Computer network Project by Bright Chukwuebuka Jiwueze

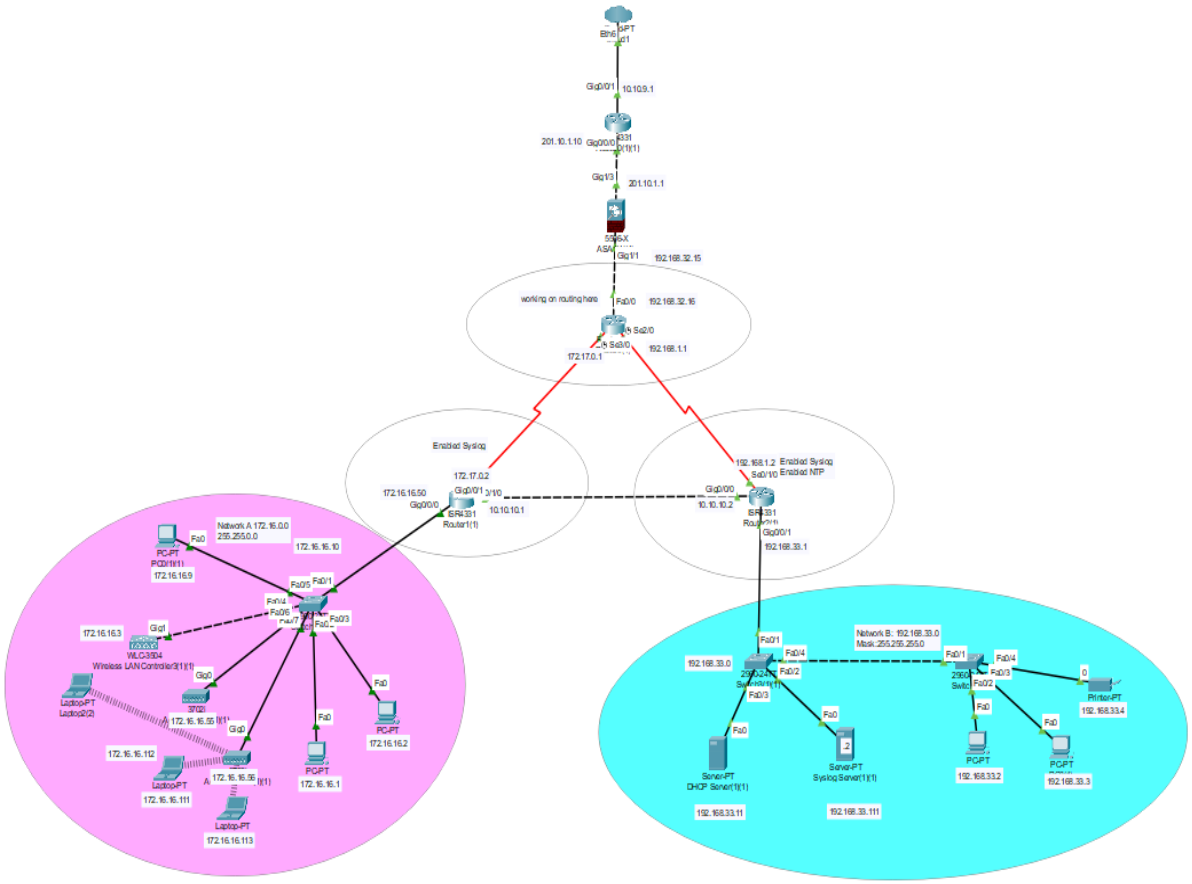
TECHNOLOGY USED: Cisco Packet Tracer

Introduction:

Network topology for a mid-sized organization presumed to be in Berlin. The office consists of the below list of Network & Security devices.

- 1 ASA Firewall
- 3 Routers
- 3 Access Switches
- 1 Wireless controller
- 2 Access points
- 1 DHCP server
- 1 Syslog server & NTP server
- 2 laptops & 5 Pc's
- 1 Printer

In this document, we discussed in detail the implementation of the entire topology with the corresponding configuration of each device.



Network A

Network A - IP configuration:

Network A is using a Class B IP address range. Class B was used because it is suitable for medium to large-sized networks.

In Class B networks, the first two octets represent the network portion of the IP address, while the last two octets are available for host assignment. With our network address of 172.16.0.0, the available range for the hosts extends from 172.16.0.1 to 172.16.255.254.

A brief explanation of the network values is given below:

- Private IP Range: 172.16.0.0 to 172.31.255.255 (See Private IP Addresses below for more information)
- Subnet Mask: 255.255.0.0 (16 bits)
- Number of Networks: 16,382
- Number of Hosts per Network: 65,534

Switch:

At the top of the network topology, we used a switch to connect various devices within a local area network (LAN) to facilitate the exchange of data packets. In Network A, our switch uses IP 172.16.16.10 and serves as a central point of connection for the following devices:

PC0, PC1, & PC2: Personal computer connected to the switch. It can be used for general computing tasks and data access such as pinging within the network.

WLC-3504 (Wireless LAN Controller): This device serves as a central management unit for wireless access points in the network. It allows for the control and configuration of the infrastructure of the wireless network.

Access Point: An access point is a device that allows wireless devices to connect to a wired network. In this topology, the access point is connected to the switch and

provides wireless connectivity to devices such as Laptop1 and Laptop2 in the network.

Configurations:

```
Switch>enable
Switch#conf t
sw1(config)#interface Vlan1
sw1(config-if)#ip address 172.16.16.10 255.255.0.0 1
sw1(config-if)#exit
sw1#copy run startup-config
```

Wires & Connections:

The switch is connected to the PCs and Access Points using Fast Ethernet ports. As a best practice, Copper Straight-Through cables was used for Fast Ethernet connections.

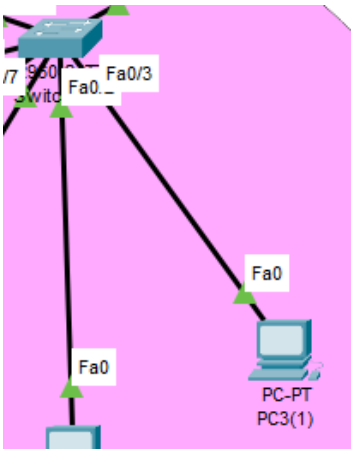


Figure 1: FastEthernet with Copper Straight-Through

To connect to the WLC, the GigabitEthernet port is configured and connected with Copper Cross-Over Cable.

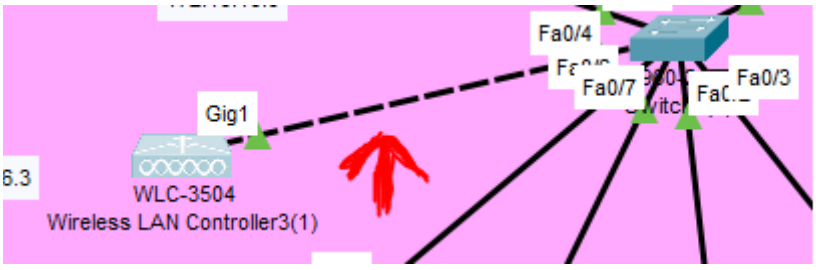


Figure 2: GigabitEthernet with Copper Cross-Over

Wireless LAN Controller (WLC-3504):

A wireless LAN controller (WLC) is a network component that manages wireless network access points and allows wireless devices to connect to the network. It provides centralized management of network components, improves network visibility, and makes monitoring of individual components simple.

To take control of routers, switches, firewalls, gateways, and other devices, WLCs are frequently used. In our network configuration, WLC is used with a combination of Access Points. So that Laptop0 and Laptop1 can use wireless networks.

Likewise, it is easier to manage APs from a single interface. WLC benefits us by bringing the option to have additional features such as security and roaming support.

Configuration:

Configure WLC with the settings below:

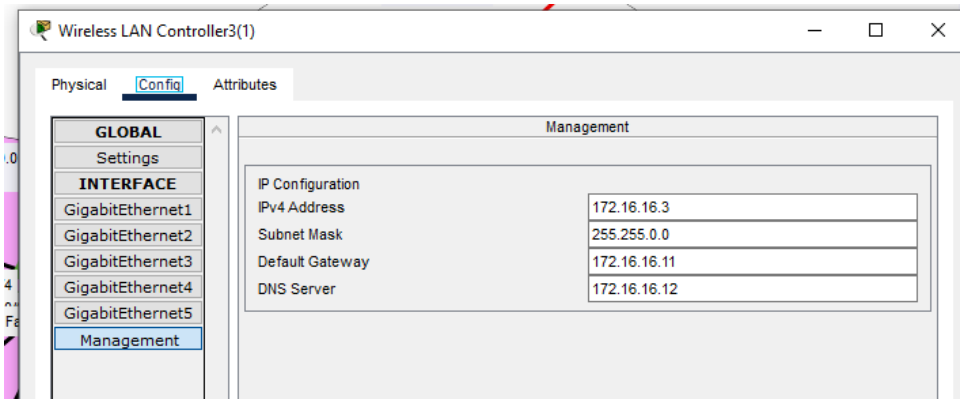
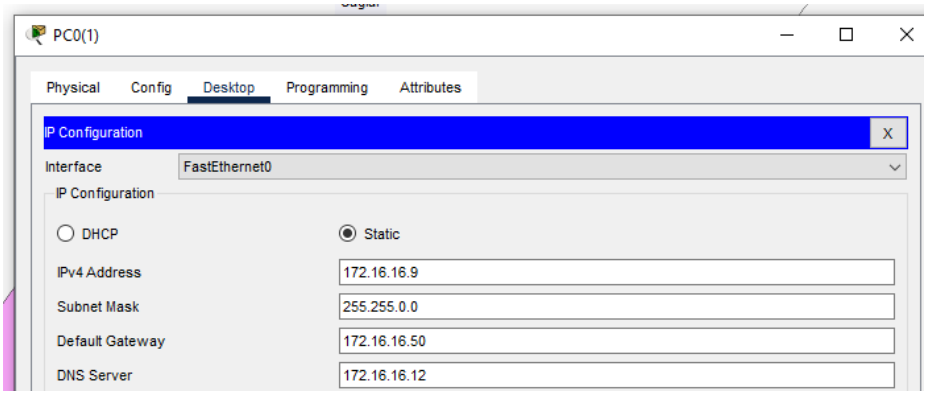


Figure 3: WLC Config

Configure PC's IP from Desktop -> IP configuration.



