



DOCUMENTATION

Configuring CISCO network devices and implementing
different network topologies using console cable and Putty
application program



KAREEM DIAA HELAL
CISCO NETWORKING DEVICES PRACTICAL TRAINING

Configuring Cisco network devices and implementing different network topologies

Table of Contents of Day 1:

1. Introduction.....	4
2. Setting the initial basic configuration of a network switch.....	4
3. Setting the device name to S2.....	5
4. Protecting console access by setting a password	5
5. Setting the enable passwords and encrypting it	6
6. Setting up an appropriate message that will be shown to anyone logging into the switch..	6
7. Making sure that all plain text passwords are encrypted	7
8. Troubleshooting the configuration and verifying the configuration.....	7
9. Saving the configuration commands in the NVRAM.....	8

Table of Contents of Day 2:

1. Introduction.....	9
2. Understanding the topology for implementation	9
3. Devices used to build the network	9
4. Connecting the devices together using an Ethernet cable.....	10
5. Configuration of R1	10
5.1 Naming the router to R1	11
5.2 Setting a password for the console port.....	11
5.3 Setting an encrypted password for the privilege EXEC mode	11
5.4 Setting an appropriate message for the banner	11
5.5 Configuring and addressing the interface settings.....	11
5.6 Saving the configuration.....	12
6. Configuration of SW1	12
6.1 Protection for the console port.....	13
6.2 Setting an encrypted password for the privilege EXEC mode	13
6.3 Making sure that all plain text passwords are encrypted.....	13
6.4 Configuring the default management interface so that it will accept connections over the network from local hosts.....	13
6.5 Saving the configuration.....	13
7. Configuration of SW2.....	14
7.1 Naming the network switch to SW2.....	14
7.2 Setting a password for both the console port and the privilege EXEC mode	14
7.3 Setting an appropriate message for the banner.....	14
7.4 Configuring the default management interface so that it will accept connections over the network from local hosts.	15
7.5 Saving the configuration	15

8. Configuration of PC	15
9. Troubleshooting	16
10. Question and Answer (Q&A) section	17

Table of Contents of Day 3:

1. LAB 1: VLAN Configuration and Troubleshooting	18
1.1 What is VLAN and its importance?	18
1.2 Configuring the initial basic switch configuration	18
1.3 Creating VLANs and specifying them for their purpose.....	19
1.4 Assign each port to its specified VLAN.....	19
1.5 Configuring VLANs on L3 switch	21
1.6 Pinging and troubleshooting.....	21
2. LAB 2: EtherChannel Configuration	23
3. LAB 3: OSPF Configuration.....	25
4. Question and Answer (Q&A) Section based on the previous configurations	27

Learning outcomes from this documentation (Objectives):

By the end of this documentation, you should be familiar the following:

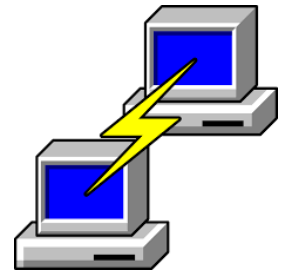
- The essential steps for configuring a switch to ensure secure and stable network operation.
- Learn how to set up the initial switch configuration using a terminal program like PuTTY.
- Gain familiarity with the main configuration modes on a switch, including User EXEC Mode, Privileged EXEC Mode, and Global Configuration Mode.
- Set up a Message of the Day (MOTD) banner to provide a security message to users when logging into the switch.
- Learn how to assign a hostname to the switch for easy identification within the network.
- Understand the process of securing console access by setting up a password to prevent unauthorized access.
- Learn how to set enable passwords and encrypt them for added security.
- Ensure that all plain text passwords are encrypted to prevent them from being displayed in configuration files.
- Verify and troubleshoot the configuration to ensure all settings have been applied correctly.
- Save the configuration commands to NVRAM to ensure they persist after a reboot.
- Understand the concept and importance of VLANs in network segmentation and security.
- Create and configure VLANs for specific purposes within a network.
- Assign switch ports to the appropriate VLANs and understand the differences between access mode and trunk mode.
- Configure VLANs on a Multilayer Switch (L3 switch) and enable inter-VLAN routing for communication across VLANs.
- Understand EtherChannel and its role in enhancing network link reliability and performance.
- Learn the differences between LACP (Link Aggregation Control Protocol) and PAgP (Port Aggregation Protocol).
- Configure OSPF (Open Shortest Path First) on routers to facilitate dynamic routing within the network.
- Understand and configure a loopback interface on the router to ensure stability and consistent routing in OSPF.
- Implement OSPF across multiple routers and verify OSPF operation through connectivity tests.
- Troubleshoot issues related to VLAN and OSPF configurations, and ensuring communication across VLANs and stability of the OSPF network.

Day 1: Configuring Switch S2 using Putty

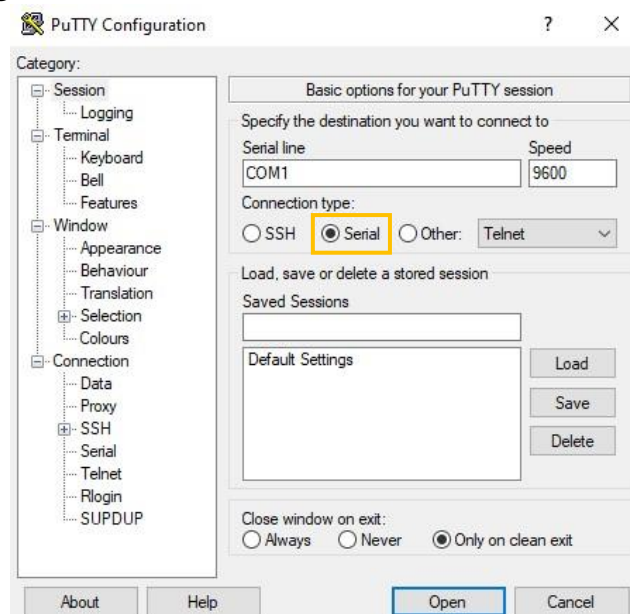
1. Introduction

This documentation provides essential steps for configuring Switch S2 to ensure secure network operation. It covers setting the device name, securing console access, configuring enable passwords, and encrypting information. Follow this guide to understand clearly Switch S2's configuration and enhance your network's security and stability.

