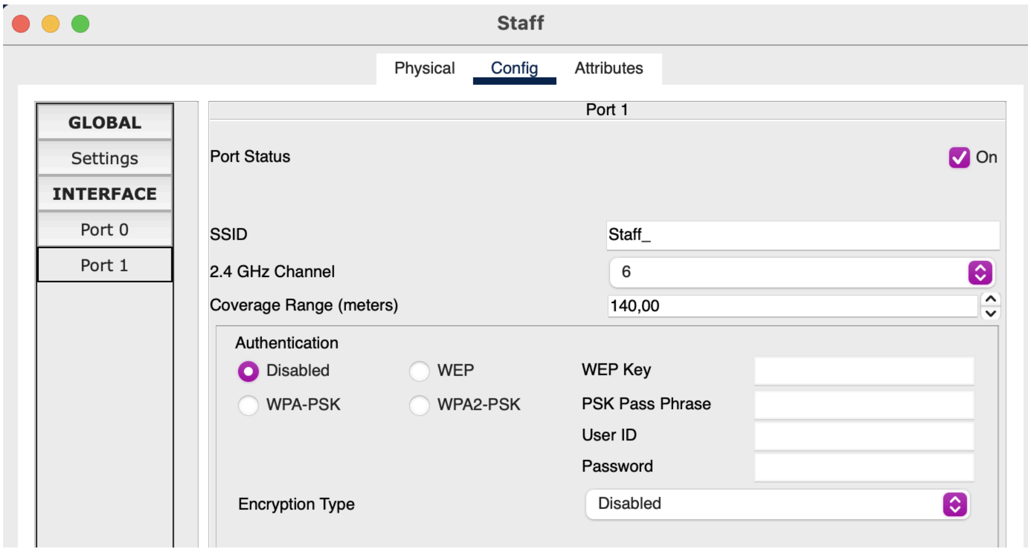
Subnet Mask: 255.255.255.0

Default Gateway: 199.168.1.1

DNS Server: 199.168.1.10

6. Wireless Connections: ***Mobile devices*** such as ***Smartphones*** and ***Laptops*** are connected wirelessly through ***Access Points*** (***AccessPoint-PT Staff*** and ***AccessPoint-PT Guest***). These access points provide wireless connectivity, allowing devices to obtain IP addresses from the ***DHCP Server*** via the routers and switches that are part of the network. The wireless access ensures flexibility, allowing devices to roam within the network and maintain consistent connectivity.

Each ***Access Point*** is configured with an ***SSID*** (***Service Set Identifier***) that identifies the wireless network, for example SSID "Staff_":



Port Status ☑ On

SSID: Staff_

2.4 GHz Channel: 6

Coverage Range (meters): 140,00

Authentication

● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK

WEP Key:

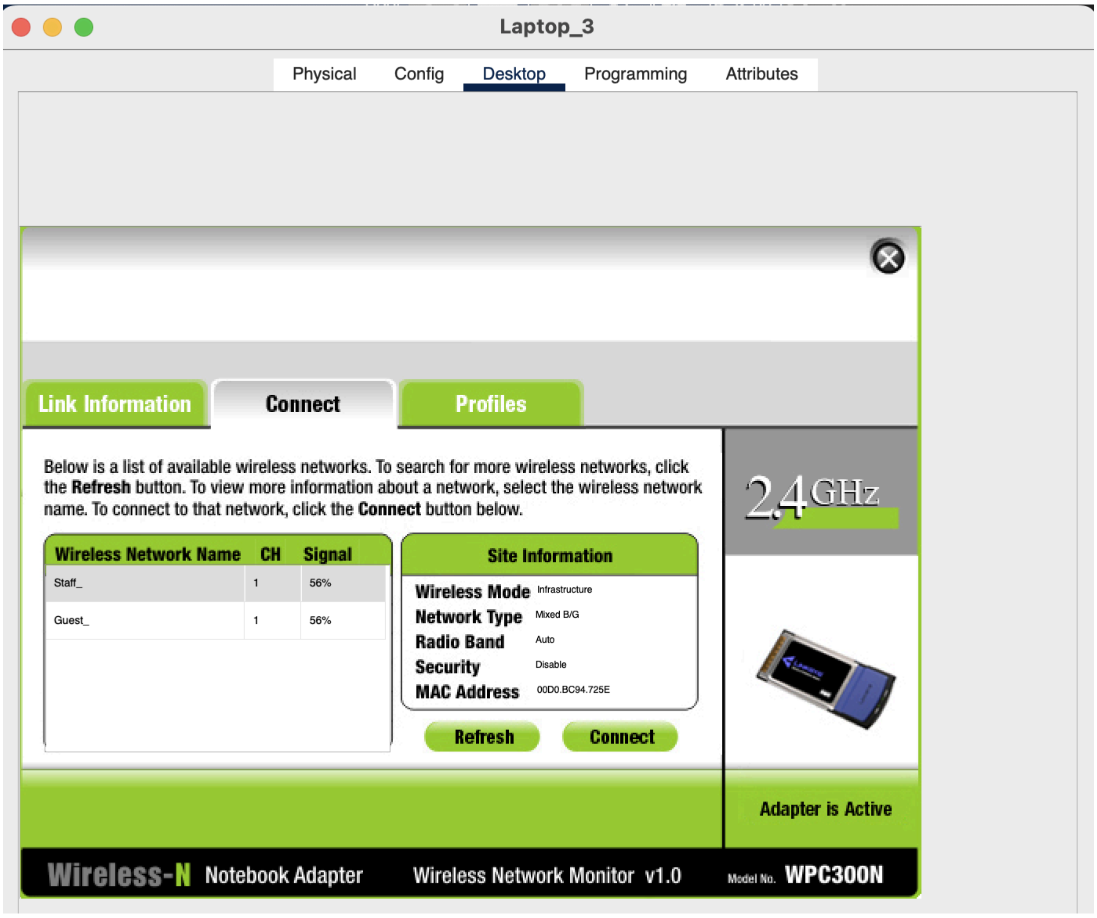
PSK Pass Phrase:

User ID:

Password:

Encryption Type: Disabled

Laptop_3 is connected with AccessPoint Staff:



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

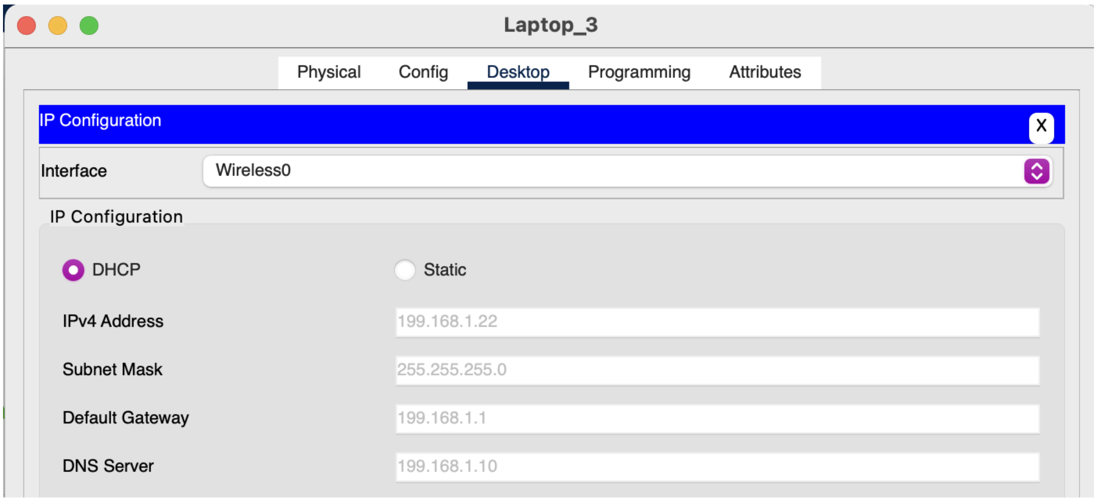
| Wireless Network Name | CH | Signal |
|---|---|---|
| Staff_ | 1 | 56% |
| Guest_ | 1 | 56% |

Site Information

| | |
|---|---|
| Wireless Mode | Infrastructure |
| Network Type | Mixed B/G |
| Radio Band | Auto |
| Security | Disable |
| MAC Address | 00D0.BC94.725E |

Refresh
Connect

IP Address for Laptop_3:



Interface: Wireless0

IP Configuration

● DHCP ○ Static

| | |
|---|---|
| IPv4 Address | 199.168.1.22 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 199.168.1.1 |
| DNS Server | 199.168.1.10 |

By using the ***DHCP Server***, this network automates the IP address assignment process, reducing configuration time for network administrators and minimizing the risk of IP address conflicts. Additionally, using the DNS Server helps simplify access to services by translating domain names to IP addresses, while the Web Server provides access to internal and external web resources.

# Result of the Project

1. ***Network Scalability***: The network is designed to be easily scalable. By using ***Class A IP Addresses*** for the WAN and ***Class C IP addresses*** for local subnets, it allows the network to grow as needed. More devices or subnets can be added without running out of IP addresses, ensuring long-term flexibility.

2. ***Simplified Address Management***: With the use of a ***DHCP server***, devices automatically receive IP addresses when they connect to the network. This automatic process reduces the need for manual IP configuration and prevents address conflicts, which is especially helpful in managing a large number of devices.

3. ***Fast and Reliable Connections***: By using ***Optical Fiber connections*** between the core router and other routers, the network ensures high-speed communication. This provides a reliable and fast connection between different subnets and the WAN, making it suitable for large-scale operations that require quick data transfer.

4. ***Wireless Mobility***: The wireless network setup, with ***Access Points*** for both staff and guest networks, offers flexibility for users to move around without losing their connection. Devices like laptops and smartphones can easily connect to the network without being limited by cables.

5. ***Efficient Routing***: The use of ***RIP*** enables dynamic routing within the network. This ensures that the network can quickly adapt to changes, find the best routes, and maintain connectivity even if a router or link fails, improving overall network stability.

6. ***Centralized Network Management***: The network includes centralized servers for ***DNS***, ***DHCP***, and ***Web hosting***, making it easier to manage, troubleshoot, and maintain the network. This centralization simplifies network operations and improves efficiency in handling services and resources.

7. ***Enhanced Security***: The network setup includes ***Firewalls*** and uses WPA2 or WPA3 encryption for wireless security. This ensures that both wired and wireless connections are protected from unauthorized access, keeping the network safe from external threats.

# Brief Conclusion

In conclusion, the network design successfully meets the requirements of a modern, scalable, and secure enterprise network. By using ***Class A IP addresses*** for the WAN and ***Class C IP addresses*** for internal subnets, the network ensures flexibility and efficient use of IP addresses. The use of a ***DHCP server*** simplifies IP address management, and the dynamic routing protocol ***RIP*** enhances communication between different subnets.

The inclusion of ***optical fiber connections*** and ***Access Points*** for wireless connectivity ensures fast, reliable, and flexible communication for all devices, both wired and wireless. The centralization of important services like ***DNS***, ***DHCP***, and ***Web hosting*** makes network management easier, while the ***Firewall*** and WPA2 encryption provide robust security.

Overall, this network setup is designed for ease of use, scalability, and security, making it a strong solution for an enterprise environment.

# References:

Cisco Networking Academy: Packet Tracer Tutorials

Official Cisco Documentation