Login to the Cisco router webpage from the laptop (Desktop -> Web Browser)

We configured the webpage as http://172.16.16.3/

Figure 4: Login to WLC after config

Let's create our WLC with the settings below.

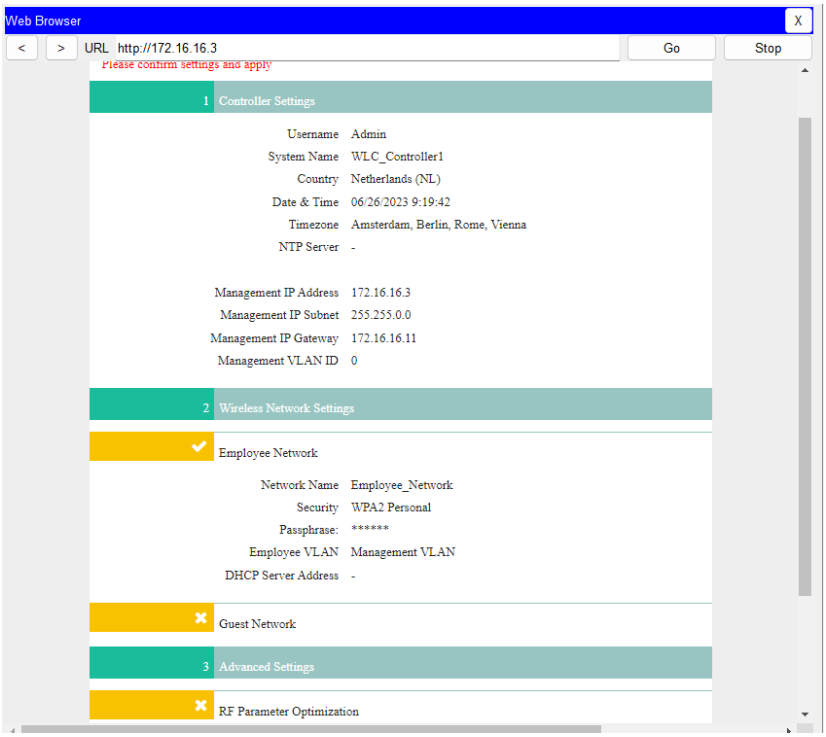


Figure 5: WLC Confirm Config Page

It might ask you to reboot the system. After waiting a while, we should be able to login to our WLC controller page.

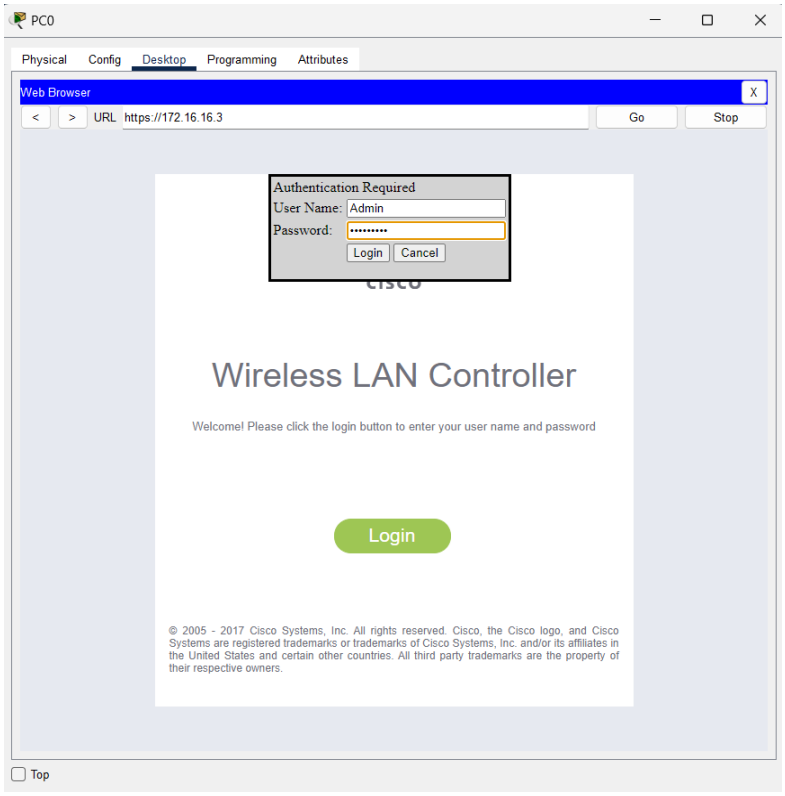


Figure 6: WLC Controller Page

Now we can monitor our network and APs using the controller page.

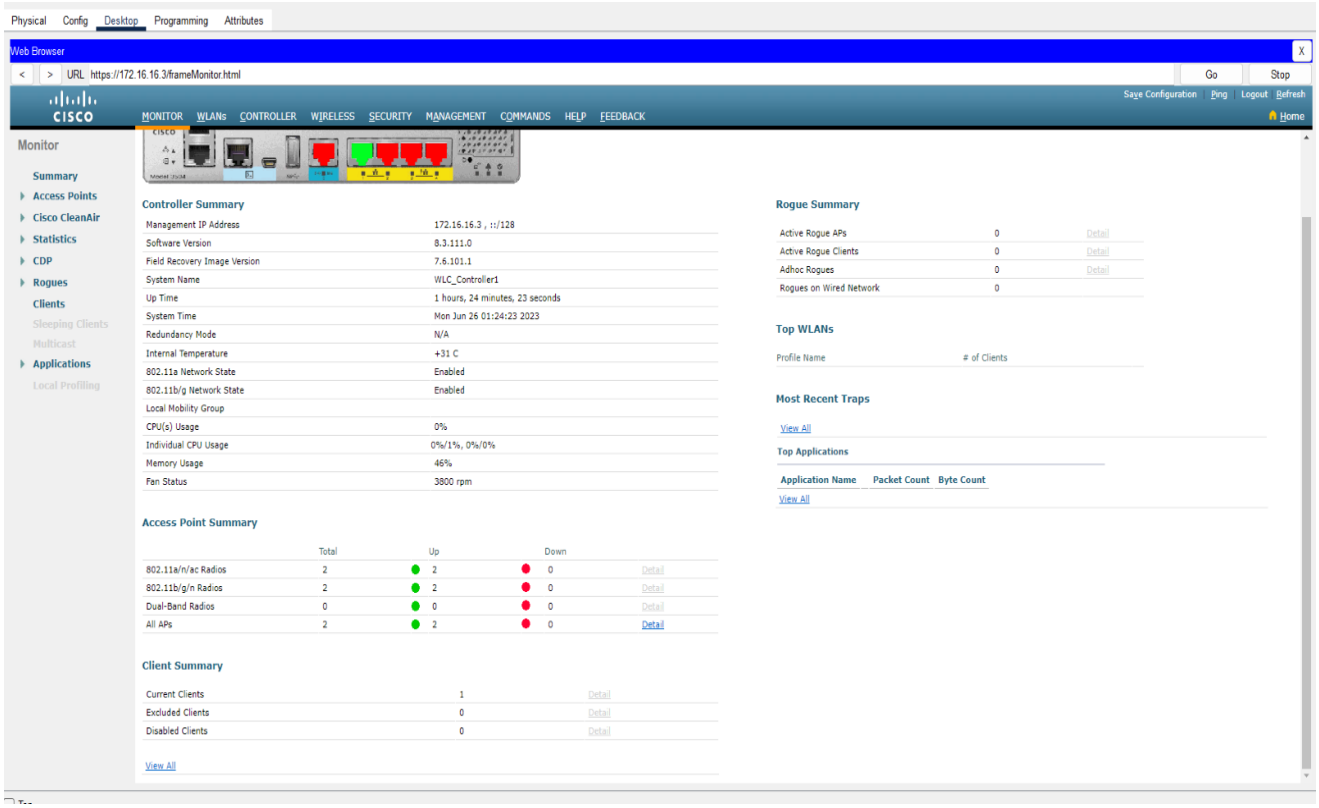


Figure 7: Monitoring network with controller page

Access Point

In our network topology, Access Points (AP) are used to provide wireless connectivity to devices within Network A. Those access points are a bridge between the wired network (connected to the switch) and wireless devices, such as laptops.