The first step to do for a switch is to set up the initial switch configuration. To set up the initial switch configuration, you will need to open a program to configure the switch from a program, here we will use **Putty** application program.



Once you open the program from your PC or laptop, you will see the interface of the program, here we will choose the connection type “Serial” because the PC is connected to the switch by a serial cable, then click Open to start the configuration.



2. Setting the initial basic configuration of the network switch

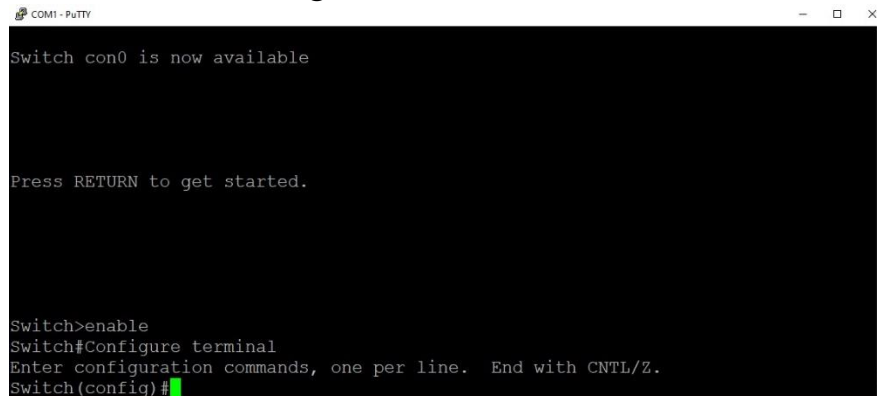
Once you start the session, you will set up the initial configuration but firstly you need to understand the main modes in the configuration of the switch.

- The first mode is “**User EXEC Mode**”, this mode provides basic monitoring commands and limited configuration. it is written by:

Switch>

- The second mode is “**Privileged EXEC Mode**”, it can access to all commands for monitoring the switch. It is written by: **Switch#**
- The third mode is “**Global Configuration Mode**”, It allows the user to configure global commands that affect the switch. It is written by: **Switch (config)#**

The first step is to use the command “enable” in the user mode, then the command “configure terminal” in the privileged mode, so that we can complete the rest of the configuration.



```
COM1 - PuTTY
Switch con0 is now available

Press RETURN to get started.

Switch>enable
Switch#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

3. Setting the device name to S2

To identify the switch, we will need to set a name for it, for example S2. To complete this step, we will write “hostname S2” in the global configuration mode.

```
Switch(config)#hostname S2
S2(config)#
```

4. Protecting console access by setting a password

To protect the switch from unauthorized access via the console, we will type this command in the global configuration mode: **line console 0**

After that, we should type the password for the console, for example “we123” as shown in the configuration. Then type **login** to confirm the password for the console port.

```
S2(config)#line console 0
S2(config-line)#password we123
S2(config-line)#login
S2(config-line)#exit
```

After configuring the console password, a syslog message will appear to confirm that the password is set up successfully.

```
*Aug 12 11:43:34.844: %SYS-5-CONFIG-I: Configured from console by consolet
```

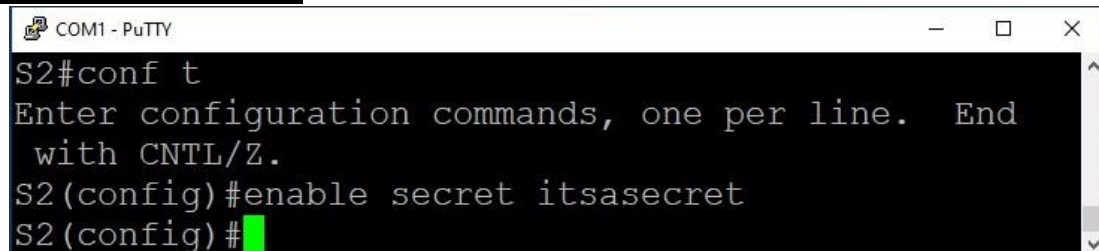
5. Setting the enable passwords and encrypting it

To control access to privileged mode, you should set the enable password by using the enable password command.

For example, **“enable password CiscoWE”**

```
S2>enable
S2#configure terminal
Enter configuration commands, one per
line. End with CNTL/Z.
S2(config)#enable password CiscoWE
```

And for more security, we use the enable secret command. For example, **“enable secret itsasecret”**



```
COM1 - PuTTY
S2#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
S2(config)#enable secret itsasecret
S2(config)#
```

6. Setting up an appropriate message that will be shown to anyone logging into the switch

To display a security message to users when logging into the switch, we use the message of the day command. We write motd and then the text we want to appear for the user when logging in. For example, **motd “Welcome Administrator. Authorized People Only!”**.

