

Communication Company Network

Done by:

Mariam Said Yousef Alshikh

Esraa Khaled Omar

Mohamed Mahmoud Ghanem

Amira Walied

Alaa Gaber

Supervisor : Eng / Ayman Basha

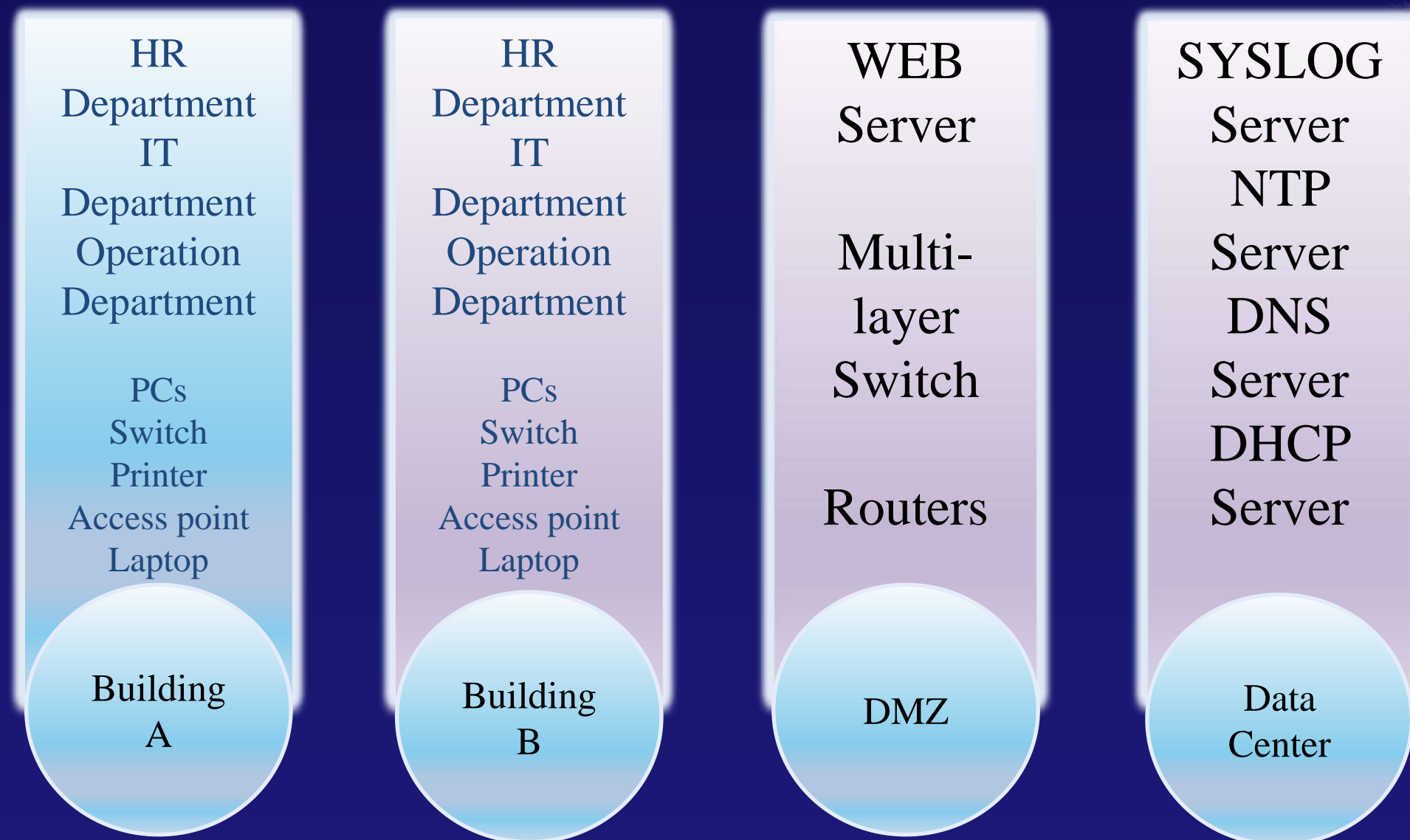
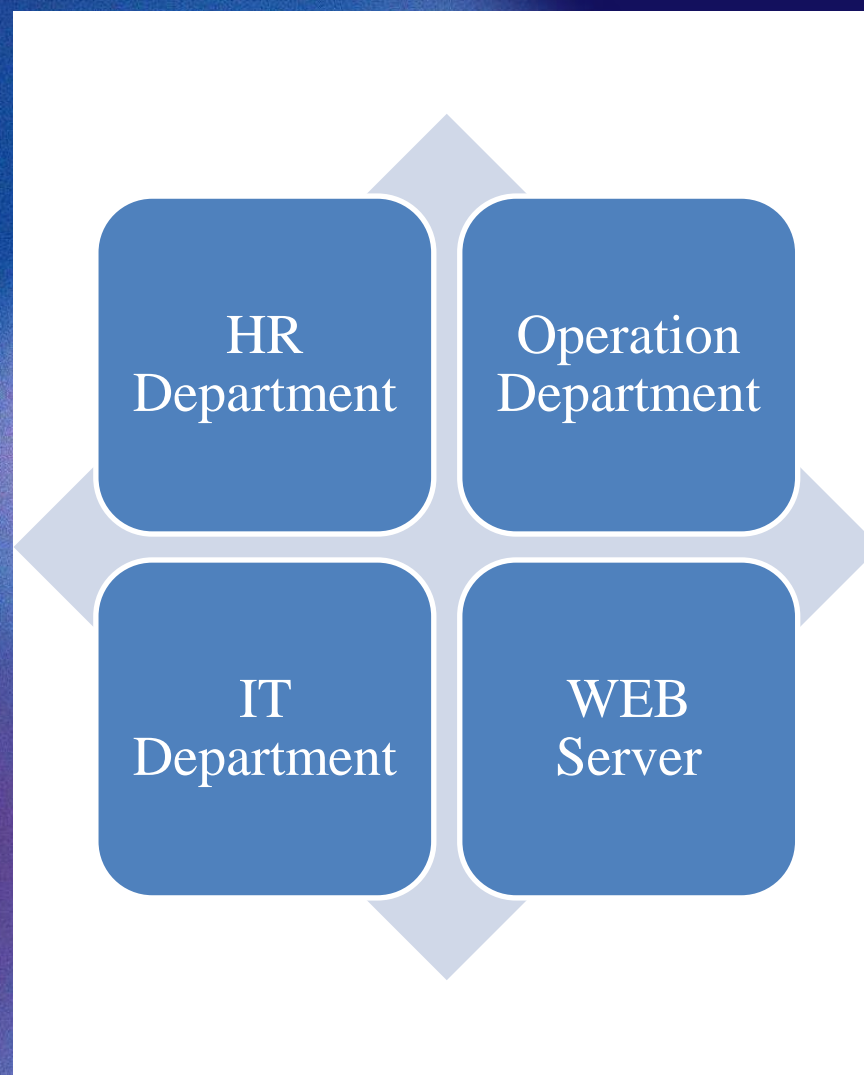
Agenda

1. Introduction
2. VLANS
3. Inter-VLAN
4. Access point
5. SERVERS
6. Protocols
7. DMZ
8. Security System

➤ Introduction

- ❑ A simple network design for a small communication company focuses on creating an efficient and secure infrastructure to connect employees, devices, services, etc.
- ❑ An efficient network is essential to facilitate the systematic & cost-efficient transfer of information through messages, files, and resources.
- ❑ The project will provide insight into concepts such as topology design, IP addressing, and how to send information in packet form to the wire networks in different corporate buildings.
- ❑ We created a topology for a company of multi-network sand virtual local area networks (VLANs) , inter-VLAN, OSPF Routing, Servers (DHCP, DNS, SYSLOG, NTP, WEB) , ACL , and Port Security using Cisco packet tracer.
- ❑ Also recommendation for development to avoid potential attacks.

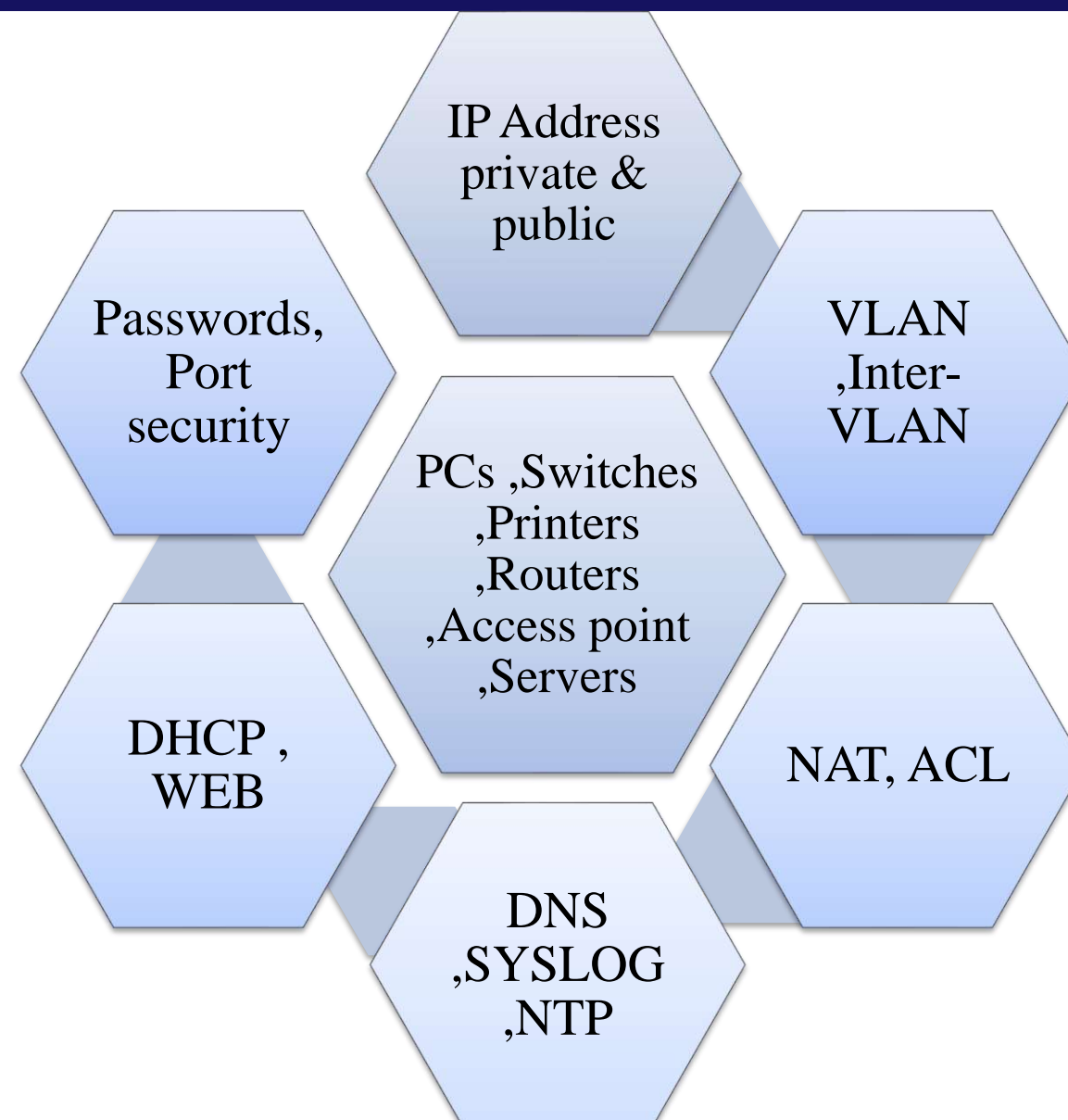
➤ Small Communication Company
Requirements of the project