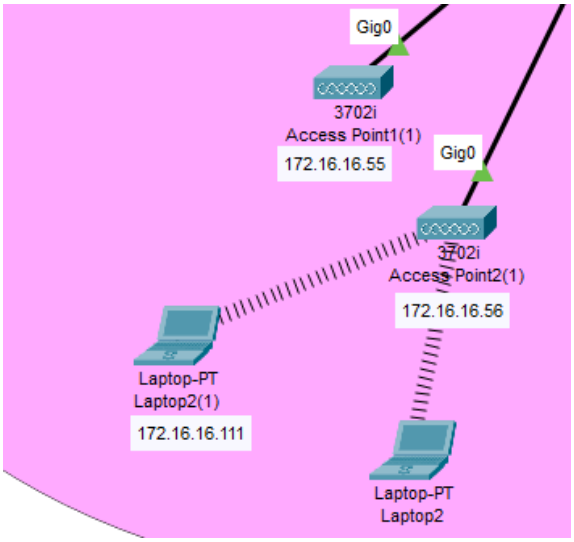


Figure 8: Access Point with laptops

Combining Access Points (APs) with a Wireless LAN Controller (WLC):

In Network A, we have combined Access Point 2 with our WLC. This offers several benefits that can be described as follows:

- **Centralized management**: In our WLC configuration (refer to Figure 7), it is possible to control all the APs in the network. An administrator can configure and monitor multiple APs in a single interface. This is an important step to simplify network administration.
- **Load Balancing:** With a WLC, client connections can be easily distributed evenly across multiple APs.
- **Increased Security:** A Wireless LAN Controller increases the security of the network by allowing centralized implementations of security measures including encryption, authorization, and authentication.

Configurations:

Configure the Access point as shown below.

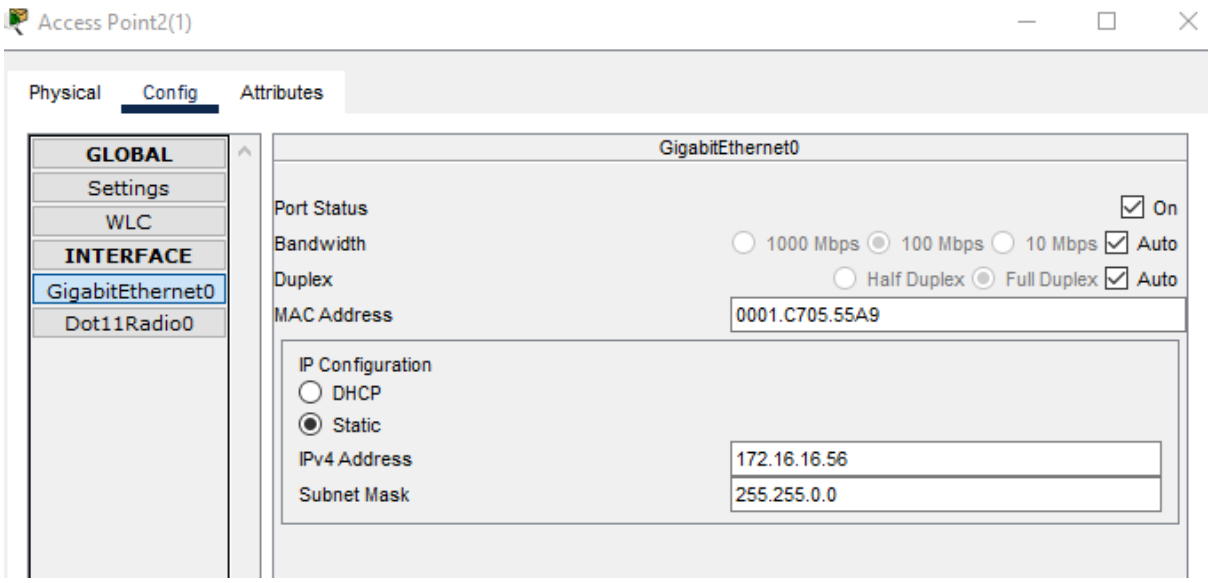
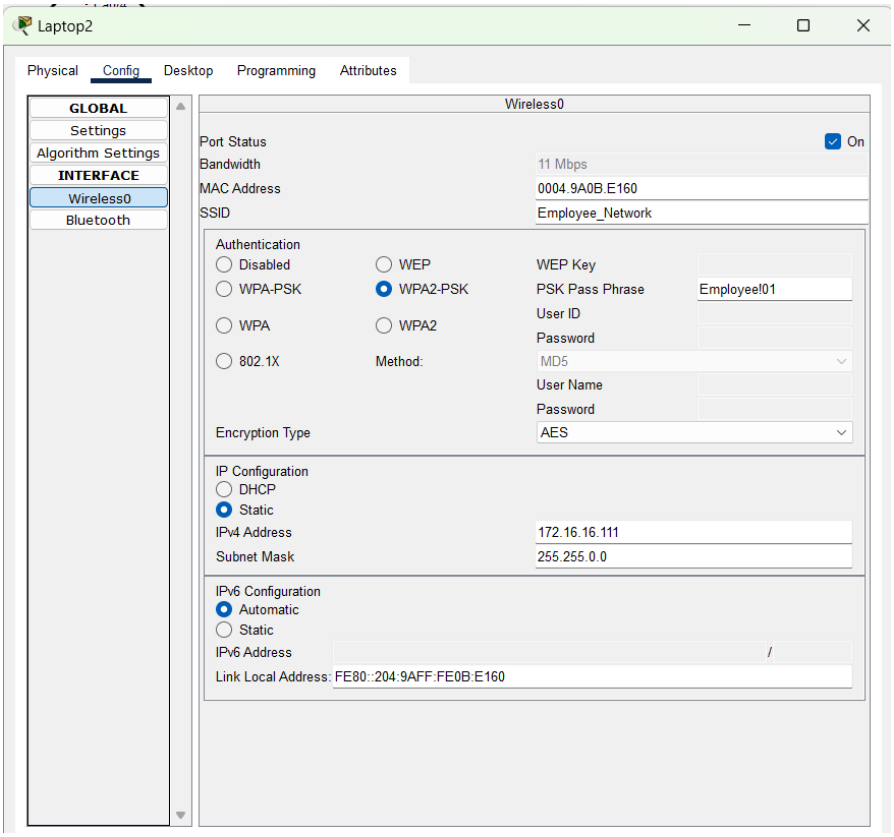
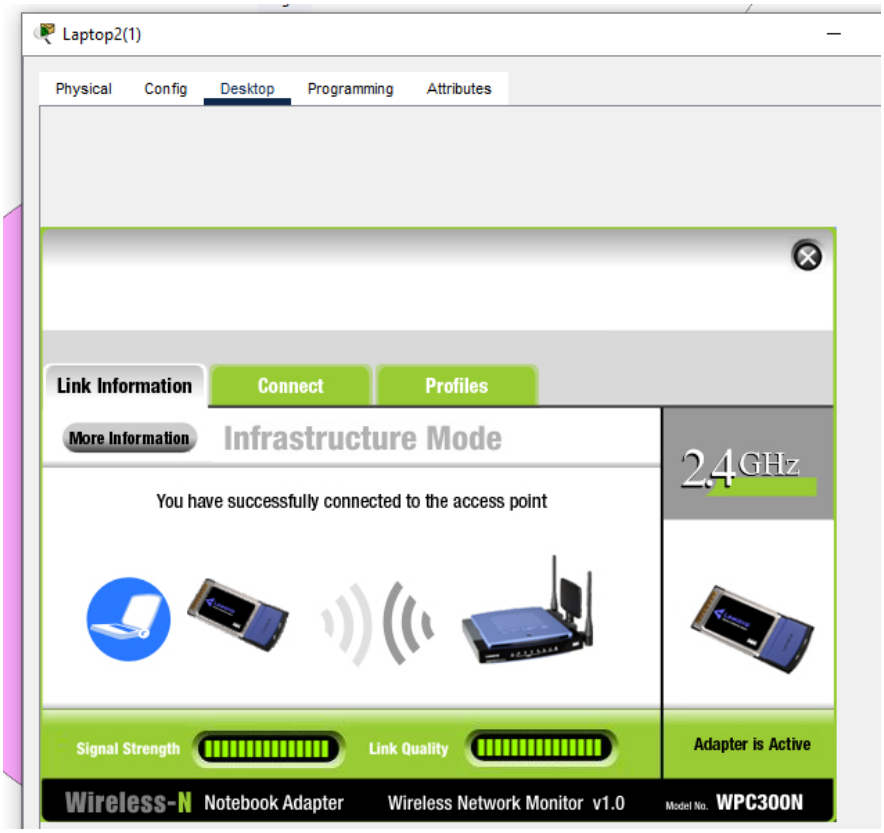


Figure 9: Access Point Config

Configure the Laptop and connect to the Wi-Fi that is created via WLC.