```
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Welcome Administrator. Authorized People Only!"
S2(config)#exit
S2#
*Aug 12 12:10:58.035: %SYS-5-CONFIG_I: Configured from console by console
```

Attention!! Don not forget the double quotations between the message you want to appear.

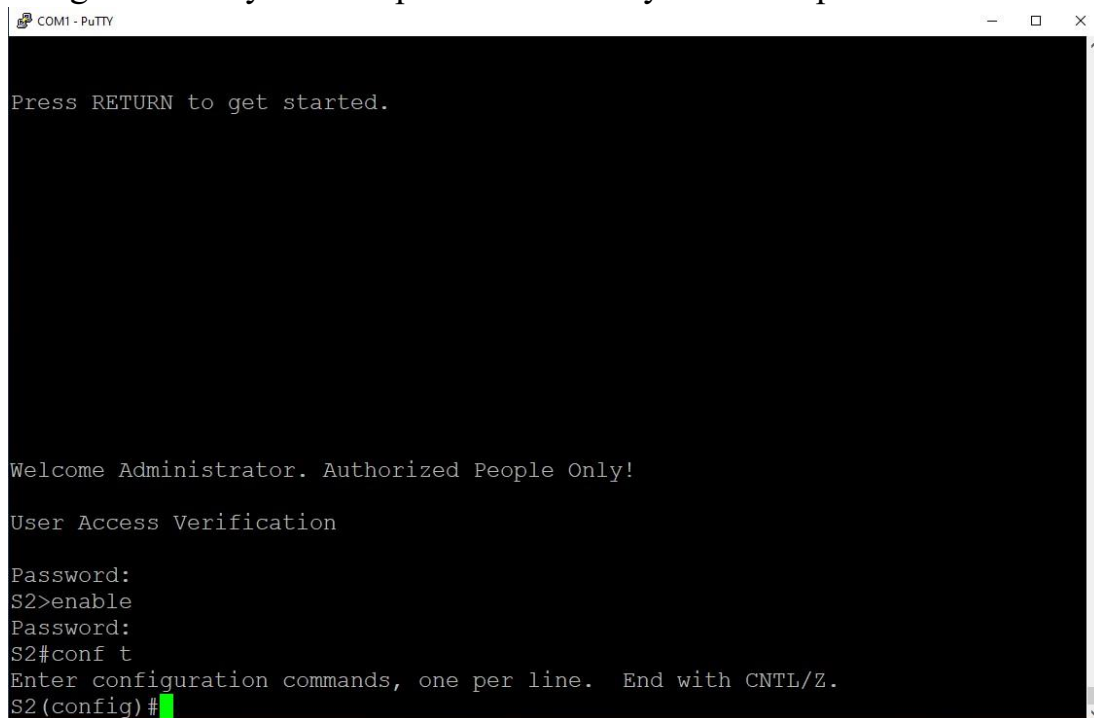
7. Making sure that all plain text passwords are encrypted

To prevent plain text passwords from being displayed in configuration files, we use the command **"Service password-encryption"** in the global configuration mode.

```
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#service password-encryption
S2(config)#exit
S2#
*Aug 12 12:06:03.522: %SYS-5-CONFIG I: Configured from console by console
```

8. Troubleshooting the configuration and verifying the configuration

Double-check to make sure everything is configured correctly by starting from the begging and try to write any command but it will display the message of the day we set up and it will ask you for the password.



```
COM1 - PuTTY
Press RETURN to get started.

Welcome Administrator. Authorized People Only!

User Access Verification

Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#
```

To ensure all settings have been applied correctly, we use the command **"show running-config"** or for short **"show run"**.

```
S2#show running-config
Building configuration...
```


Here as shown in the two figures, the passwords we set are encrypted successfully. But you may use an advanced tool to ensure more security.

```
!  
enable secret 5 $1$8266$UmpTAl1MmlNFsQnV3WmKo/  
enable password 7 112A1016141D3C29  
!
```

```
line con 0  
password 7 095B4B584B56  
login
```

9. Saving the configuration commands in the NVRAM

To save and ensure that all the configuration is saved, we will use this command in the privileged mode: **copy running-config startup-config**. And it automatically will be saved in your Non-volatile random-access memory (NVRAM).