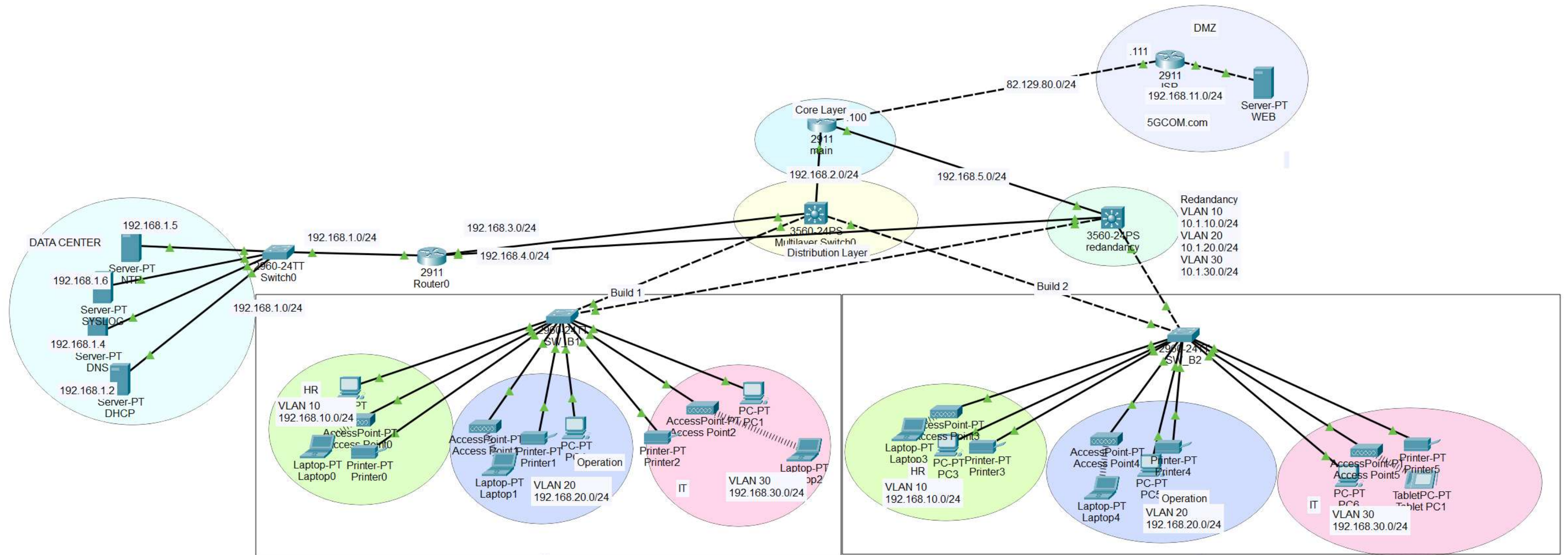
➤ Small Communication Company Tasks

We have done following tasking

Design Network Topology Devices Configuration IP Address VLAN Configuration Servers Configuration Security