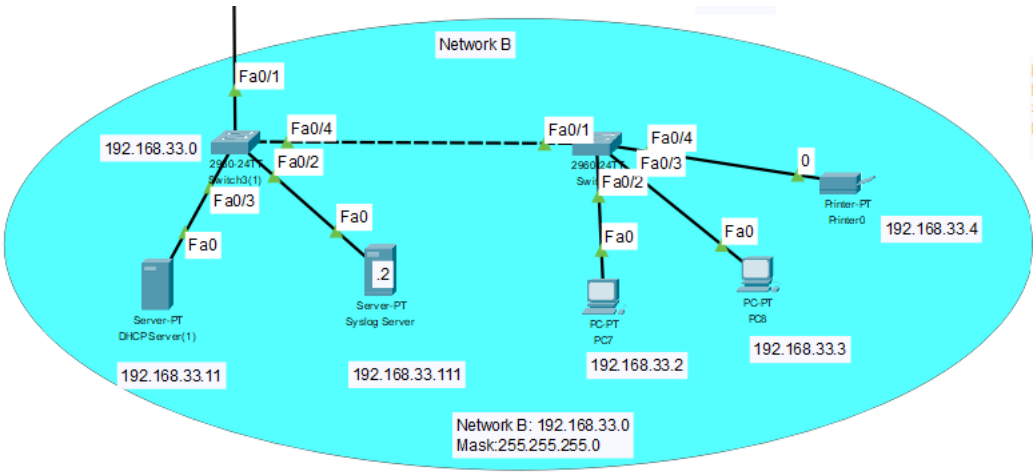


Go into the Laptop and see the Wi-Fi settings (Desktop -> PC Wireless)



Network B

In network B, there are various networking devices that are connected to each other and responsible for different tasks. Here in this network, we've used two access switches, two servers one for DHCP and one for Syslog to capture the log events and an NTP server for clock synchronization, two end devices, and a printer are all connected via copper straight-through cables.



Dissecting the network B:

Access switch: A switch is a networking device that connects devices within a local area network (LAN). It is a layer 2 device that operates at the data link layer or sometimes at the network layer (Layer 3) of the OSI model. A switch receives incoming network packets and forwards them to their intended destination based on the destination MAC (Media Access Control) address. The switch maintains a forward table that contains the physical address of all the devices in the LAN; Based on this it delivers the packet rather than broadcasting.

Some of the benefits of the switches are to provide full-duplex communication, which allows data to be sent and received parallel on a port. It also improves network efficiency, performance, and security by facilitating direct communication between devices and reducing network redundancy. In our topology in Network B, we've two access switches: the first switch is connected to the DHCP server and Syslog server, and NTP server and the second switch is connected to the end devices such as PCs and a printer. The default gateway address for this network is 192.168.33.0 and the subnet mask is 255.255.255.0

Dynamic Host Configuration Protocol Server:

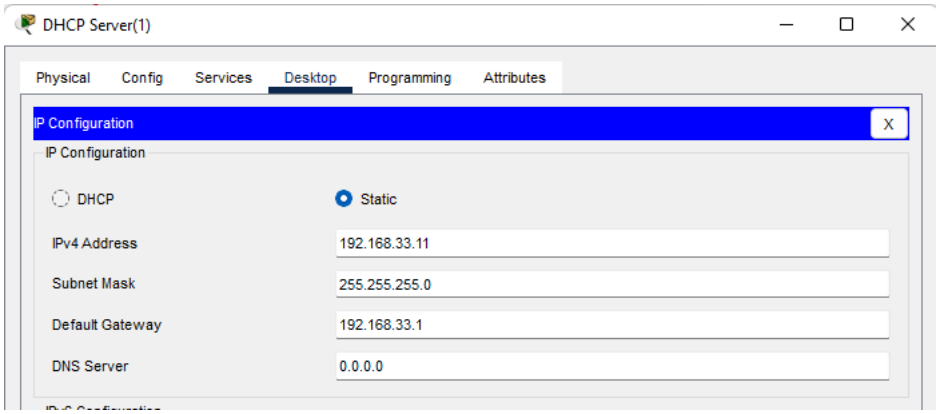
DHCP stands for Dynamic Host Configuration Protocol. DHCP is a mechanism that automatically assigns the dynamic IP address to the devices that are connected and configured to it, and it is unique. DHCP server cannot assign the IP address but also assigns the subnet mask, default gateway, and DNS server.

Working of DHCP server:

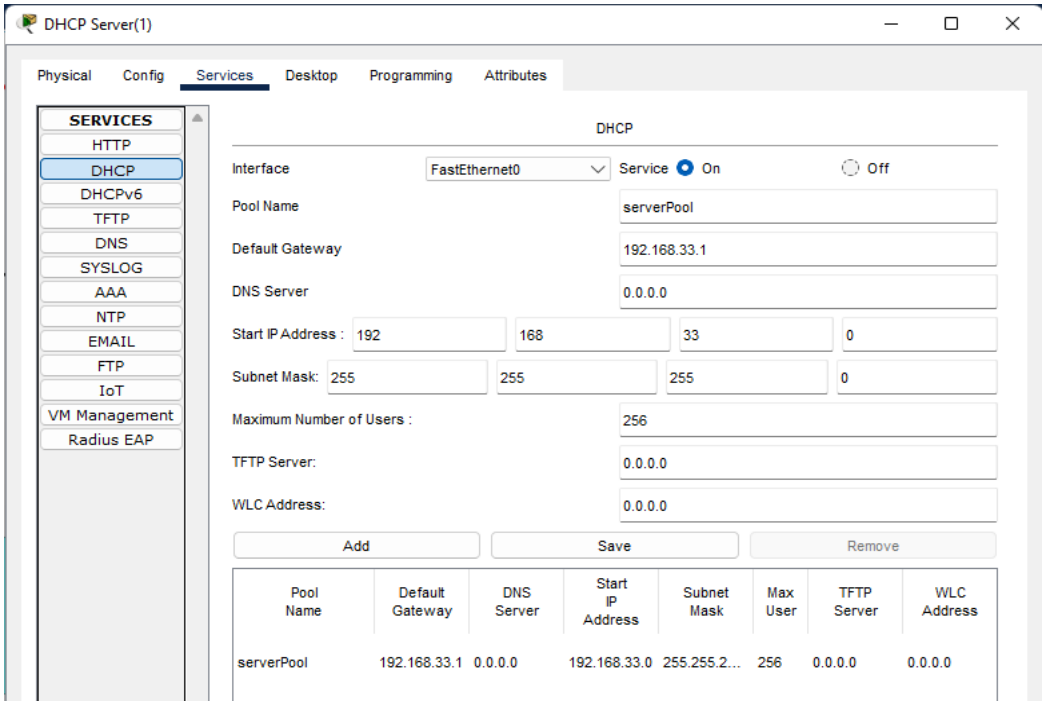
Based on the underlying four steps depicts the working of DHCP.

1. DHCP Discover – When a host machine sends a broadcast request, looking for the DHCP server.
2. DHCP offers – The DHCP server offers an address.
3. DHCP request – The host requests to lease the address.
4. DHCP acknowledgment – DHCP server acknowledges the host request and sends the IP addresses to the host.

Let's configure the DHCP server: First click on the DHCP server and navigate to the Desktop option and select IP configuration here assign the static IPv4, subnet mask, and default gateway address as shown in the below screenshot.



Once the IP address is configured and then move the services option and select DHCP turn on the service and specify the pool name, default gateway, DNS server, start Ip address, subnet mask, and maximum users and click on save.



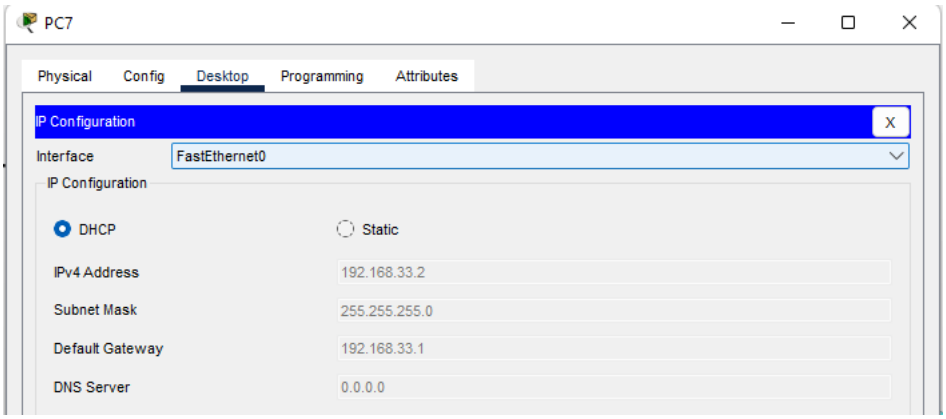
Once we are done with adding the scope for DHCP then enable the DHCP on end devices in our case we're using the service for PC 7, PC 8, and Printer. When a PC is configured to get the IP address automatically, they send a broadcast request for an IP address on the network and then the DHCP server serves the request by assigning the IP address from its scope.