```
S2#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
Compressed configuration from 2424 bytes to 1279 bytes[OK]
```

Just a reminder to save your commands to prevent losing your settings if the switch is turned off.

Day 2: Network Topology Configuration using Putty

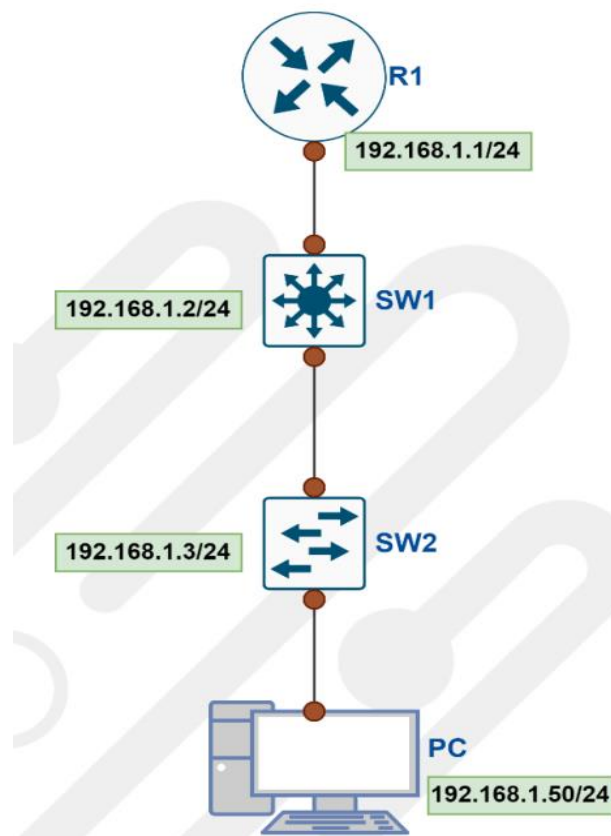
1. Introduction

This documentation provides essential configurations for configuring a simple network topology in which a PC can successfully communicate with a router (R1) and two switches (SW1 and SW2).

It covers configuration such as device naming, establishing connections between devices, setting up passwords for security, configuring interface settings on the router and switches, and configuring the PC with the IP. By following this step-by-step guide, you should be able to create a simple network topology.

2. Understanding the topology for implementation

Here in the following topology as shown in the figure, we will need to connect a router with a multilayer switch to be connected with the other switch and the second switch will be connected to the computer.



3. Devices used to build the network

- A network router: Cisco 1900 Series
- A multilayer switch (Layer 3 switch)
- A network switch: Catalyst 3650
- A computer

4. Connecting the devices together using an Ethernet cable

As we known from the previous documentation that to configure any network device you will obviously need to connect it with a console cable to the computer where you are monitoring from using application Putty.

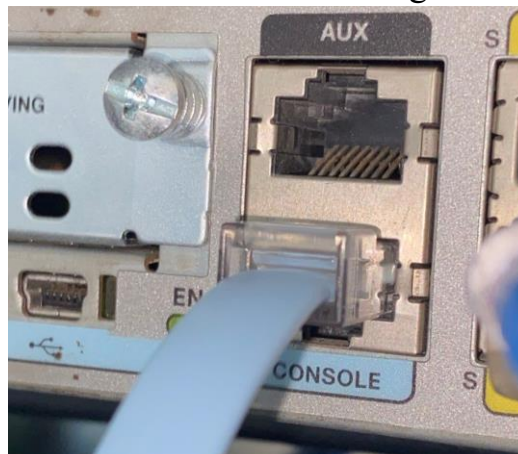


In this documentation, when configuring R1, SW1, and SW2, we will connect the network device to the PC using the console cable. The ethernet port will be connected to the network device we want to configure and the serial interface will be on the backside of the computer.



5. Configuration of R1

At the beginning of the configuration, we will need to connect the router to the PC using a console cable. As shown in the figure:



5.1 Naming the router to R1

Of course, in any network it is important to differentiate between all the devices in the network, that's why it's important to set a hostname for the device. As shown in the configuration, here is how to set a hostname for the router:

```
Router> enable
```

```
Router# configure terminal
```

```
Router (config)# hostname R1
```

```
Router#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router (config) #hostname R1
```

5.2 Setting a password for the console port

It is very important to set a password for the console port to allow the access for authorized people only. In the next example, the password of the console will be "wel23". Here is how to set a password for the console port:

```
R1 (config)# line console 0
```

```
R1 (config-line)# password wel23
```

```
R1 (config-line)# login
```

```
R1 (config) #line console 0
```

```
R1 (config-line) #password wel23
```

```
R1 (config-line) #login
```

5.3 Setting an encrypted password for the privilege EXEC mode

To secure the router and switches, it's important to set an encrypted password for privileged EXEC mode. In the next example, the password for the privilege mode is "comm", here is how:

```
R1 (config)# enable secret comm
```

```
R1 (config) #enable secret comm
```

5.4 Setting an appropriate message for the banner

A Message of the Day (MOTD) banner is an important parameter for warning unauthorized users and providing important information when people try to access the devices. To set a MOTD, use the following command:

```
R1 (config)# banner motd "Authorized Access Only!"
```

```
Router (config) #banner motd "Authorized Access Only!"
```

Attention!! Don't forget the quotation marks between the text you want to appear when anyone try to access the configuration.

5.5 Configuring and addressing the interface settings

In this topology, R1 is connected with SW1 using interface GigabitEthernet 0/0. So that, here is how to address the interface settings:

```
R1 (config)# interface GigabitEthernet 0/0
```

```
R1 (config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1 (config-if)# no shutdown
```

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

5.6 Saving the configuration

To save and ensure that all the configuration is saved, we will use this command in the privileged mode: **copy running-config startup-config**

And it automatically will be saved in the Non-Volatile Random-Access Memory (NVRAM). And instead, you can write **"wr"** for short, it has the same purpose.

```
R1(config)#do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Reminder: It's very important to save your work after finishing the configuration to prevent losing your settings if the switch is turned off.

6. Configuration of SW1

At the beginning of the configuration, you will need to connect the multilayer switch to the PC using a console cable. As shown in the picture:



Additionally, SW1 (Multilayer Switch) will be connected to SW2 (Network Switch) using an Ethernet cable. As shown in the picture:



6.1 Protection for the console port

Protection for the console port is important to ensure that only authorized users can access the device's console. Here is how protect it:

```
Core_1 (config)# line console 0
```

```
Core_1 (config-line)# password wel23
```

```
Core_1 (config-line)# login
```

```
Core_1 (config)# line console 0
Core_1 (config-line)# password wel23
Core_1 (config-line)# login
Core_1 (config-line)# exit
```

6.2 Setting an encrypted password for the privilege EXEC mode

To secure the privilege EXEC mode, set an encrypted password by writing:

```
Core_1 (config)# enable secret comm
```

```
Core_1 (config)# enable secret comm
```

6.3 Making sure that all plain text passwords are encrypted

To prevent plain text passwords from being displayed in configuration files, we use the command "Service password-encryption" in the global configuration mode

```
Core_1 (config)# service password-encryption
```