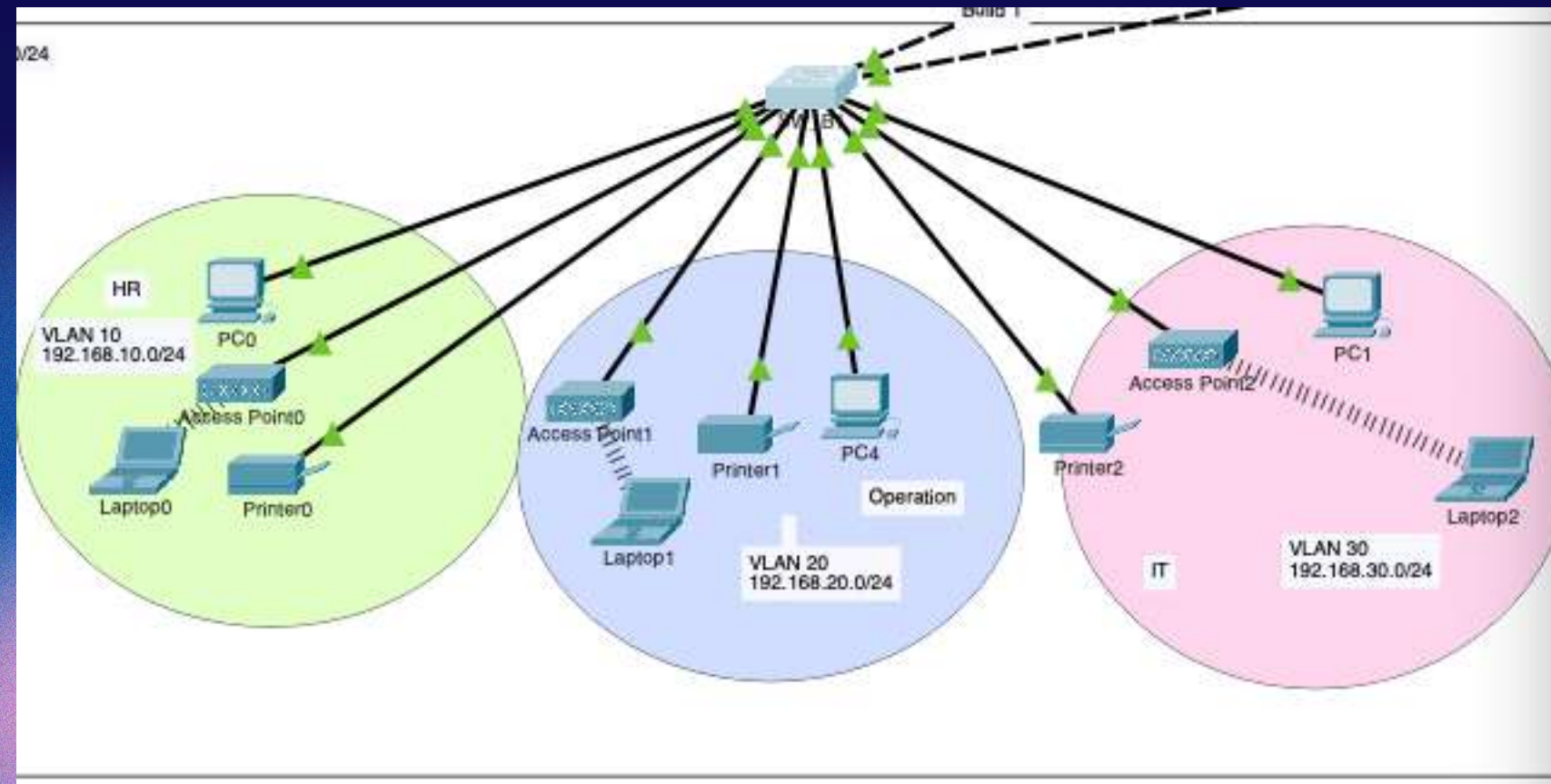


➤ Block Diagram



➤ VLAN Configurations

Build A

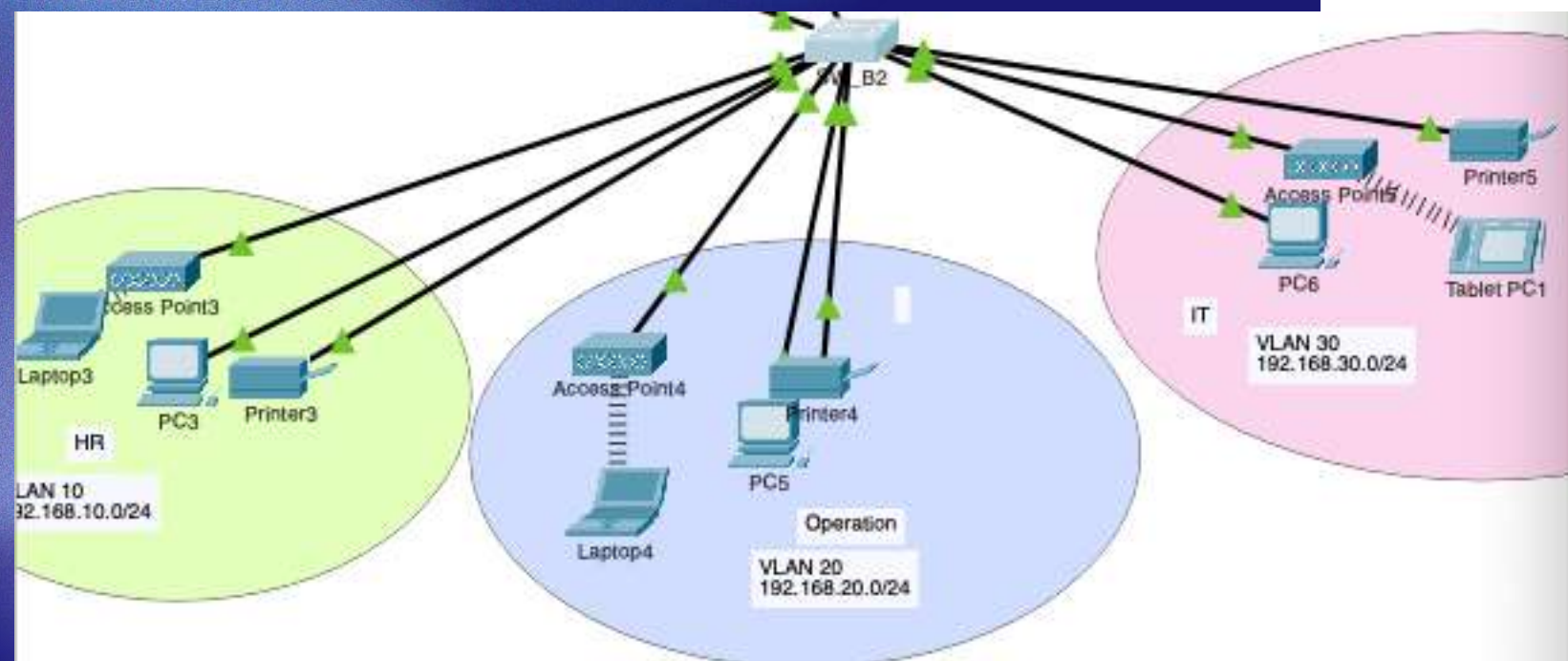


IOS Command Line Interface

```
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24
10 HR	active	Gig0/1, Gig0/2, Fa0/2, Fa0/5, Fa0/8
20 Operation	active	Fa0/3, Fa0/6, Fa0/9
30 IT	active	Fa0/4, Fa0/7, Fa0/10, Fa0/11, Fa0/12

Build B

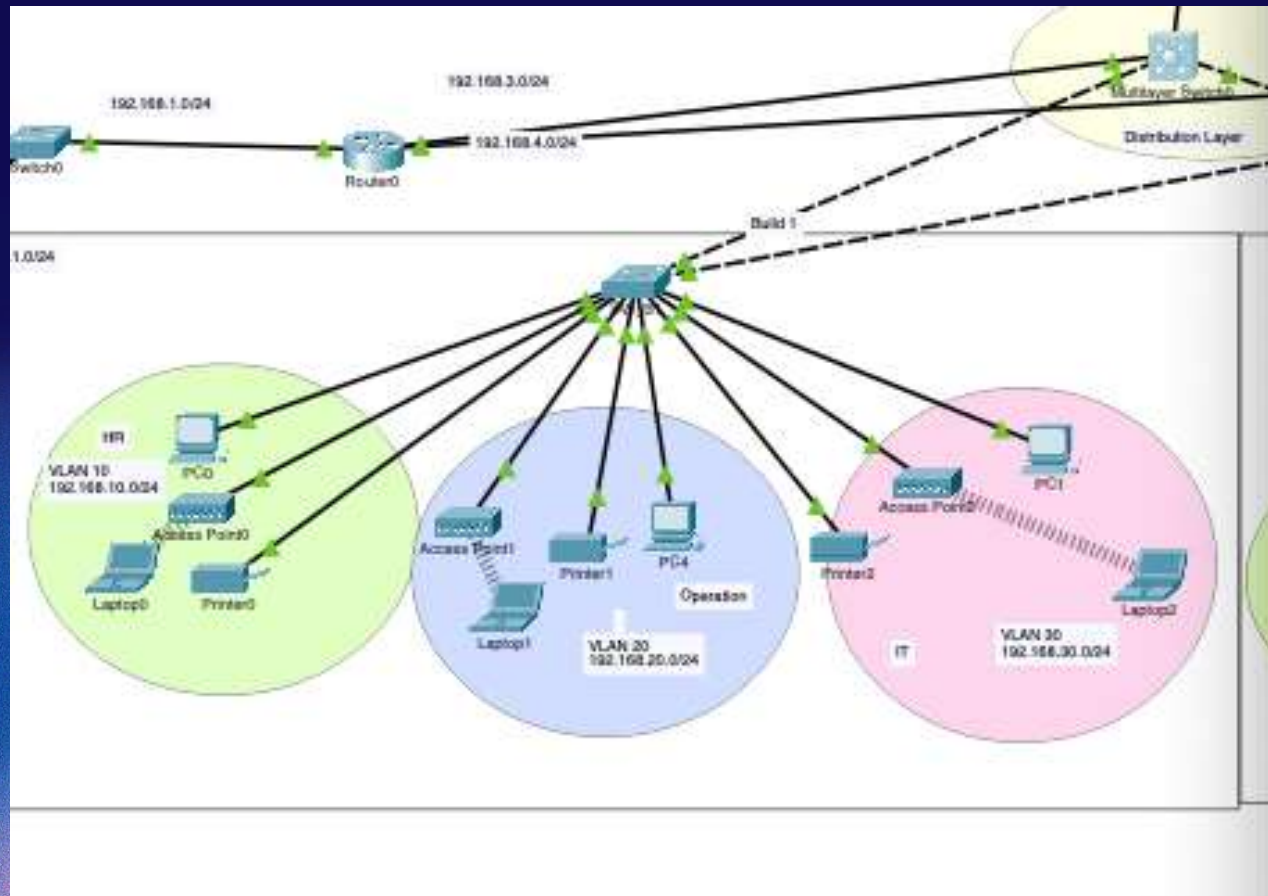


```
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 HR	active	Fa0/1, Fa0/2, Fa0/8
20 Operation	active	Fa0/3, Fa0/6, Fa0/9
30 IT	active	Fa0/4, Fa0/7, Fa0/10

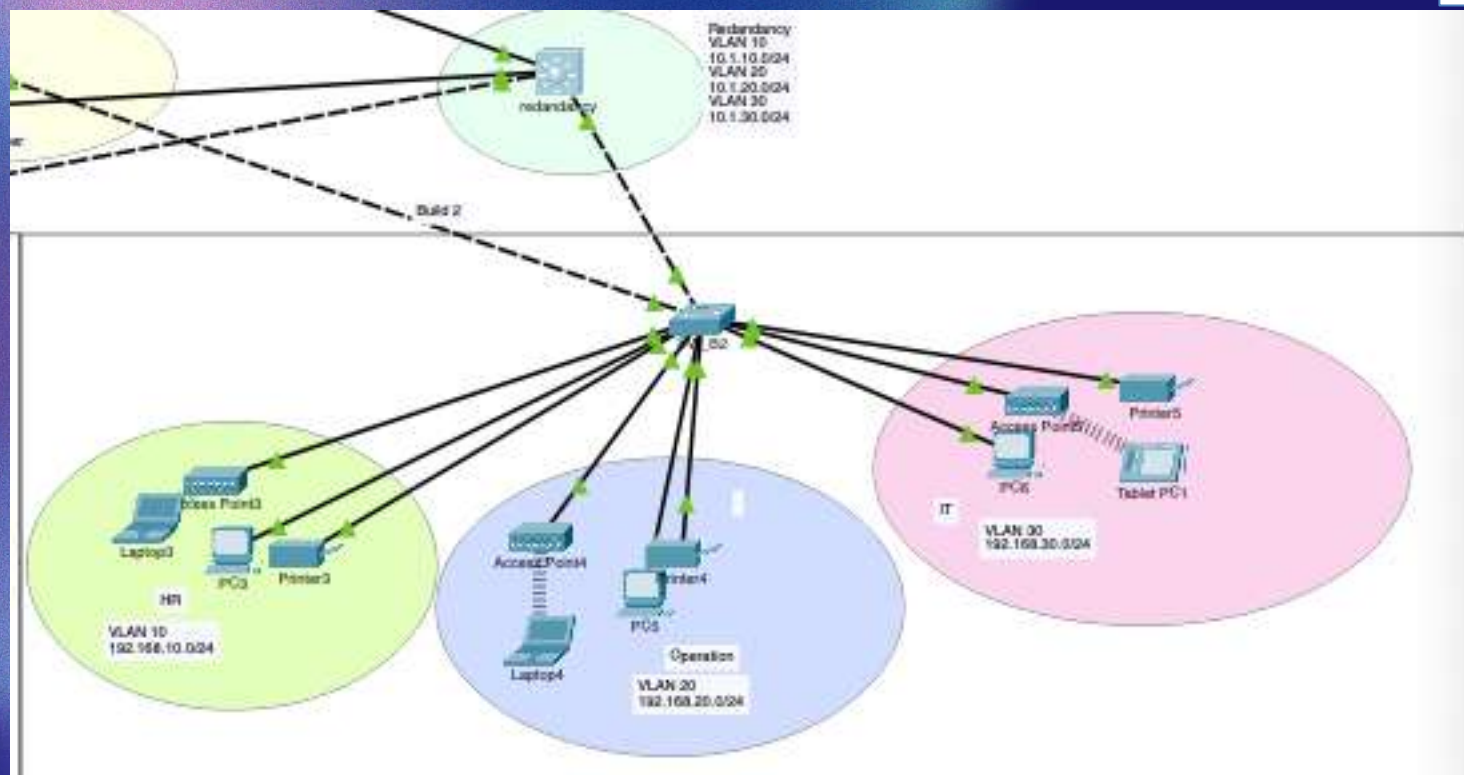
➤ Inter-VLAN Configuration

Multi-layer Switch 1



```
down
FastEthernet0/22      unassigned      YES unset  down
down
FastEthernet0/23      unassigned      YES unset  down
down
FastEthernet0/24      unassigned      YES unset  down
down
GigabitEthernet0/1    unassigned      YES unset  down
down
GigabitEthernet0/2    unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively down
down
Vlan10                 192.168.10.1    YES manual up
up
Vlan20                 192.168.20.1    YES manual up
up
Vlan30                 192.168.30.1    YES manual up
up
```