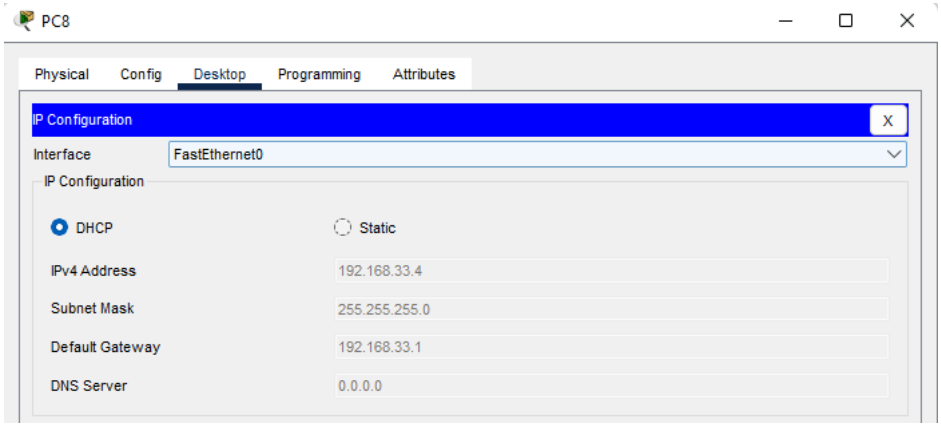
The scope refers to the range of IP addresses that a DHCP can provide to the devices. In our DHCP server, we've used scope starting from 192.168.33.0 which can offer IP addresses to 256 devices and is customizable. It assigns the IP on a lease basis only for a certain period once the time is over it sends a renewal request to get the IP address

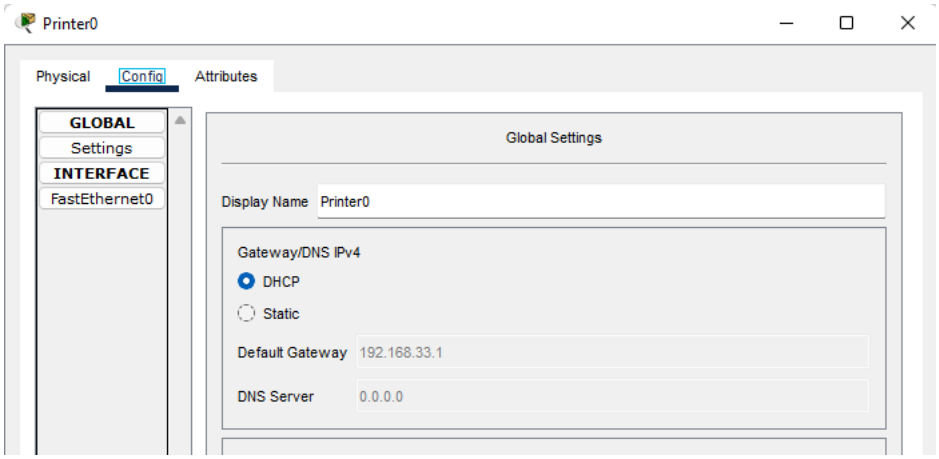
and leasing is used to make sure DHCP shouldn't run out of IPs the default lease time for wired connections is 8 days and for wireless its 8 hours.

There is also a provision to request a permanent IP address from the DHCP by using an address reservation. It ensures that a specific device always gets the same IP by using its MAC address and is usually provided to the printers, routers, and servers. DHCP uses a UDP port in which the client works on port 68 and the server works on port 67.

To enable, select the PC 7 and navigate to the Desktop option and select the IP configuration here select DHCP and wait about 5 seconds now the device is assigned an IP address from the DHCP server. The same steps are applicable for PC 8 and Printer and these steps are captured in the below snapshots.







Syslog Server:

Syslog is a logging mechanism that collects logs of all the network devices such as routers and switches and provides them to the system administrator for further analysis. With this logging mechanism, network management, and troubleshooting activities will become easier. We can use a Syslog Server to store these logs. Syslog provides log information based on different levels.

There are 8 levels of Syslog, these levels are mentioned below:
0, Emergency
1, Alert
2, Critical
3, Error
4, Warning
5, Notification
6, Informational
7, Debug

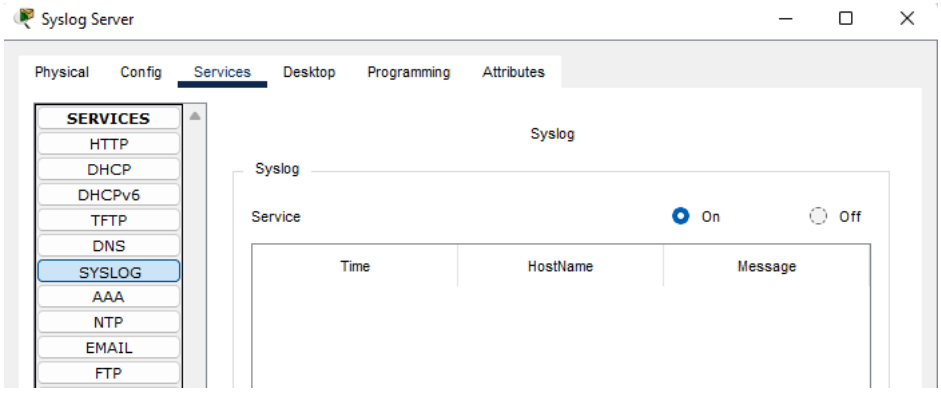
The above levels depict all the critical information for the system besides the normal messages. The importance of these logs starts from 0 which represents the crucial syslog message, it is an emergency. Logs are ordered based on their severity. The least important log is debug which is 7.

There is also a provision to change the message format in syslog, users can configure it as per the requirements.

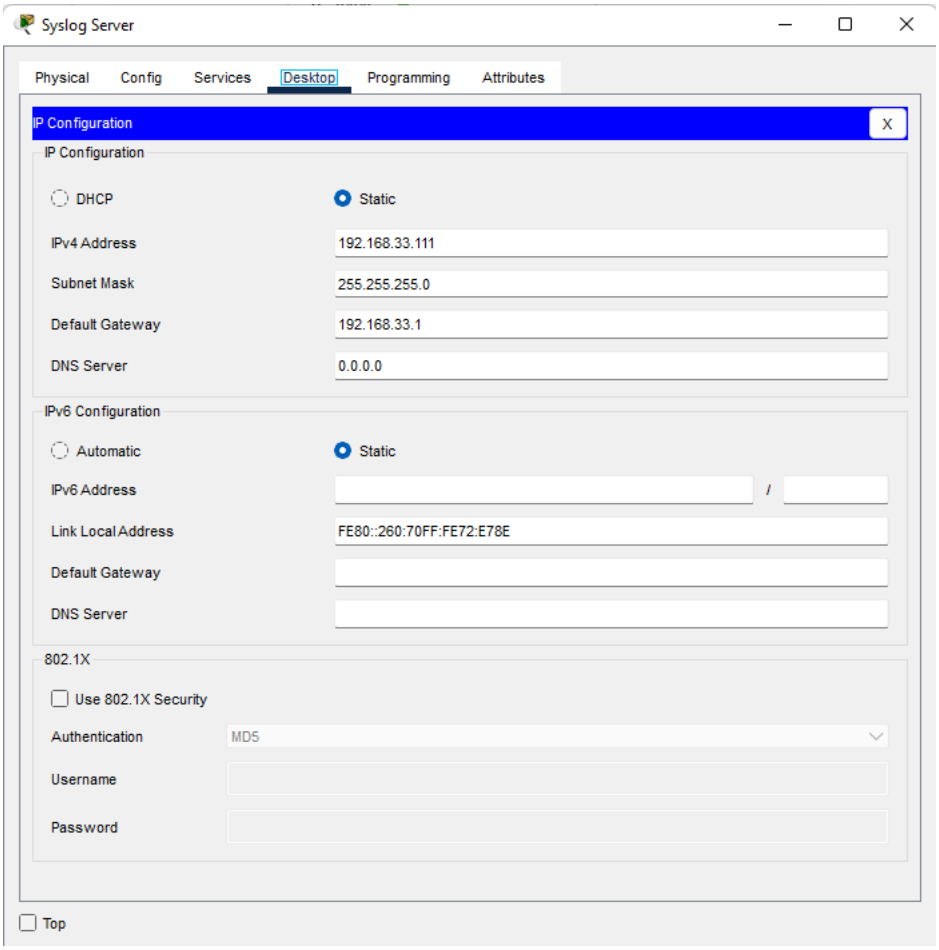
SYSLOG LEVELS seq no:timestamp: %facility-severity-MNEMONIC:description			
LEVEL	NUM.	DESCRIPTION	DEFINITION
Emergency	0	System unstable	LOG_EMERG
Alert	1	Immediate action needed	LOG_ALERT
Critical	2	Critical conditions	LOG_CRIT
Error	3	Error conditions	LOG_ERR
Warning	4	Warning conditions	LOG_WARNING
Notification	5	Normal but significant conditions	LOG_NOTICE
Informational	6	Informational message only	LOG_INFO
Debugging	7	Debugging messages	LOG_DEBUG

Source: The image is taken from cisco.

To configure the Syslog server. First, we need to enable it by default syslog is enabled, if not we can do that by clicking on the services options under that we need to select syslog and click on. Below snapshots show the GUI of the syslog.



Once it is enabled then assign the Ip address to do this, navigate to Desktop > IP configuration > specify the IP address in my case I'm using 192.168.33.111 and the default gateway is 192.168.33.1 same is demonstrated in the below snapshot.