6.4 Configuring the default management interface so that it will accept connections over the network from local hosts

Configuring the management interface allows the switch to be managed over the network. The switch has a lot of VLANs (Virtual Local Area Networks) but the default management interface is vlan 1. Here is how to configure the default management interface:

```
Core_1 (config)# interface vlan 1
```

```
Core_1 (config-if)# ip address 192.168.1.2 255.255.255.0
```

```
Core_1 (config-if)# no shutdown
```

```
Core_1 (config)# interface vlan 1
```

```
Core_1 (config-if)# ip address 192.168.1.2 255.255.255.0
```

```
Core_1 (config-if)# no shutdown
```

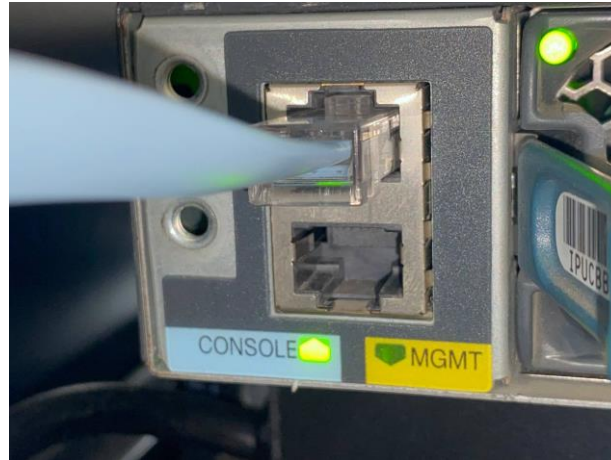
6.5 Saving the configuration

Don't forget to save the work after finishing the configuration by writing: [wr](#)

```
Core_1#wr
Building configuration...
[OK]
```

7. Configuration of SW2

As we did for the router and SW1, the same for SW2. Connect the console cable to the network switch with the PC ash shown in the picture:



7.1 Naming the network switch to SW2

Setting the hostname of the switch by typing:

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch (config)# hostname SW2
```

```
Switch>enable
```

```
Switch#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#hostname SW2
```

7.2 Setting a password for both the console port and the privilege EXEC mode

Setting the password for the console and the privilege mode as we did before by writing:

```
SW2 (config)# line console 0
```

```
SW2 (config-line)# password wel23
```

```
SW2 (config-line)# login
```

```
SW2 (config-line)# exit
```

```
SW2 (config)# enable secret comm
```

```
SW2 (config)#line console 0
```

```
SW2 (config-line)#password wel23
```

```
SW2 (config-line) #login
```

```
SW2 (config-line) #exit
```

```
SW2 (config) #
```

```
SW2 (config) #
```

```
SW2 (config) #enable secret comm
```

7.3 Setting an appropriate message for the banner

Here is how to set a MOTD banner:

```
SW2 (config)# banner motd "Authorized Access Only!"
```

```
SW2 (config) #banner motd "Authorized Access Only!"
```

7.4 Configuring the default management interface so that it will accept connections over the network from local hosts

To configure the default management interface, write:

```
SW2 (config)# interface vlan 1
SW2 (config-if)# ip address 192.168.1.3 255.255.255.0
SW2 (config-if)# no shutdown
SW2 (config)# interface vlan 1
SW2 (config-if)# ip address 192.168.1.3 255.255.255.0
SW2 (config-if)#
SW2 (config-if)#
SW2 (config-if)# no shutdown
SW2 (config-if)# exit
```

7.5 Saving the configuration

Again, don't forget to save your work.

```
SW2#wr
Building configuration...
Compressed configuration from 2374 bytes to 1233 bytes[OK]
```

8. Configuration of PC

The first thing to do for a computer is to set an IP address for it whether by static or dynamically. In this example, we will set the IP address for the PC statically, follow the following steps:

1. Open the cmd of your computer but choose "RUN AS ADMINISTRATOR".
2. Write **ipconfig** to know what is the name of the Ethernet.

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1d93:57b7:8b00:cbad%8
    IPv4 Address. . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

And here all the details of the IP address are shown. At this step, we knew that the Ethernet Adapter name is "Ethernet 2".

3. Write the following command:

```
Netsh interface ip set address name="Ethernet 2" static 192.168.1.4 255.255.255.0 192.168.1.1
```

```
C:\Windows\system32>netsh interface ip set address name="Ethernet 2" static 192.168.1.4 255.255.255.0 192.168.1.1
```


9. Troubleshooting

To ensure that the work we did is successful, we should troubleshoot it by pinging the PC by its ip address to all other devices and it should ping successfully.

Here is pinging the PC to the network router:

```
C:\Users\vip>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging the PC to the multilayer switch SW1:

```
C:\Users\vip>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging the PC to the network switch SW2:

```
C:\Users\vip>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=2ms TTL=255
Reply from 192.168.1.3: bytes=32 time=2ms TTL=255
Reply from 192.168.1.3: bytes=32 time=2ms TTL=255
Reply from 192.168.1.3: bytes=32 time=6ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

All of the above pings are 0% loss which means that our network is configured successfully and now the PC can send any packet to the two switches and the router.