Multi-layer Switch 2

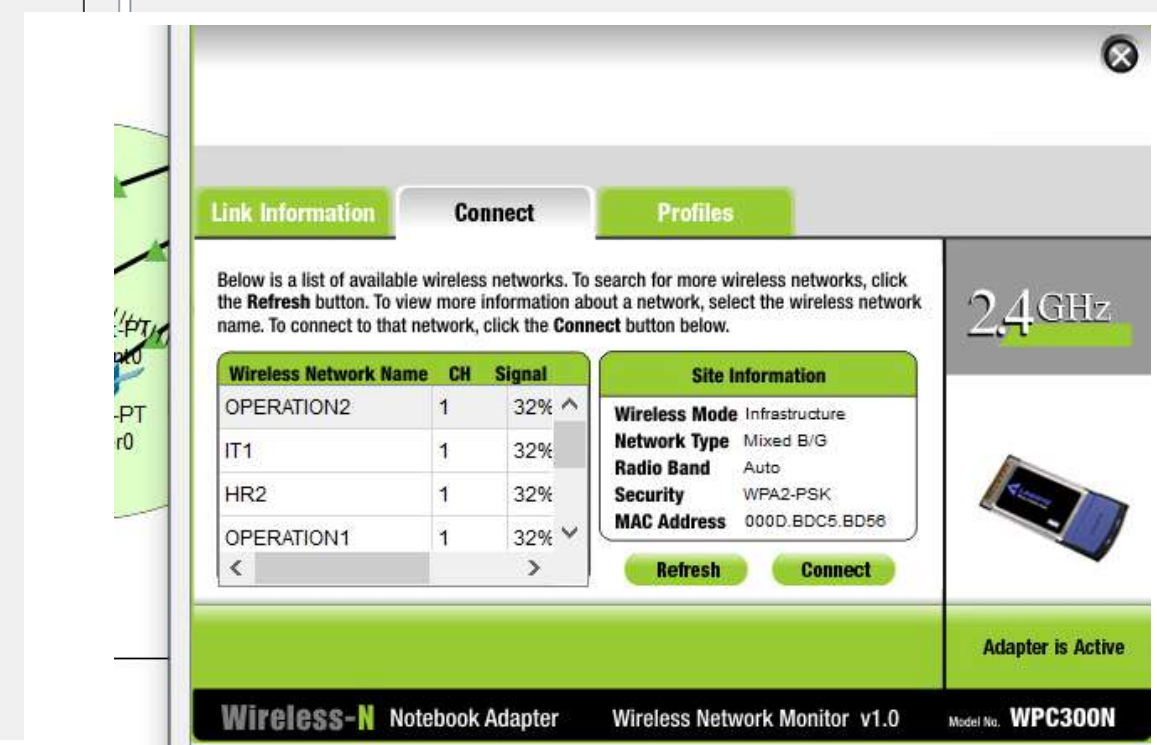
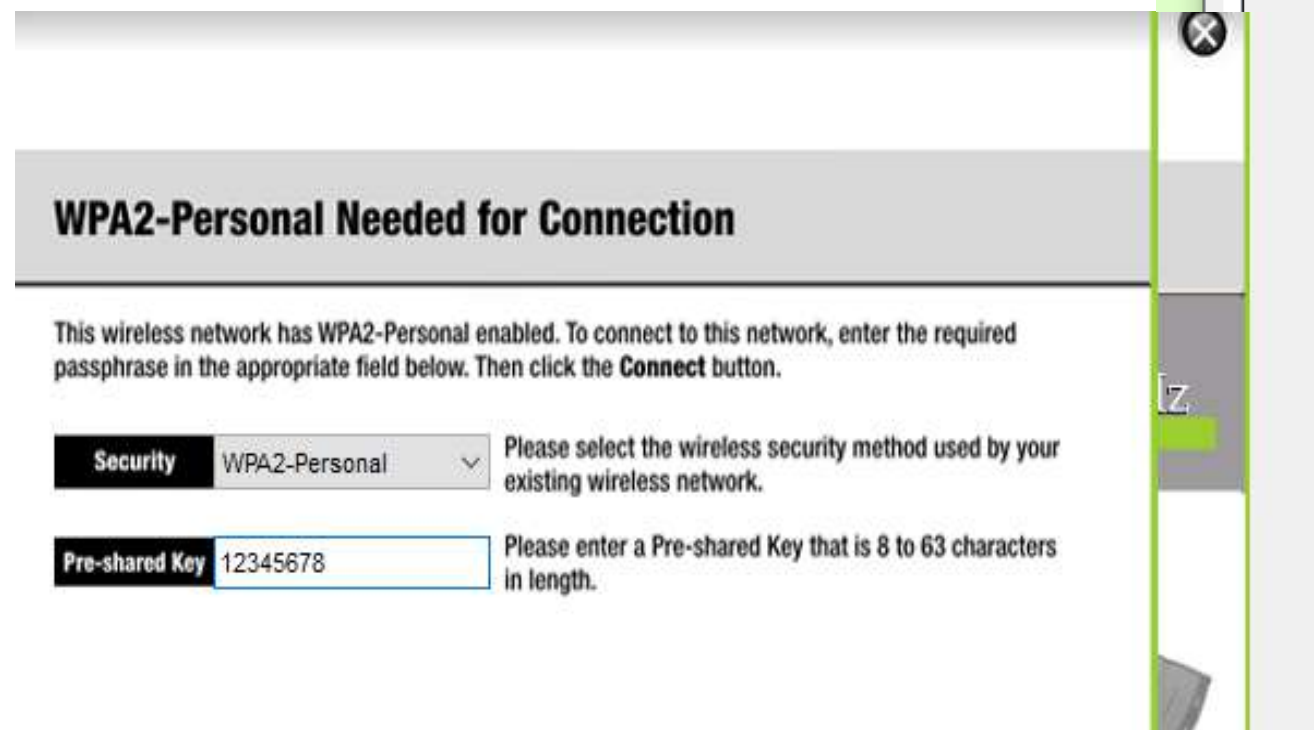
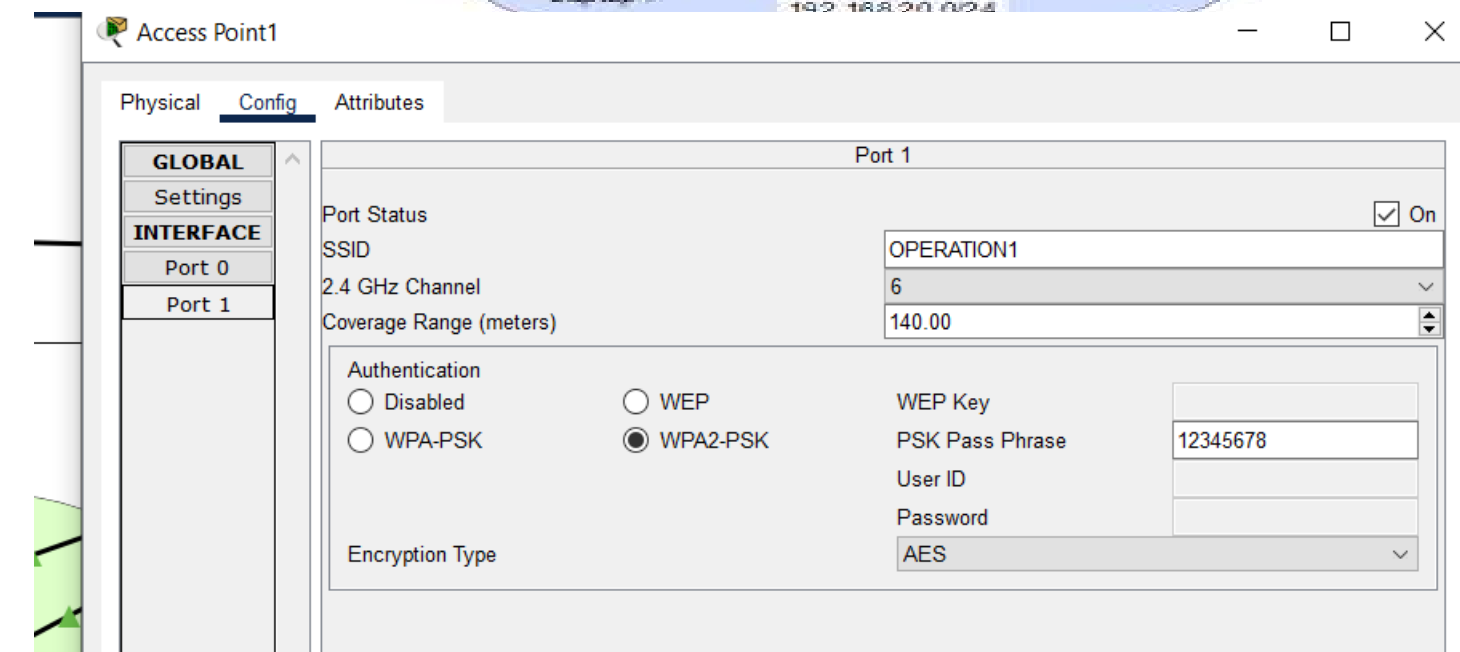
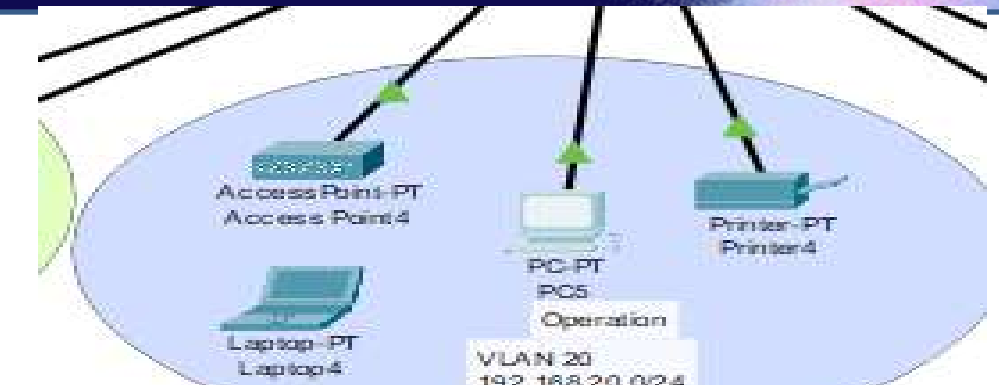
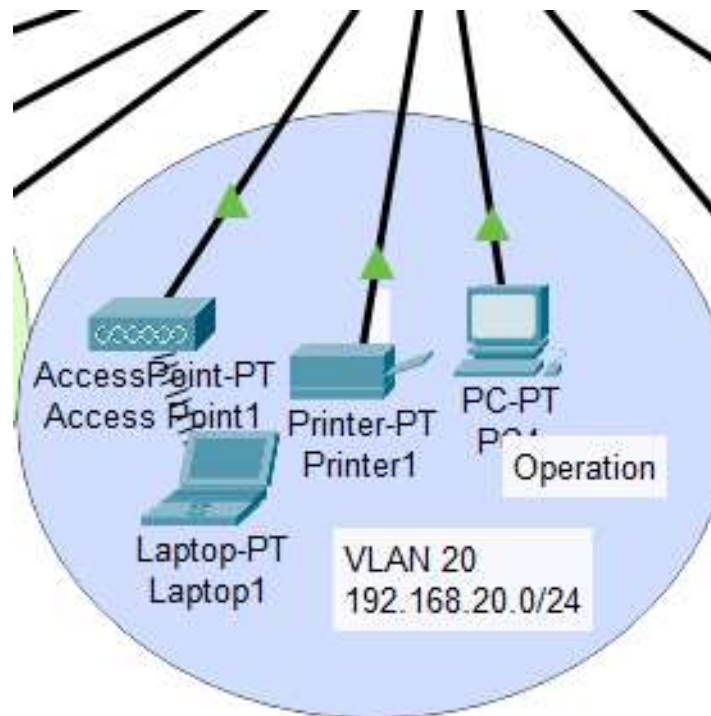


```
down
FastEthernet0/22      unassigned      YES unset  down
down
FastEthernet0/23      unassigned      YES unset  down
down
FastEthernet0/24      unassigned      YES unset  down
down
GigabitEthernet0/1    unassigned      YES unset  down
down
GigabitEthernet0/2    unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively down
down
Vlan10                 10.1.10.1       YES manual up
up
Vlan20                 10.1.20.1       YES manual up
up
Vlan30                 10.1.30.1       YES manual up
up
```


Access Point

It serves as a central point for providing connectivity between wireless devices (such as smartphones, laptops, and printers) and the wired network.

- **Placement:** Ensure proper placement to maximize coverage.
- **Configuration:** Use management tools to set security and access parameters.
- **Testing:** Test the range and signal strength.