It is also by default enabled on all Cisco devices such as routers and switches are not enabled, we can manually enable it by using the "logging on" command. In our topology, we've placed the log server in Network B, Router 1, and Router 2 to capture the events.

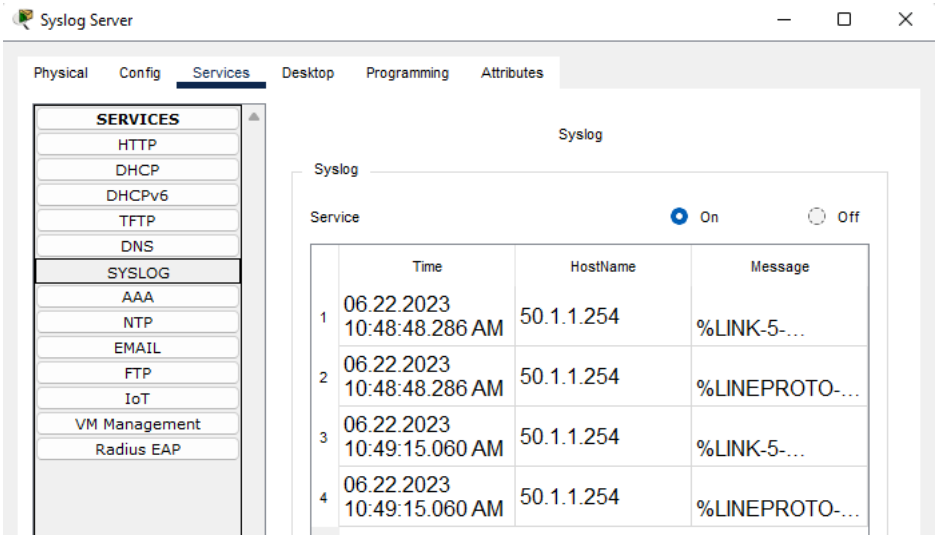
Commands to configure the Syslog server:

Enable the Syslog on switch 4
Switch2B (config)# logging on
To store the Syslog messages, you should specify the IP address of the Syslog server.
Switch2B (config)# logging 192.168.33.111

While troubleshooting or daily routine configuration practices by network admins, they can investigate the specific events of interest logs. Therefore, users can change the severity levels. To do this, we can use the "logging trap" command with the desired severity levels.

Switch1B (config)# logging trap debugging ->set the severity level to debug. So, we will see critical, alert, and emergency-level events in the logs.

Switch1B (config)# logging 192.168.33.111
To see the logs on a Cisco router, you can use “show logging” command.
Switch2B # show logging
The same tasks are demonstrated in the screenshots below.
Once the configuration is done on the server and other devices, we can see the logs captured under the Syslog services.

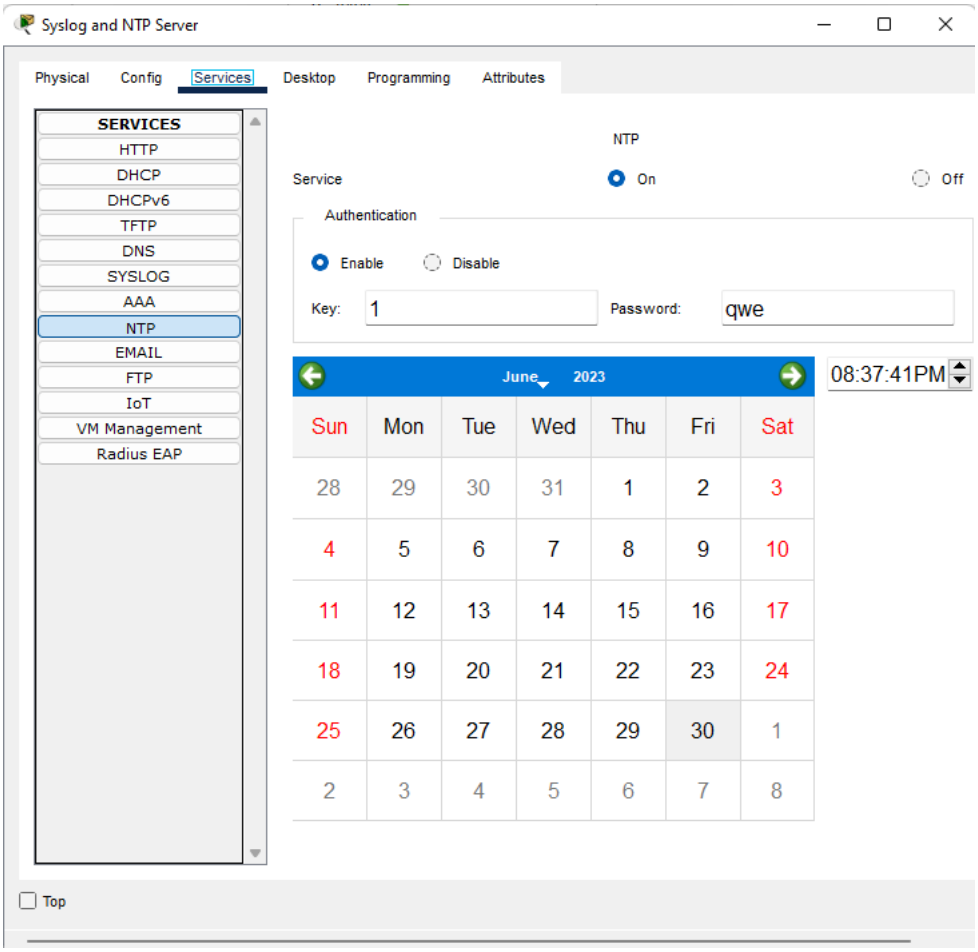


Network Time Protocol Server (NTP):

NTP stands for Network Time Protocol. It has the important job of clock synchronization over a network. Even if any of the devices are not synced properly with the time and are delayed by a few minutes, it can affect the analysis of logs and packets. Every device on the network will have an internal clock and date, they're all not synced properly. To synchronize properly across all the devices, we use an NTP server.
NTP uses stratum values to identify the accuracy of the clock. It ranges from 0 to 15 where 0 represents the most accurate and 15 is the least. NTP uses UDP port number 123. And this NTP server is synchronized across all the routers.

Commands to configure the NTP server:

To configure the NTP server. First, we need to enable it by default NTP is enabled, if not we can do that by clicking on the services options under that we need to select NTP and click on it. Below snapshots show the GUI of the same.



After enabling this, we've configured the NTP server in router 2 to synchronize the device timing with the NTP server.

Router_lan2 (config)#ntp authentication-key 1 md5 08305B4B 7 -> configuring NTP (Network Time Protocol) authentication with an MD5 key on a router's LAN2 interface.

Router_lan2 (config)# ntp authenticate -> to enable authentication for NTP.

Router_lan2 (config)# ntp trusted-key 1 -> to trust NTP authentication key 1 on a router 2

Router_lan2 (config)# ntp server 192.168.33.111 key 1 -> router 2 is configured to synchronize its time with the NTP server located at IP address 192.168.33.111

Show ntp association -> command used to display information about the NTP associations on a router 2.

```
Router_lan2#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
*~192.168.33.111127.127.1.1     1    183      16      0      0.00           0.00
-137269716641998.19
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router_lan2#sh
Router_lan2#show cloc
Router_lan2#show clock
20:54:37.838 UTC Fri Jun 30 2023
```

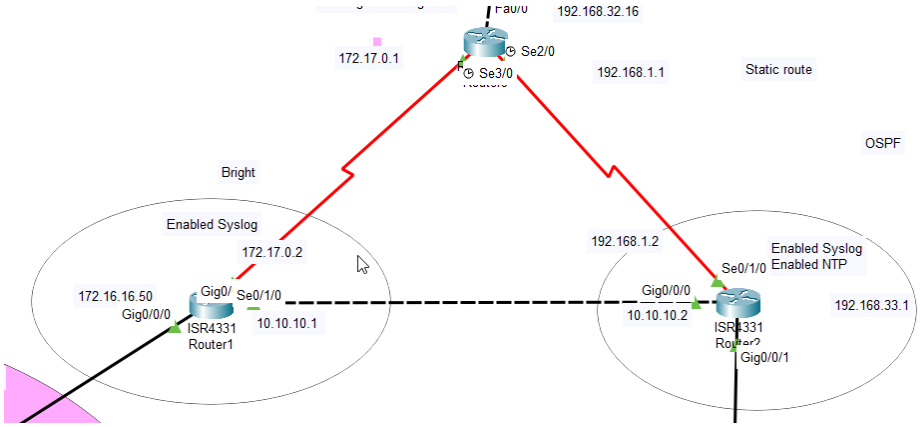
Once access switch 3 is configured and proceeding to switch 4, we're configuring it with all the end devices. In our topology, we've 2 PCs and a printer connected to access switch 4. These devices get the IP address from the DHCP server.