10. Question and Answer (Q&A) Section

Based on the previous configuration, the following questions clarify the configuration we did:

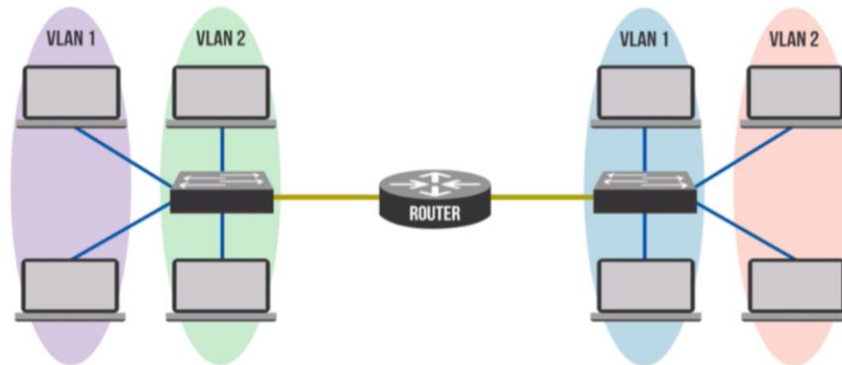
- What command did you use to save the configuration to NVRAM?
 - `#Copy running-config startup-config`
- What is the shortest version of this command that still works?
 - `#wr`
- Why should every router have a Message of the Day (MOTD) banner?
 - It provides a warning or important information to anyone trying to access the network device. It can serve as a warning to unauthorized access by displaying a message that access is restricted and unauthorized use is prohibited.
- What command do you use to view the configuration?
 - `#show running-config`
- Why do you need to enter the no shutdown command on the interface?
 - To bring an interface out of the down state. By default, interfaces on routers and switches are disabled, so without the no shutdown command, the traffic will have a big problem and no traffic will be passed.
- What is the command to save the configuration from RAM to NVRAM?
 - `#copy running-config startup-config`

Day 3: VLAN, EtherChannel, and OSPF Configurations

LAB 1: VLAN Configuration and Troubleshooting:

1.1 What is VLAN and its importance?

A VLAN (Virtual Local Area Network) is a logical grouping of network devices that allows them to communicate as if they were on the same physical network, regardless of their actual location. Importance of VLANs: higher security, higher performance, increases the number of broadcasts, and more flexibility.



1.2 Configuring the initial basic switch configuration

At the beginning of every network device, we must configure the initial basic configuration, here is the basic network configuration:

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch (config)# hostname SW2
```

```
SW2 (config)# line console 0
```

```
SW2 (config-line)# password comm
```

```
SW2 (config-line)# login
```

```
SW2 (config-line)# exit
```

```
SW2 (config)# enable secret wel23
```

```
SW2 (config)# banner motd "Don't touch my switch!"
```

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#line console 0
SW2(config-line)#password comm
SW2(config-line)#login
SW2(config-line)#ex
SW2(config-line)#exit
SW2(config)#enable sec
SW2(config)#enable secret wel23
SW2(config)#banner motd "Kareem, Don't touch my switch!"
```

1.3 Creating VLANS and specifying them for their purpose

To create a vlan, follow the following steps:

```
SW2 (config)# vlan 10
```

```
SW2 (config-vlan)# name it
```

An the same for both vlan 20 and vlan 30:

```
SW2 (config)# vlan 20
```

```
SW2 (config-vlan)# name comm
```

```
SW2 (config-vlan)# exit
```

```
SW2 (config)# vlan 30
```

```
SW2 (config-vlan)# name hr
```

```
SW2 (config)#vlan 10
SW2 (config-vlan) #name it
SW2 (config-vlan) #exit
```

```
SW2 (config)#vlan 20
SW2 (config-vlan) #name comm
SW2 (config-vlan) #exit
```

```
SW2 (config)#vlan 30
SW2 (config-vlan) #name hr
SW2 (config-vlan) #exit
```

1.4 Assign each port to its specified VLAN

There are two types of modes that exists in the switchport:

- **Access mode:** the access mode is used to connect end devices such as PCs that belong to a single VLAN and the port carries traffic for only one VLAN, and all frames that pass through are untagged.
- **Trunk mode:** the trunk mode is used to connect switches to each other or to other network devices that need to handle multiple VLANs. The trunk mode carries traffic for multiple VLANs. VLAN tags are used to identify which VLAN each frame belongs to. The default native VLAN is VLAN 1, and traffic for the native VLAN is sent untagged.

For the switch ports that will be connected to the PCs, they will have the access mode as shown in the figure:

```
SW2 (config)#int range g1/0/1-2
SW2 (config-if-range)#switchport mode access
SW2 (config-if-range)#switchport access vlan 10
SW2 (config-if-range)#exit
```

In this configuration, the interfaces GigabitEthernet 1/0/1 and 1/0/2 will be in vlan 10 and they are access mode.

The interfaces GigabitEthernet 1/0/3 and 1/0/4 will be also access mode but in vlan 20:

```
SW2(config)#int range g1/0/3-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#exit
```

The interfaces GigabitEthernet 1/0/5 and 1/0/6 will be also access mode but in vlan 30:

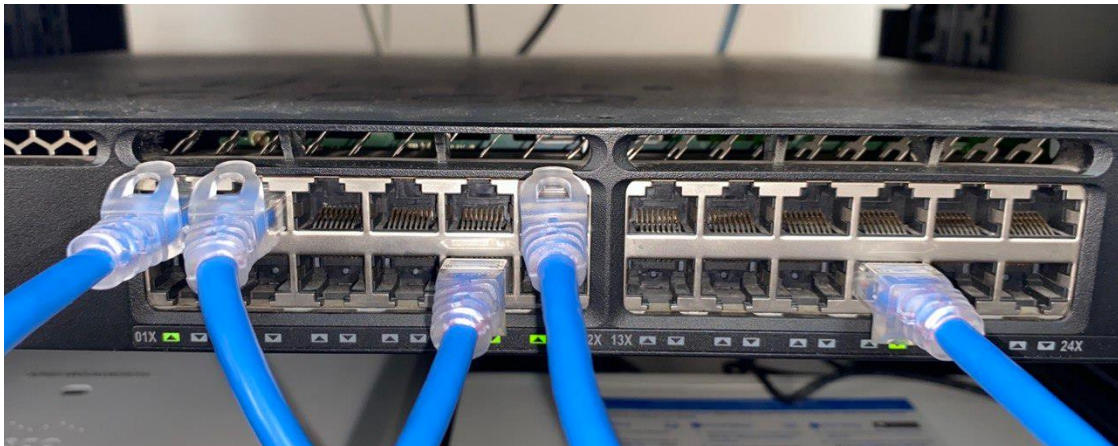
```
SW2(config)#int range g1/0/5-6
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
SW2(config-if-range)#exit
```