Common Uses

- **Home**

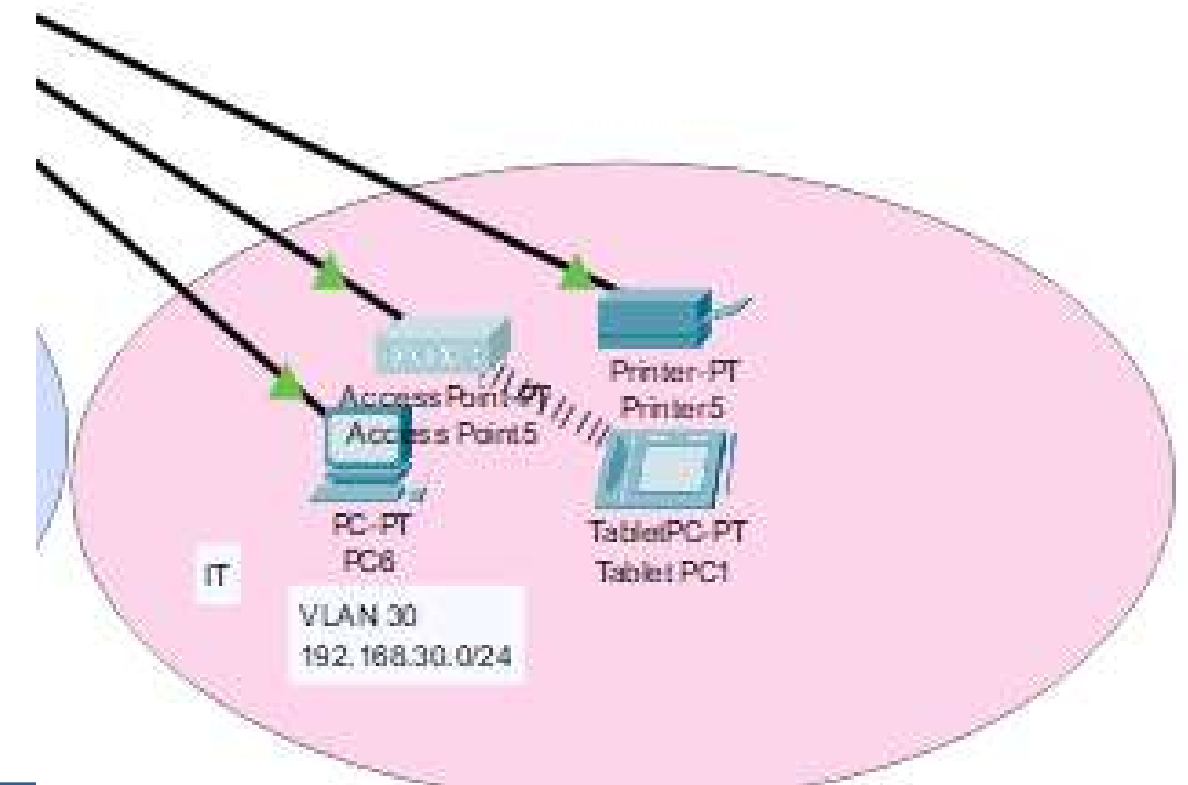
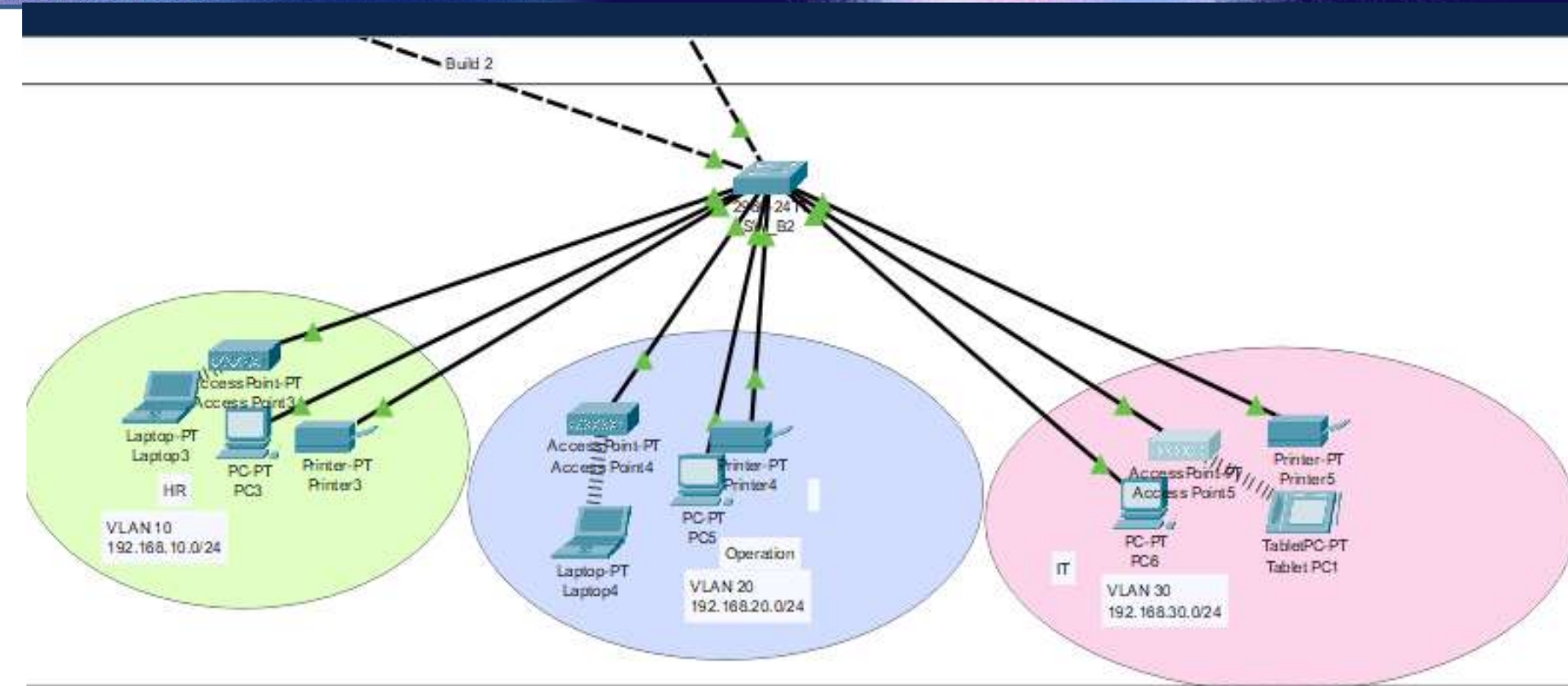
To provide wireless internet access throughout the home.

- **Offices**

To facilitate access to the network and shared resources.

- **Public Areas:**

Such as cafes and airports, to provide internet access for visitors.



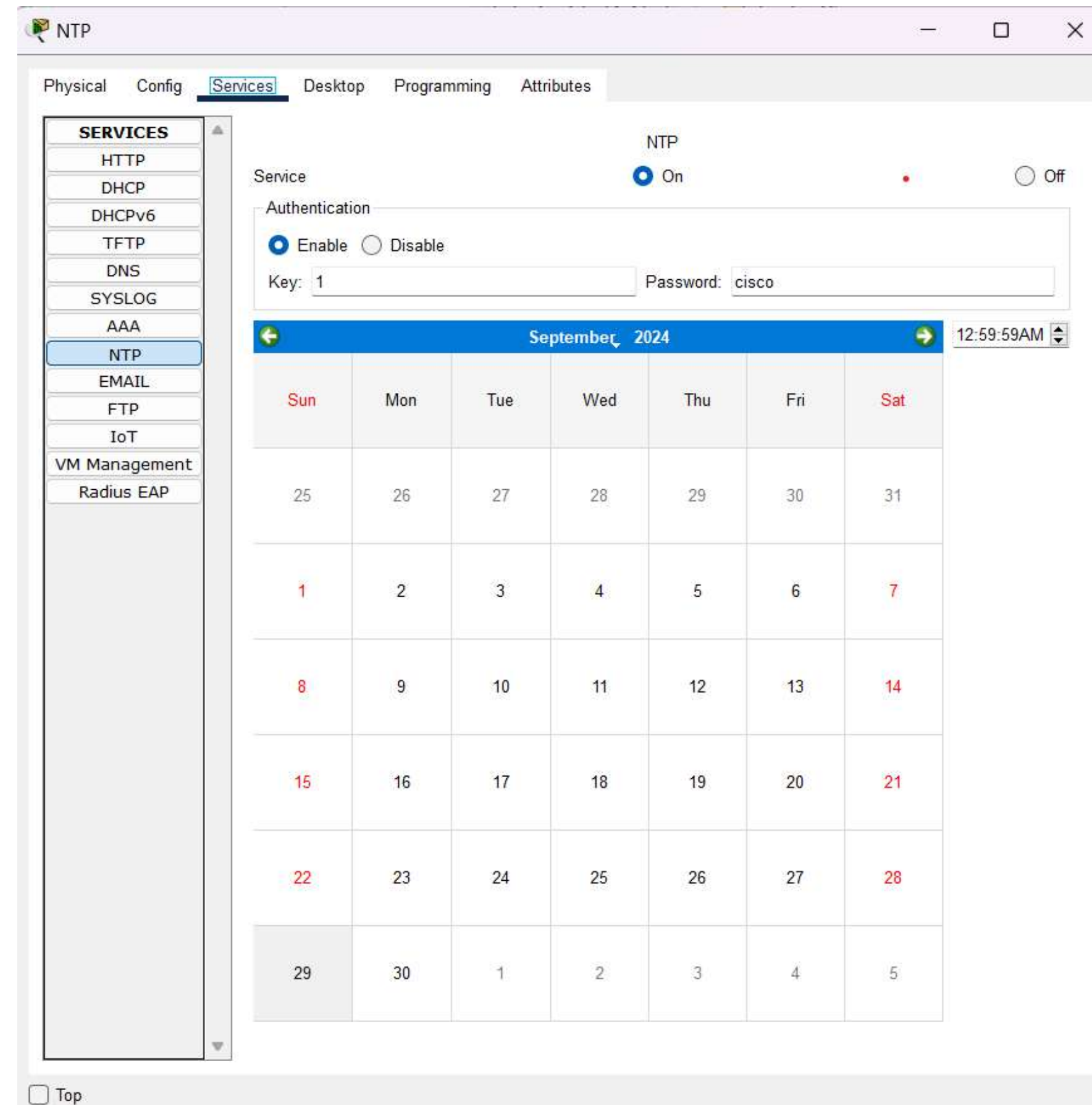
NTP Server

❑ What is NTP:

is a protocol designed to synchronize the clocks of computers or network devices over a network.