Open Shortest Path First:

For communication between the 3 internal routers and to enable the communication between Network A and B, we have configured a routing protocol known as OSPF (Open Shortest Path First), OSPF is a link-state routing protocol, it gathers link-state information from available routers, and builds a topology map of the network. The topology is produced as a routing table and presented to the internet for routing packets by their destination IP address.

```
router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 network 172.32.0.0 0.0.255.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.33.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
 network 172.17.0.0 0.0.255.255 area 0
!
router ospf 2
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 network 172.32.0.0 0.0.255.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.33.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
!
router ospf 3
 log-adjacency-changes
 network 172.17.0.0 0.0.255.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
!
```

These routers share what we call link state advertisement with each other using **Hello** messages, they discuss with each other all the information they have within their various networks, and with that information, they use it to form an identical link state databases(routing tables) in all the routers which cause each router in the internal topology to be able to route traffic from any of the two networks.

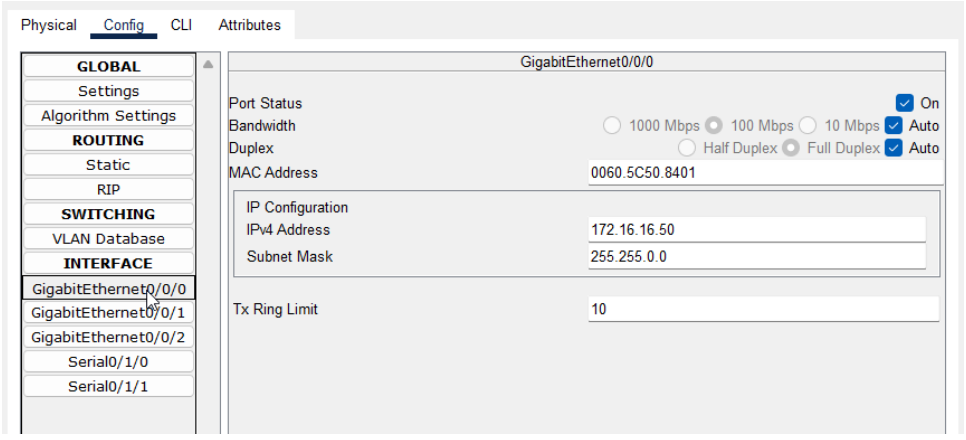


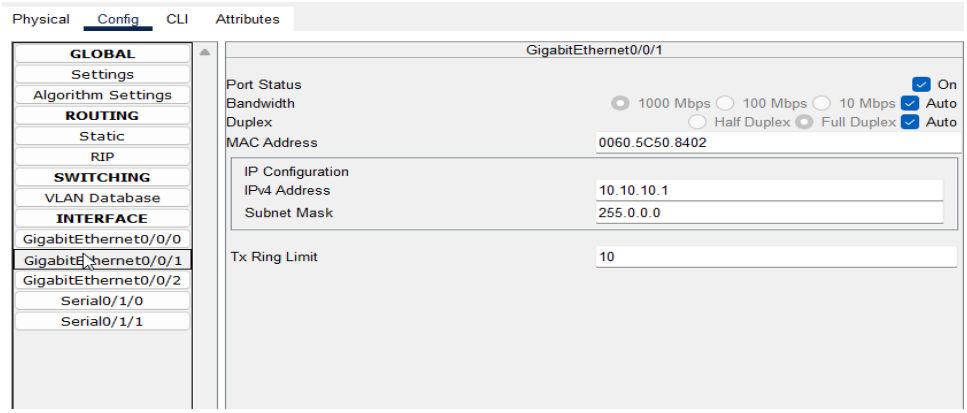
STATIC AND DYNAMIC ROUTING:

Static routing uses already configured routes to send traffic to its destination while dynamic routing uses an algorithm to determine the shortest path, in this project work, we configured a static route on router 3 to use the already configured route that we have, to route traffic to and from firewall and outside router.

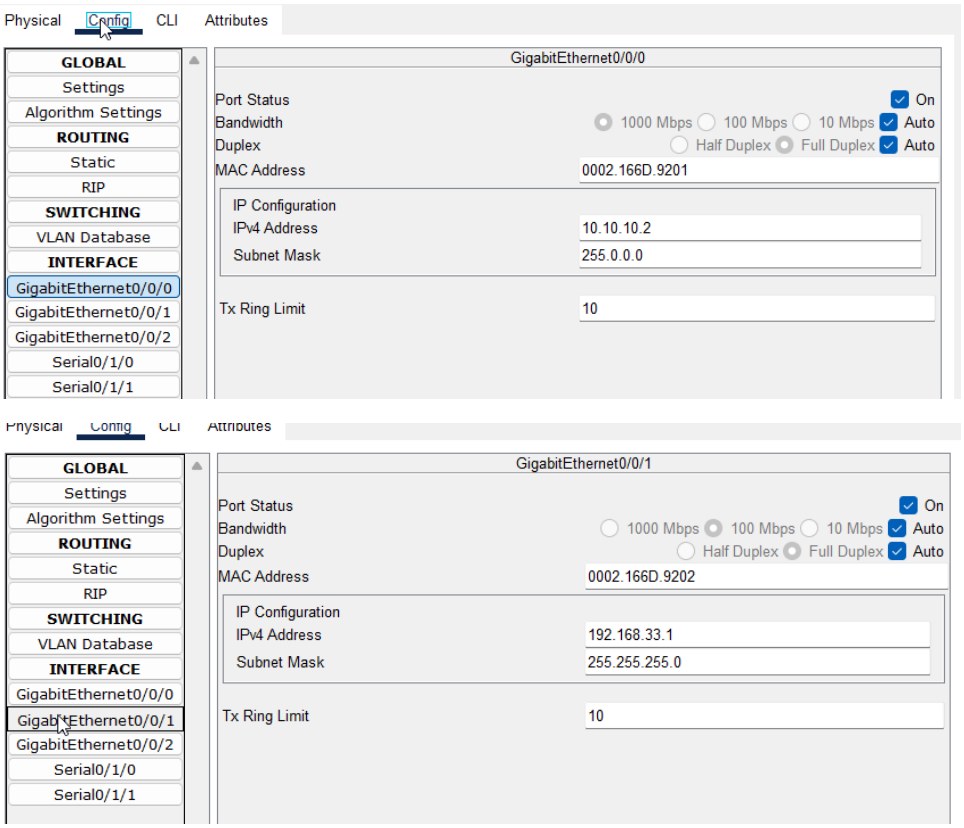
```
ip route 201.10.1.0 255.255.255.0 FastEthernet0/0
```

Router 1 is in control of network A; the connection was made using a copper straight-through cable through interface Gig0/0/0 with an IP address of 172.16.16.50 and subnet mask of 255.255.0.0 (the subnet controlling network A). At interface Gig0/0/1, it is connected using a copper cross-over cable to network B through router 2 with an IP address of 10.10.10.1 255.0.0.0, Syslog is enabled on this router for monitoring the flow of traffic.

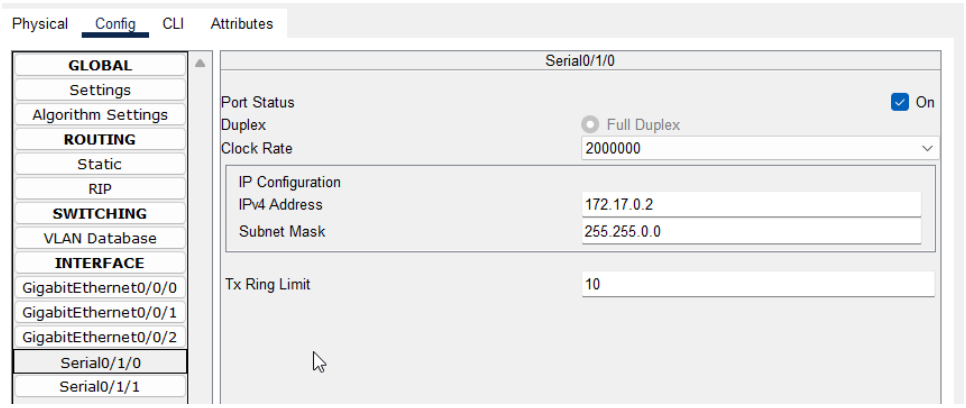


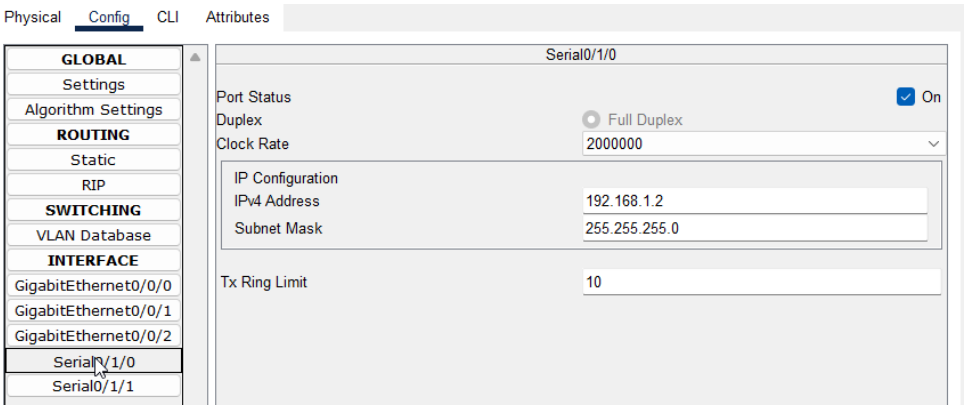


Router 2 is in control of network B; the connection was also made using a copper straight-through cable through interface Gig0/0/1 with an IP address of 192.168.33.1 and subnet mask of 255.255.255.0 (the subnet controlling network B) this IP address is dynamic because it is from a DHCP server. At interface Gig0/0/0, it is connected using a copper cross-over cable to network A through router 1 with an IP address of 10.10.10.2 255.0.0.0, Syslog was enabled on this router for monitoring the flow of traffic. NTP (Network Time Protocol) was also configured in this router for clock synchronization among devices in the network.