And the interfaces connected to the other switches will be trunk mode and automatically will be in vlan 1 as shown. The interfaces GigabitEthernet 1/0/10 is connected to a switch and GigabitEthernet 1/0/11 is connected to a Multilayer Switch.

```
SW2(config)#int range g1/0/10-11
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#exit
```

The interface GigabitEthernet 1/0/20 is connected to another switch which will also be trunk:

```
SW2(config)#interface g1/0/20
SW2(config-if)#switchport mode trunk
```



1.5 Configuring VLANs on L3 switch

For the Multilayer switch configuration, we must also configure the vlans on it and verify them but will be given an IP address and a subnet mask to make the vlans communicate with each other:

1. Configuring vlan 10 on the L3 switch:

```
Switch(config)#interface vlan 10
Switch(config-if)#no shut
Switch(config-if)#ip add 192.168.10.1 255.255.255.0
```

Here we gave the vlan 10 an ip address and a subnet mask and then started it to be available on the network. We will do the same for vlan 20 and vlan 30 on the L3 switch.

2. Configuring vlan 20 on the L3 switch:

```
Switch(config)#interface vlan 20
Switch(config-if)#ip add 192.168.20.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
```

3. Configuring vlan 30 on the L3 switch:

```
Switch(config)#interface vlan 30
Switch(config-if)#no shut\
*Jan  2 01:25:54.203: %LINEPROTO-5-UPDOWN: Line protocol
o shut
Switch(config-if)#ip add 192.168.30.1 255.255.255.0
Switch(config-if)#no shut
```

Alright! but there will be a simple command to write on the L3 switch to make the PCs at each vlan communicate with each other which is:

```
Switch(config)#ip routing
```

1.6 Pinging and troubleshooting

Before pinging, we have to check for the ip addresses that are assigned to each vlan. As shown in the figure, each ip address is assigned to its vlan successfully:

```
Switch(config)#do show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
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
```

Here we used the command **"show ip interface brief"** to check each interface and its assigned ip address.

And now it's time to ping the PCs with each other to check the connectivity:

```
C:\Windows\system32>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

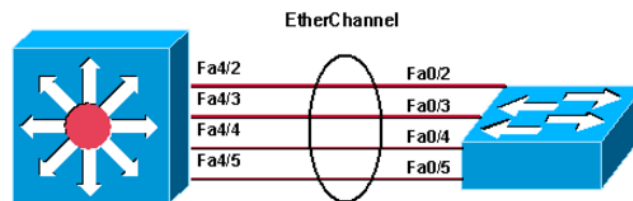
C:\Windows\system32>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
```

As you can see that the connectivity is successful and now any device in vlan 10, 20, or 30 can communicate with any vlan in the network.

LAB 2: EtherChannel Configuration

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.



To implement an EtherChannel, you must first understand that there are two ways to use an EtherChannel link:

1. LACP (Link Aggregation Control Protocol)

LACP is an IEEE standard defined in IEEE 802.3ad. LACP lets devices send Link Aggregation Control Protocol Data Units (LACPDU) to each other to establish a link aggregation connection.

2. PAgP (Port Aggregation Protocol)

PAgP is a proprietary specification designed and authored by Cisco.

The first thing to do is to combine the interfaces together to make the EtherChannel link using the following steps:

```
Switch (config)# interface range GigabitEthernet0/1 – 2
Switch (config-if-range)# channel-group 1 mode active
Switch (config-if-range)# interface port-channel 1
Switch (config-if-range)# switchport trunk encapsulation dot1Q
```

```
SW1(config-if)#interface range g3/0/1-2
SW1(config-if-range)#channel-group 2 mode desirable
SW1(config-if-range)#interface port-channel 2
SW1(config-if)#switchport trunk encapsulation dot1q
```

```
SW1(config)#interface range g3/0/3-4
SW1(config-if-range)#channel-group 1 mode active
SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport trunk encapsulation dot1q
```

For the EtherChannel link, we have to understand that it cannot be two interfaces opposite to each other to be “Passive” in LACP or “Auto” in PAgP. It must be at least one active (or desirable) and one passive (or auto). And it's better if the both interfaces are active (or desirable).