❑ Steps to Configure NTP Server:

- **Click on the server** to open the configuration window.
- Go to the **"Services" tab**.
- From the left menu, select **NTP**.
- **Turn NTP Service ON** (ensure the button is green).
- Setting date and clock



NTP Status in Main & Multilayer_SW0

Multilayer Switch0

```
Switch# show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is EA73871E.00000238 (22:9:34.568 UTC Thu Sep 26 2024)
clock offset is 0.00 msec, root delay is 3.00 msec
root dispersion is 10.59 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 5, last update was 28 sec ago.
Switch#
```

Main Router

```
Router# show ntp status
%SYS-5-CONFIG_I: Configured from console by console

Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is EA73862A.0000019F (22:5:30.415 UTC Thu Sep 26 2024)
clock offset is 1.00 msec, root delay is 0.00 msec
root dispersion is 10.30 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 2 sec ago.
Router#
```

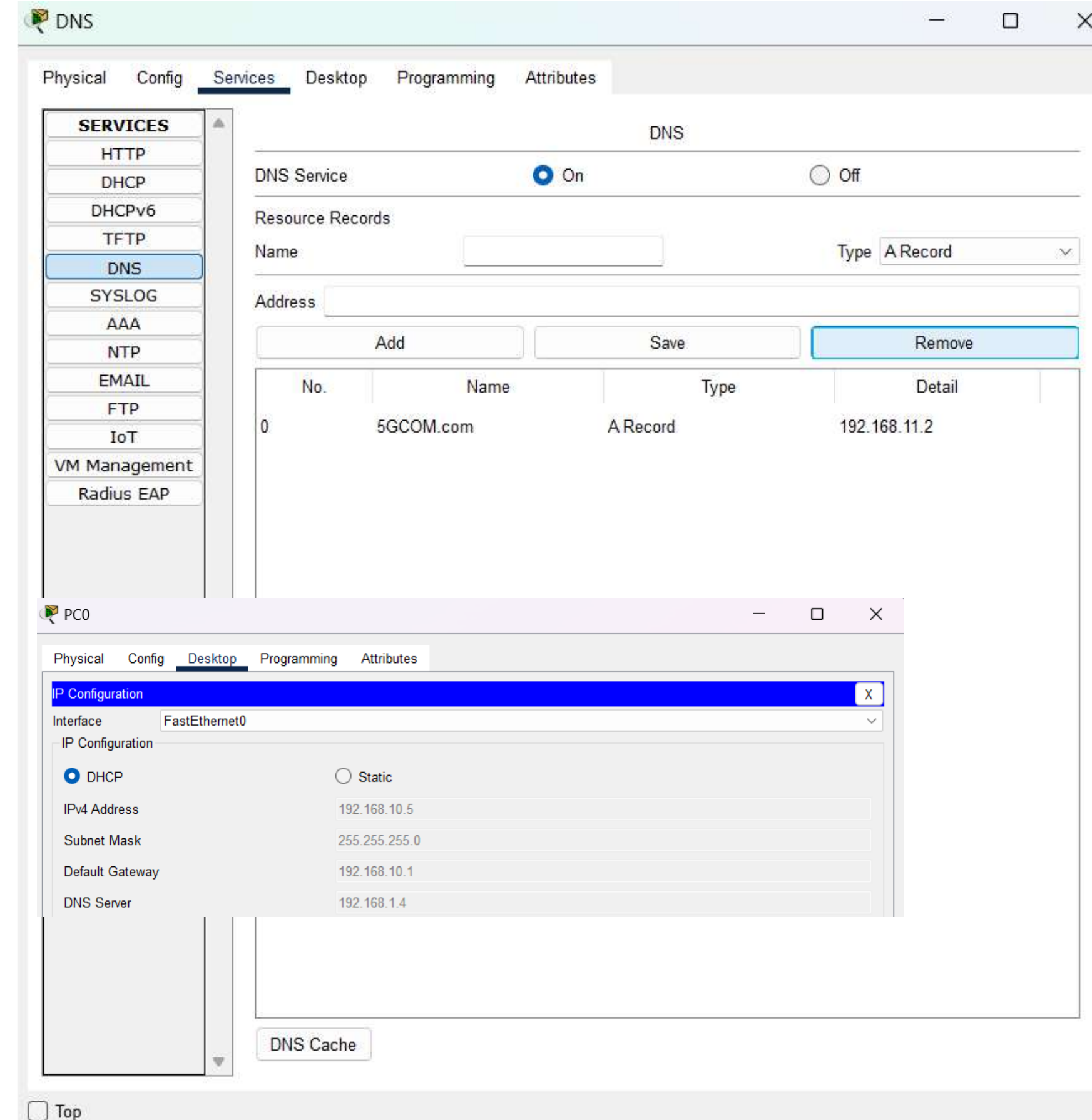

DNS Server

❑ What is DNS?

- DNS (Domain Name System) is like the phonebook of the internet.
- It translates human-readable domain names (e.g., 5GCOM.com) into IP addresses (e.g., 192.168.11.2).

❑ Configuration :

- **Click on the server** to open the configuration window.
- Go to **the "Services" tab**.
- From the left menu, select **DNS**.
- **Turn DNS Service ON** (ensure the button is green).
- Under **"Name"**, enter the domain name you want to resolve (5GCOM.com).
- Under **"Address"**, enter the corresponding IP address of the website (e.g., 192.168.11.2 for PC1 or another device that will host the web service).
- Click **Add** to save the record.



DHCP Server

❑ What is DHCP?

- **DHCP** stands for **Dynamic Host Configuration Protocol**, a network management protocol used to automatically assign IP addresses and other configuration settings to devices on a network.

❑ Steps to Configure DHCP Server:

- **IP DHCP pool [name]**: Creates a DHCP pool on Cisco devices.
- **Configure Gateway** : Assign default gateway and DNS settings.
- **Configure DNS-Server [DNS IP]**: Specifies DNS server for clients
- **Network [IP/subnet]**: Specifies the range of IP addresses to assign.
- **Click Add** to save
- **Start the DHCP Service.**

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.4

Start IP Address : 192 168 1 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 254

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan20_2	10.1.20.1	192.168.1.4	10.1.20.3	255.255.2...	253	0.0.0.0	0.0.0.0
vlan30_2	10.1.30.1	192.168.1.4	10.1.30.3	255.255.2...	253	0.0.0.0	0.0.0.0
vlan10_2	10.1.10.1	192.168.1.4	10.1.10.3	255.255.2...	253	0.0.0.0	0.0.0.0
vlan30	192.168.30.1	192.168.1.4	192.168.30.3	255.255.2...	253	0.0.0.0	0.0.0.0
vlan20	192.168.20.1	192.168.1.4	192.168.20.3	255.255.2...	253	0.0.0.0	0.0.0.0
vlan10	192.168.10.1	192.168.1.4	192.168.10.3	255.255.2...	253	0.0.0.0	0.0.0.0
serverPool	192.168.1.1	192.168.1.4	192.168.1.2	255.255.2...	254	0.0.0.0	0.0.0.0

Syslog Server

❑ What is Syslog?

- Syslog (System Logging Protocol) is a standard protocol used to send and receive log messages from various network devices and servers.

❑ Configure the Router :

- ❖ Click on the **Router** to open its configuration window.
- ❖ Go to the **CLI tab** to access the command-line interface.
- ❖ Enter the following commands to configure Syslog logging on the network device:
 - ❑ enable
 - ❑ configure terminal
 - logging host 192.168.1.6
 - logging trap debugging
 - logging on
 - exit

The screenshot shows the SYSLOG configuration window with the 'Services' tab selected. The 'Syslog' service is turned 'On'. Below the service status, there is a table of log messages. The table has three columns: 'Time', 'HostName', and 'Message'. The messages are numbered 1 through 8. The first four messages are from 192.168.1.1 and the last four are from 192.168.5.1. The messages are: %SYS-5-CONFIG_I: Configure..., %SYS-5-CONFIG_I: Configure..., %SYS-5-CONFIG_I: Configure..., %SYS-6-LOGGINGHOST_STARTSTOP:..., %SYS-5-CONFIG_I: Configure..., %SYS-5-CONFIG_I: Configure..., %SYS-5-CONFIG_I: Configure..., %SYS-6-LOGGINGHOST_STARTSTOP:....

	Time	HostName	Message
1 -		192.168.1.1	%SYS-5-CONFIG_I: Configure...
2 -		192.168.5.1	%SYS-5-CONFIG_I: Configure...
3 -		82.129.80.111	%SYS-5-CONFIG_I: Configure...
4 -		192.168.4.2	%SYS-6-LOGGINGHOST_STARTSTOP:...
5 -		192.168.4.2	%SYS-5-CONFIG_I: Configure...
6 -		192.168.3.2	%SYS-5-CONFIG_I: Configure...
7 -		192.168.1.1	%SYS-5-CONFIG_I: Configure...
8 -		192.168.1.1	%SYS-6-LOGGINGHOST_STARTSTOP:...

Below the table, the CLI tab is active, showing the following commands and output:

```
Router(config)#
Router(config)#logging 192.168.1.6
Router(config)#logging tra
Router(config)#logging trap d
Router(config)#logging trap debugging
Router(config)#logg
Router(config)#logging o
Router(config)#logging on
Router(config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

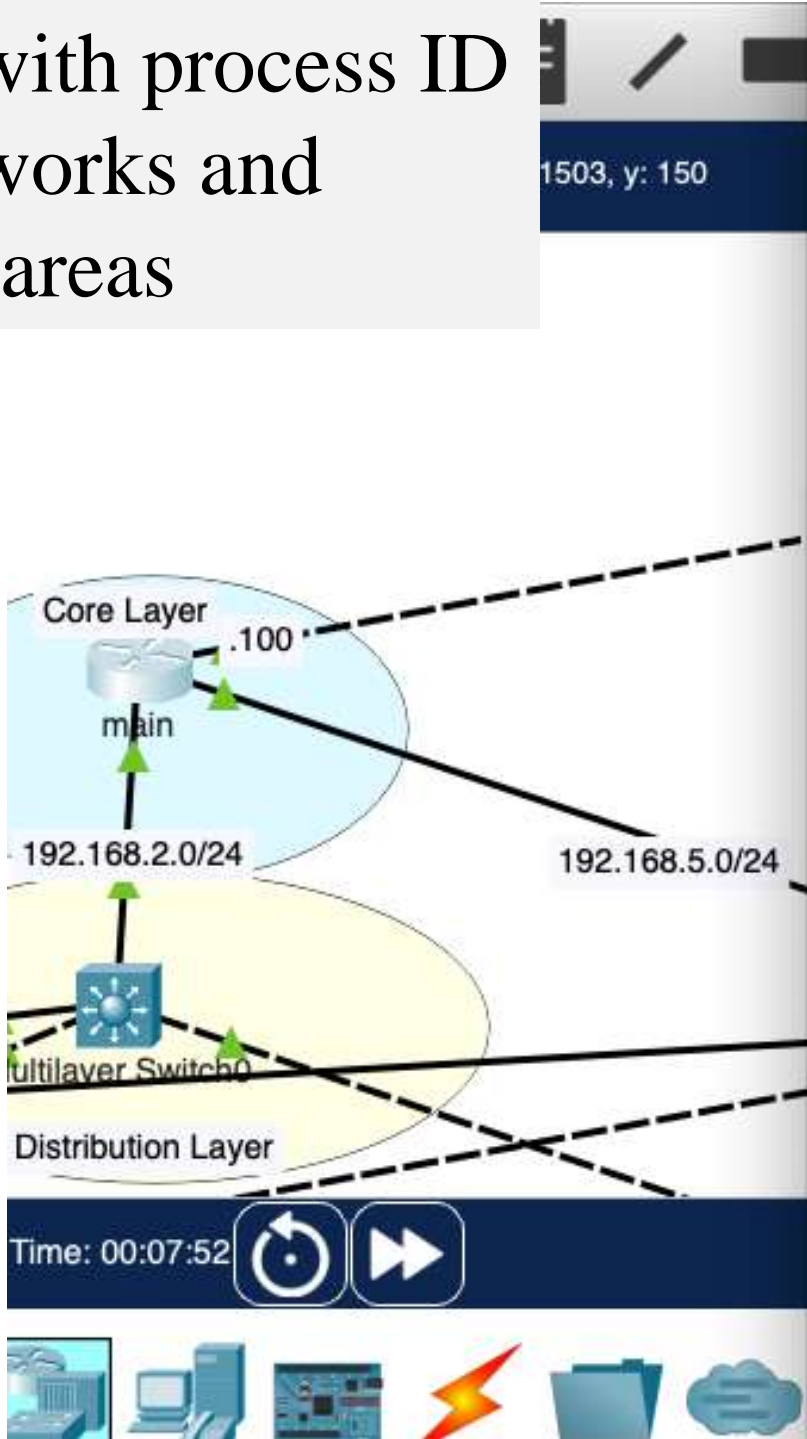
A 'Clear Log' button is located at the bottom right of the window.

1. OSPF Routing

OSPF Routing protocol

OSPF Configuration

- ❑ Enable OSPF with process ID
- ❑ Define the networks and assign them to areas



Result in main router
Routing table