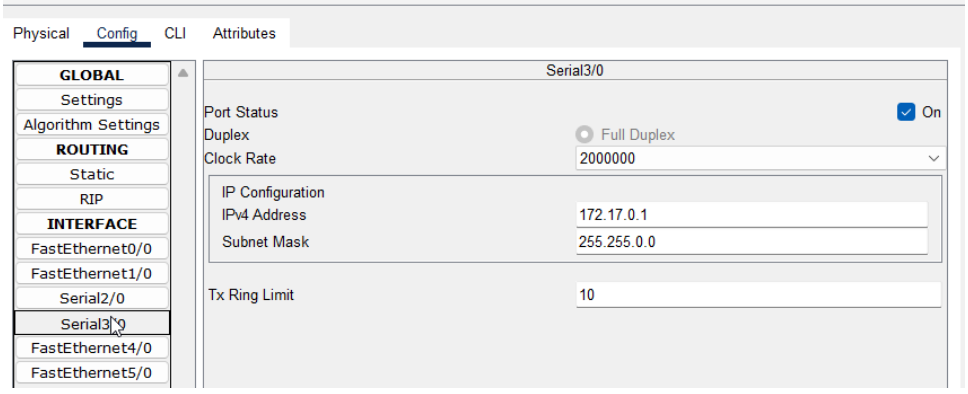


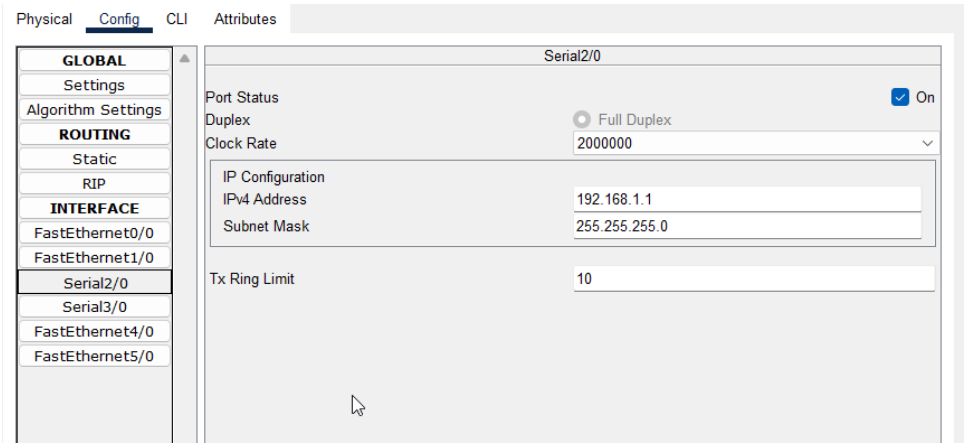
Both routers connect this internal network to the firewall and outside network through router 3, both connections were done serially to router 3, router 1 was connected to router 3 through interface Se0/1/0 with an IP address of 172.17.0.2 255.255.0.0, router 2 was connected to router 3 through interface Se0/1/0 with an IP address of 192.168.1.2 255.255.0.0.

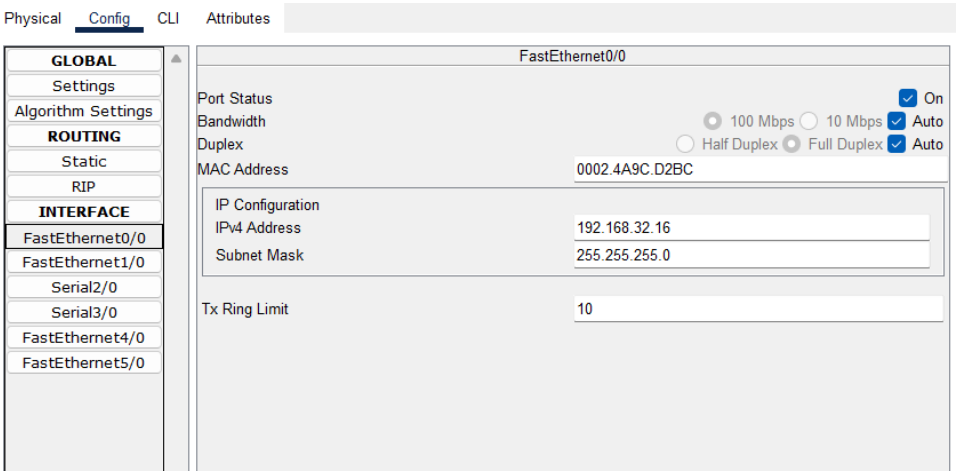




Router 3 got its connection to router 1 through interface Se3/0 with an IP address of 172.17.0.1 255.255.0.0, and also, got its connection to router 2 through interface Se2/0 with an IP address of 192.168.1.1 255.255.0.0, this router connects this entire network to the firewall and outside network using a copper cross over cable through interface Fa0/0 with an IP address of 192.168.32.16 255.255.255.0.







Cisco Adaptive Security Appliance (ASA):

Perimeter Security:

ASA firewalls are commonly deployed at the network perimeter to create a secure boundary between an internal network and the Internet. They monitor and control incoming and outgoing traffic, inspect packets, and apply security policies to prevent unauthorized access, data breaches, and network attacks.

Access Control:

ASA firewalls provide granular access control mechanisms, allowing administrators to define and enforce security policies based on specific criteria such as IP addresses, ports, protocols, or user identities. This ensures that only authorized traffic is allowed to pass through the firewall, reducing the risk of unauthorized access or data leakage. ASA firewalls utilize ACLs to define specific rules for permitting or denying traffic. This helps in preventing unauthorized access to sensitive data and resources.

```
!
access-list inside_to_outside extended permit ip any any
!
!
access-group inside_to_outside in interface outside
!
```

The provided above command creates an access control list that permits all IP traffic from any source IP address to any destination IP address on the inside network. It then applies this access control list to the inbound traffic on the outside interface. This configuration allows unrestricted outbound traffic from the inside network while controlling inbound traffic based on other rules defined in the ACL or default ASA policies.

Stateful Inspection:

ASA firewalls maintain a stateful inspection table that keeps track of the state of network connections. This allows them to analyze traffic in the context of established connections, ensuring that only legitimate traffic is allowed and preventing unauthorized access attempts.

In an ASA firewall configuration, the terms "inside" and "outside" refer to the interfaces and their associated security levels. The security levels determine the trustworthiness of a particular network or interface.

Inside Interface:

The inside interface of an ASA firewall is typically connected to the internal network, which contains trusted resources such as servers, workstations, or other network devices. It is the interface that faces the more secure side of the network. The inside interface is assigned a higher security level, often set to 100, indicating a high level of trust for the internal network.

The security level of 100 on the inside interface allows traffic originating from this interface to flow freely to interfaces with lower security levels (such as the outside interface). By default, traffic from a higher security level interface to a lower security level interface is allowed, while traffic from a lower security level interface to a higher security level interface is denied unless specifically permitted by firewall rules.

```
!
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 192.168.32.15 255.255.255.0
!
```

Outside Interface:

The outside interface of an ASA firewall is typically connected to the external network, which is usually the Internet or any untrusted network. It faces the less secure side of the network. The outside interface is assigned a lower security level, often set to 0, indicating a lower level of trust for external traffic.

The security level of 0 on the outside interface restricts inbound traffic from lower security level interfaces (such as the Internet) unless explicitly allowed by firewall rules. It provides a layer of protection by preventing direct access from untrusted networks to the internal network. Outbound traffic from the inside interface to the outside interface is allowed by default.

```
!
interface GigabitEthernet1/3
 nameif outside
 security-level 0
 ip address 201.10.1.1 255.255.255.0
!
```

By assigning different security levels to the inside and outside interfaces, the ASA firewall enforces traffic flow policies based on the security levels. This setup helps in controlling and securing the network by allowing traffic from trusted internal networks to flow to less secure external networks while restricting direct inbound traffic from untrusted networks.

It's important to note that the terms "inside" and "outside" are just naming conventions, and they can be customized based on the specific network configuration. The security levels, however, play a crucial role in determining the traffic flow and access control between interfaces within the ASA firewall.

We enabled passwords in Cisco ASA firewalls to set a password for privileged mode access. This password is used when executing the "enable" command to gain administrative privileges on the firewall. And the enable password is encrypted by default, as displayed in the image below. This adds additional security so that the password is not in a readable format.

```
.
ASA Version 9.6(1)
!
hostname ASAFirewall
enable password eZbz6Nu8W0PM4/OS encrypted
names
!
```

References:

https:>ipcisco.com/lesson/syslogserver/#:~:text=Syslog%20is%20a%20logging%20mechanism,check%20Cisco%20Syslog%20Configuration%20Example.