Important show command to use for ensuring the connectivity:

SW1# Show etherchannel summary

```
SW1#show etherchannel summary
```

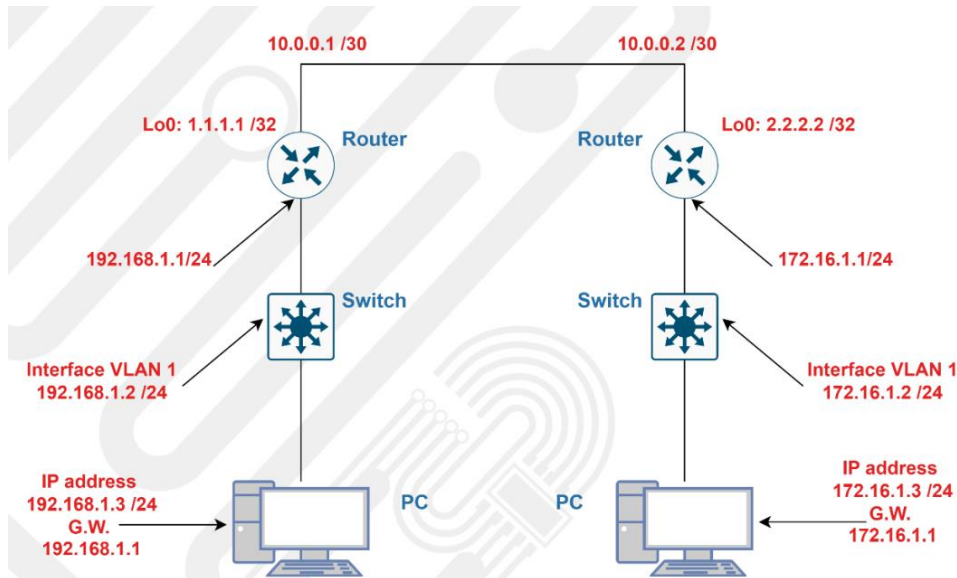
In the following output, we can see that the two ports are SU or State Up which means that our configuration was successful!

```
Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)        LACP        Gi3/0/3 (P) Gi3/0/4 (P)
2      Po2 (SU)        PAgP        Gi3/0/1 (P) Gi3/0/2 (P)
```

LAB 3: OSPF Configuration

In this scenario, we will configure OSPF on the router and introduce a loopback interface to demonstrate its use and importance in OSPF:



The configuration on the PCs giving the addressing from the cmd:

```
C:\Windows\system32>netsh interface ip set address name="ethernet 2" static 192.168.30.30 255.255.255.0 192.168.30.1

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8006:c8a5:4839:272e%10
    IPv4 Address. . . . . : 192.168.30.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.1
```

The configuration on the switches:

```
vlan 10
name IT
exit
vlan 20
name comm
exit
interface GigabitEthernet 0/1
switchport mode trunk
no ip address
no shutdown
interface GigabitEthernet 0/0
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
```

Then, you should configure the loopback interface:

```
Interface loopback 1
```

```
Ip address 100.1.1.1 255.255.255.255
```

```
Router(config)#interface loopback 1
```

```
Router(config-if)#ip add 200.1.1.1 255.255.255.255
```

After that, you should implement the OSPF on each router. For short, here is the OSPF configuration for router 1 and it will be similar to the other one:

```
Router ospf 1
```

```
Network 200.1.1.1 0.0.0.0 area 0
```

```
Network 10.1.1.0.0 0.0.0.3 area 0
```

```
Network 11.1.1.0.0 0.0.0.3 area 0
```

```
Router(config)#Router ospf 1
```

```
Router(config-router)#network 11.1.1.0 0.0.0.3 area 0
```

```
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
```

```
Router(config-router)#network 200.1.1.1 0.0.0.0 area 0
```

Finally, you should configure a command to let the internal router to send the packet to the main router if the destination is not in the internal network, which is the purpose of the following command: IP default-gateway 200.1.1.1

Pinging to ensure the connectivity:

```
Router(config)#do ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.40.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.40, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router(config)#
```

And pinging the loopback interface for checking up:

```
Router(config)#do ping 200.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router(config)#
```

Question and Answer (Q&A) Section based on the previous configurations:

LAB 1 Q&A:

- What steps did you take to ensure that VLAN 30 can communicate with other VLANs?
 1. Use the multilayer switch (to act as the gateway of the network)
 2. Assign an ip address and a subnet mask for each vlan on the multilayer switch
 3. Use the command “No shutdown” to make the vlans up state
 4. And finally, use the command “ip routing” to ensure that data can be transmitted between the different vlans on the network.

```
Switch(config)#ip routing
```

- Why is it important to keep the Management VLAN isolated, and how did you verify this in your configuration?

The management vlan is used for network administration tasks. Keeping it isolated ensures that unauthorized devices cannot access sensitive network management interfaces, which protects the network from threats.

I verified isolation by ensuring that the management vlan was not allowed on trunk links used by other vlans and that only authorized devices had access to this VLAN.

- If a ping from the HR PC to another VLAN fails, what troubleshooting steps would you take to identify and resolve the issue?
 1. Use the multilayer switch (to act as the gateway of the network)
 2. Assign an ip address and a subnet mask for each vlan on the multilayer switch
 3. Use the command “No shutdown” to make the vlans up state
 4. And finally, use the command “ip routing” to ensure that data can be transmitted between the different vlans on the network.

```
Switch(config)#ip routing
```

LAB 2 and LAB 3 Q&A:

- What would happen if the loopback interface was not advertised in OSPF?

The loopback interface wouldn't be reachable by other routers in the OSPF network, which could lead to routing issues or loss of communication with the router's services.
- Why is it important for the router's loopback interface to be stable and always up in OSPF?

The loopback interface is used as the router's ID in OSPF. It ensures consistent and stable routing, making the network more reliable.
- How can you troubleshoot if a device in one VLAN cannot reach the loopback interface?

Check the device's IP configuration, verify VLAN and trunk configurations, ensure OSPF is correctly configured, and make sure the loopback interface is advertised in OSPF.
- What benefits does OSPF provide in a network like this, compared to static routing?

OSPF automatically adjusts to changes in the network, finds the best paths, and scales better for larger networks, unlike static routing, which requires manual updates.