```
10.0.0.0/24 is subnetted, 3 subnets
O    10.1.10.0/24 [110/2] via 192.168.5.2, 00:4294967262:4294967276,
GigabitEthernet0/2
O    10.1.20.0/24 [110/2] via 192.168.5.2, 00:4294967262:4294967276,
GigabitEthernet0/2
O    10.1.30.0/24 [110/2] via 192.168.5.2, 00:4294967262:4294967276,
GigabitEthernet0/2
82.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    82.129.80.0/24 is directly connected, GigabitEthernet0/1
L    82.129.80.100/32 is directly connected, GigabitEthernet0/1
O    192.168.1.0/24 [110/3] via 192.168.2.2, 00:4294967262:4294967276,
GigabitEthernet0/0
[110/3] via 192.168.5.2, 00:4294967262:4294967276,
GigabitEthernet0/2
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/0
L    192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/2] via 192.168.2.2, 00:4294967262:4294967276,
GigabitEthernet0/0
O    192.168.4.0/24 [110/2] via 192.168.5.2, 00:4294967262:4294967276,
GigabitEthernet0/2
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.5.0/24 is directly connected, GigabitEthernet0/2
L    192.168.5.1/32 is directly connected, GigabitEthernet0/2
O    192.168.10.0/24 [110/2] via 192.168.2.2, 00:4294967262:4294967276,
GigabitEthernet0/0
O    192.168.11.0/24 [110/2] via 82.129.80.111, 00:4294967262:4294967276,
GigabitEthernet0/1
O    192.168.20.0/24 [110/2] via 192.168.2.2, 00:4294967262:4294967276,
GigabitEthernet0/0
O    192.168.30.0/24 [110/2] via 192.168.2.2, 00:4294967262:4294967276,
GigabitEthernet0/0
```

02:25:30

Simulation

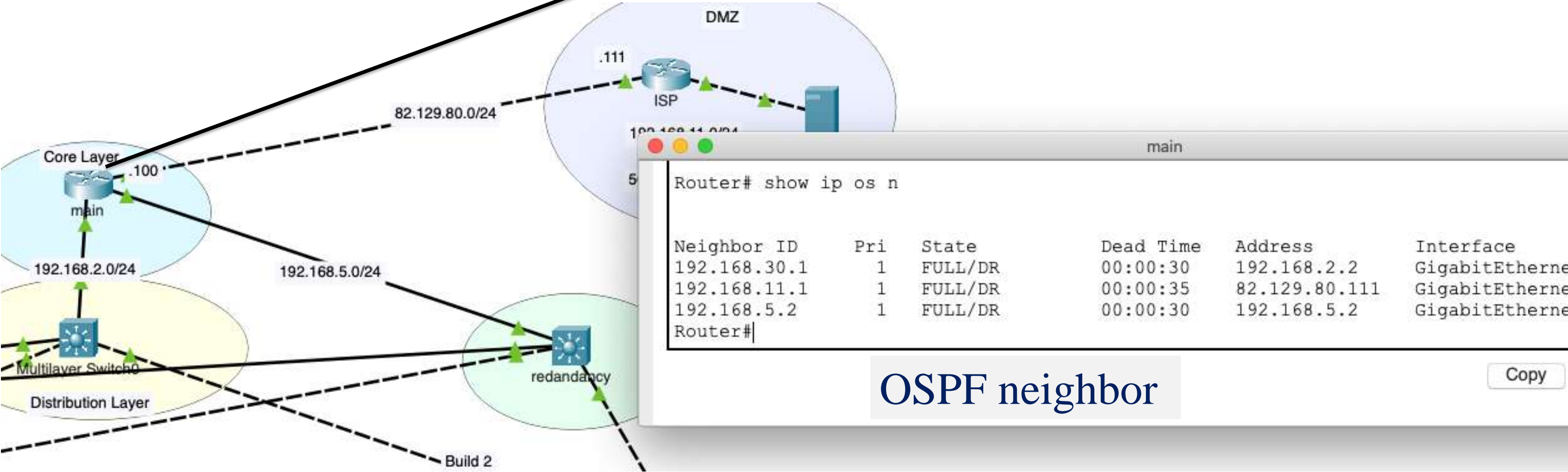
Source Destination

OSPF Routing

OSPF Routing protocol

OSPF Configuration

Result in main router

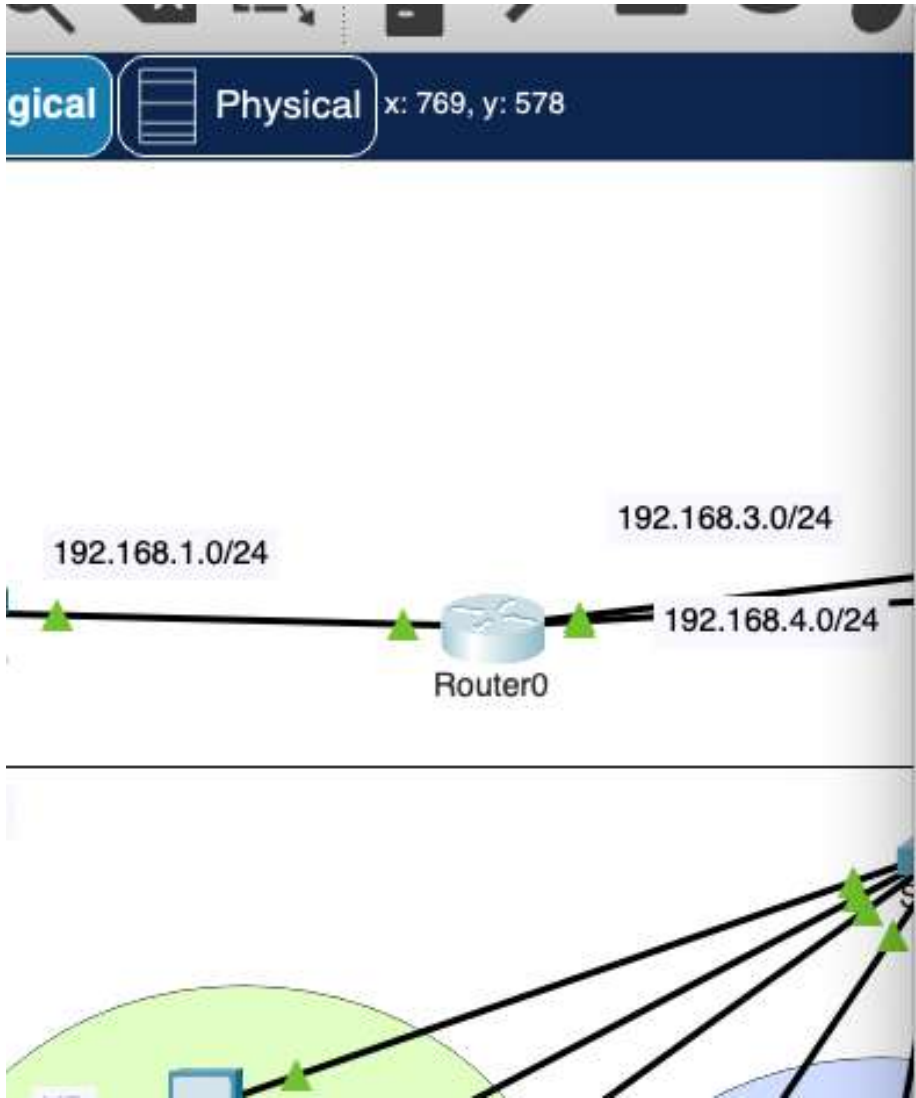


OSPF Routing

OSPF Routing protocol

OSPF Configuration

Routing table



```
Gateway of last resort is not set

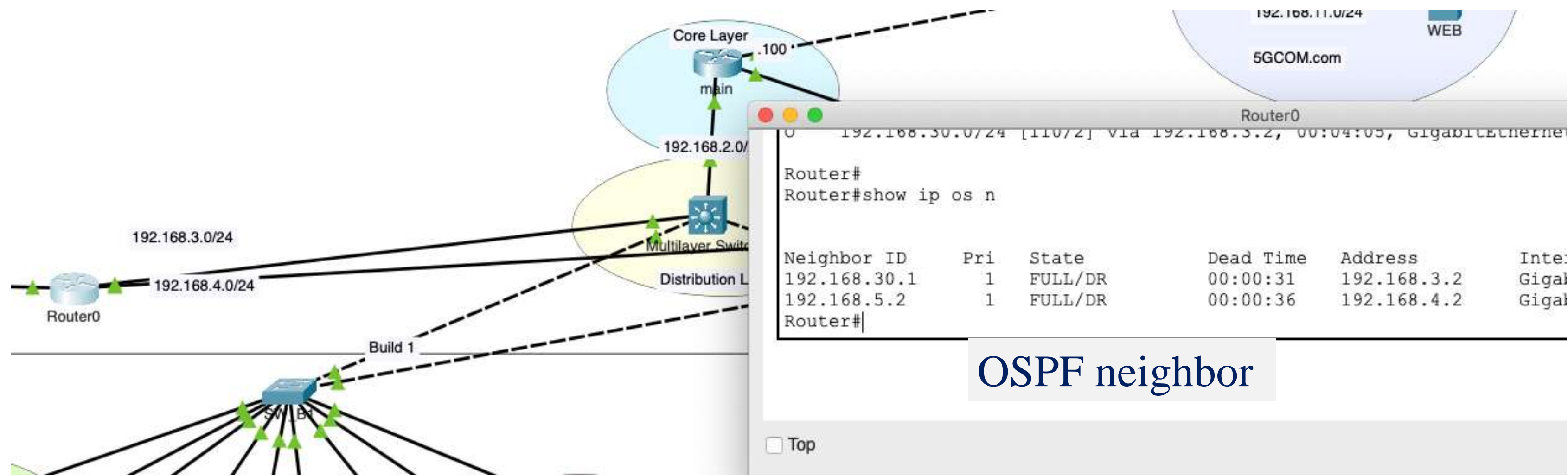
  10.0.0.0/24 is subnetted, 3 subnets
O       10.1.10.0/24 [110/2] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
O       10.1.20.0/24 [110/2] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
O       10.1.30.0/24 [110/2] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
  82.0.0.0/24 is subnetted, 1 subnets
O       82.129.80.0/24 [110/3] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
                                     [110/3] via 192.168.3.2, 00:03:55, GigabitEthernet0/1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/2] via 192.168.3.2, 00:03:55, GigabitEthernet0/1
  192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1
  192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/2
L       192.168.4.1/32 is directly connected, GigabitEthernet0/2
O       192.168.5.0/24 [110/2] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
O       192.168.10.0/24 [110/2] via 192.168.3.2, 00:04:05, GigabitEthernet0/1
O       192.168.11.0/24 [110/4] via 192.168.4.2, 00:03:55, GigabitEthernet0/2
                                     [110/4] via 192.168.3.2, 00:03:55, GigabitEthernet0/1
O       192.168.20.0/24 [110/2] via 192.168.3.2, 00:04:05, GigabitEthernet0/1
O       192.168.30.0/24 [110/2] via 192.168.3.2, 00:04:05, GigabitEthernet0/1

Router#
```


OSPF Routing

OSPF Routing protocol

OSPF Configuration



NAT

NAT Protocol

Port Address Translation (PAT)

The diagram illustrates a network setup for Port Address Translation (PAT). A central router, labeled 'main', is connected to three networks: a core layer (168.2.0/24), an ISP (82.129.80.0/24), and a DMZ (192.168.11.0/24). The DMZ contains a web server (WEB) and an ISP router (ISP). The ISP router is connected to the DMZ and the ISP. The DMZ is also connected to the ISP. The DMZ is labeled 'DMZ' and contains the ISP router and the WEB server. The ISP is labeled 'ISP' and contains the ISP router. The DMZ is labeled '5GCOM.com'.

A web browser window is shown with the URL `http://192.168.11.2` and the page content:

5G Communications

Connecting the World,

About Us Ser

About Our Company

We provide top-notch communication solutions for

A terminal window shows the output of the command `Router#show ip nat tr`:

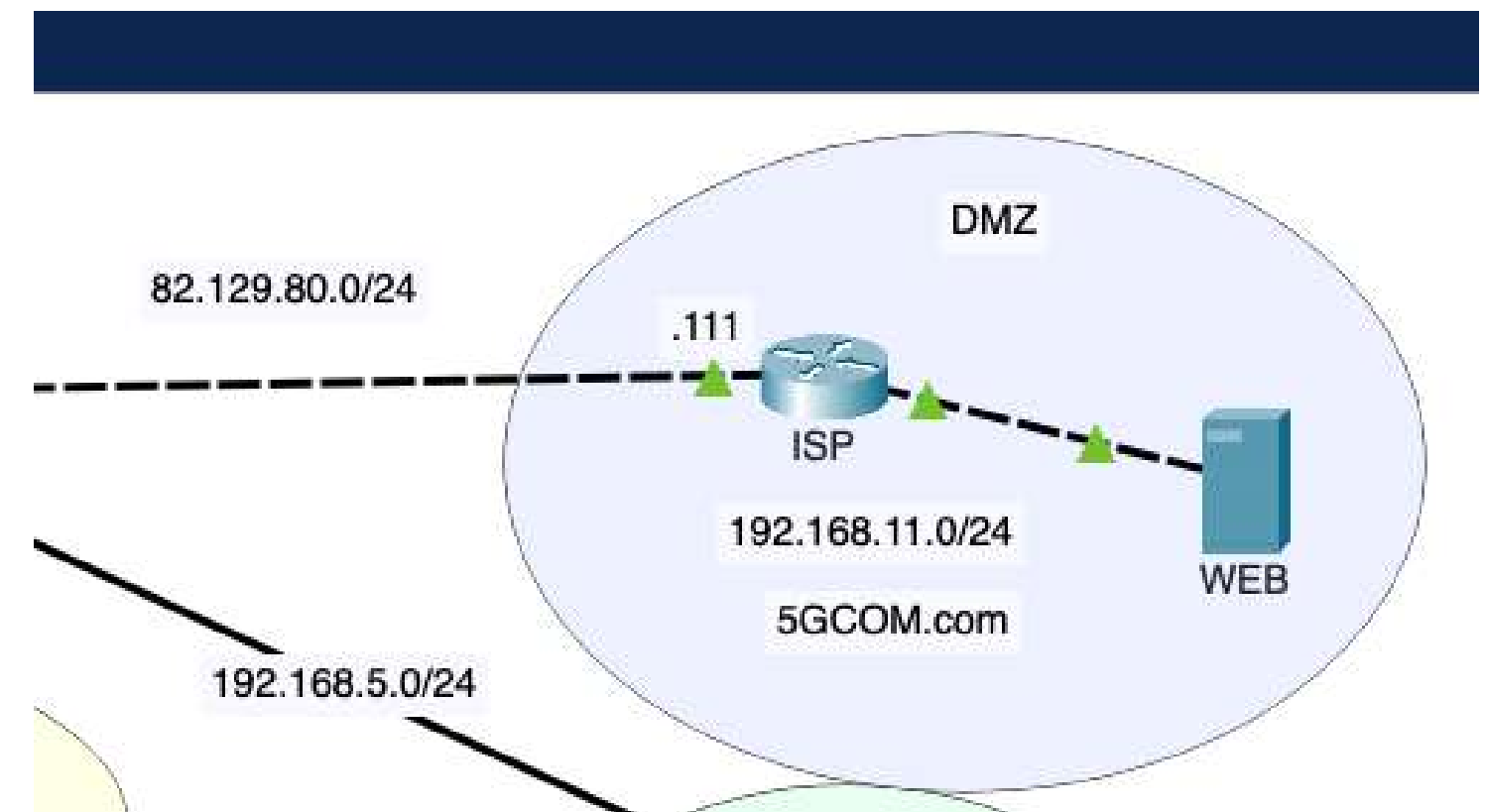
```
Router#show ip nat tr
Pro  Inside global    Inside local    Outside local    Outside global
udp  82.129.80.100:123  192.168.1.5:123  82.129.80.111:123  82.129.80.111:123
tcp  82.129.80.100:1025 192.168.10.5:1025 192.168.11.2:80    192.168.11.2:80
Router#
```


DMZ

A DMZ (Demilitarized Zone)

Setup Works in a DMZ

- ❖ Web server is assigned a private IP (192.168.11.2) in a dedicated DMZ zone, separated from the internal LAN.
- ❖ The server offers public-facing services (HTTP on port 80 in this case), accessible to external users but not directly connected to the internal network.



Router Password Configuration and Network Login

❑ Local Password Authentication

- **Local Password Setup:** configured local password authentication to secure router access. This method involves creating a password directly on the router for users trying to log in through a console and also used the **secret** command, which provides encrypted storage of the password.

❑ Privilege Levels

- Routers have **16 different privilege levels (0–15)**, with **level 15** being the highest level, providing full administrative access.

❑ Enable secret

- The **enable secret** is used to move from user EXEC mode (privilege level 1) to privileged EXEC mode (privilege level 15).
- I configured the enable secret to allow authorized users to elevate their privileges after logging in.

```
Current configuration : 1133 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$gyuIXJhnplcKI.3q1Kd2a/
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username IT privilege 15 secret 5 $1$mERr$3HhIgMGBA/9qNmzgzcuxv0
username user secret 5 $1$mERr$DqFv/bNKU3CFm5jwSLasx/
!
!
license udi pid CISCO2911/K9 sn FTX1524C45G-
!
!
!
```


Access Control Lists (ACLs)

- ❑ ACLs are used to filter traffic in a network based on specific conditions. There are two main types of ACLs in network security:
 - **Standard ACLs and Extended ACLs.**
 - Both serve different purposes and offer different levels of control over the traffic passing through a network device.

❑ We configured an **Extended IP Access List (ACL)** on the router to enhance network security and manage traffic more efficiently.

```
Router>ena
Router#show acc
Extended IP access list 100
    10 permit tcp any any eq www
    20 deny icmp any any echo
    30 permit ip any any (1877 match(es))
```

- ❑ **This ACL effectively:**
 - Allows **HTTP web traffic** (TCP port 80).
 - Denies **ICMP ping requests** for security reasons.
 - Permits all other IP traffic to ensure basic network communication.

Feature	Standard ACL	Extended ACL
Filtering Criteria	Based only on source IP address	Based on source IP, destination IP, protocol, port
Configuration Range	1-99, 1300-1999	100-199, 2000-2699
Use Case	Basic filtering, less specific control	Detailed traffic filtering with precise control
Placement	Close to destination	Close to source
Flexibility	Limited, filters by source IP only	Highly flexible, filters by IP, protocol, and port

Port Security

How It Works

1. Limit Devices:

- Example: Only **2 devices** are allowed to connect to a port.

2. Monitor Devices:

- The switch checks the **MAC addresses** of connected devices.

3. Action on Violation:

- If a new (unauthorized) device tries to connect, the switch takes action based on the violation mode (e.g., shutting down the port).

```
Switch>
Switch>ena
Switch#show por
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/2      1              1              0      Shutdown
Fa0/3      1              1              0      Shutdown
Fa0/4      1              0              0      Shutdown
Fa0/5      1              1              0      Shutdown
Fa0/6      1              1              0      Shutdown
Fa0/7      1              1              0      Shutdown
Fa0/8      1              1              0      Shutdown
Fa0/9      1              1              0      Shutdown
Fa0/10     1              0              0      Shutdown
Fa0/12     1              0              0      Shutdown
```

```
switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      1              1              0      Shutdown
Fa0/2      1              0              0      Shutdown
Fa0/3      1              0              0      Shutdown
Fa0/4      1              0              0      Shutdown
Fa0/6      1              1              0      Shutdown
Fa0/7      1              1              0      Shutdown
Fa0/8      1              1              0      Shutdown
Fa0/9      1              0              0      Shutdown
Fa0/10     1              0              0      Shutdown
Switch#|
```