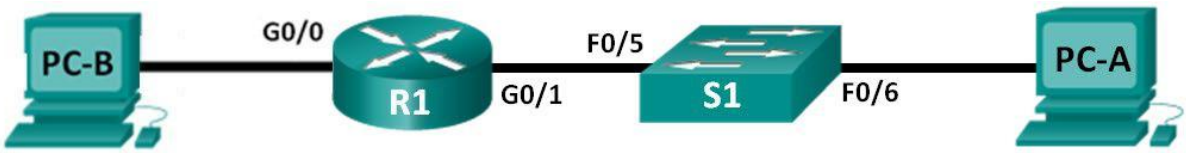
CCNA ITN Lab 2 **Instruction** **Deadline: 11.12.**

Name: Shabnaz Khanam

IPv4 Subnetting
Basic IPv4 and IPv6 LAN
Router and Switch Configuration
TFTP Server



NP Course NP Chapter 4-5

PrepExam: ITN Module Group Exams 8-10
ITN Module Group Exams 11-13

Tasks: Task 1 - Building a Switch and Router Network
Task 2 - IPv6 Addresses at Network Devices and Hosts
Task 3 - TFTP to Back Up and Restore a Running Configuration

Task 1 - Building a Switch and Router Network

Packet Tracer Topology

Part 1: Subnet Addressing

Available are the IP addresses of 192.168.0.0 / 24

PC-A LAN: There are 27 PCs in that LAN, the Router Interface shall get the last available IP address in its subnet, the switch shall get the second to the last available IP address in its subnet, and the Host Interface shall get the first available IP address in its subnet.

PC-B LAN : There are 17 PCs in that LAN, the Router Interface shall get the last available IP address in its subnet, and the Host shall get the first available IP address in its subnet.

Record the correct addresses and masks in the following table.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.0.1	255.255.255.0	N/A
S1	VLAN 1	192.168.0.2	255.255.255.0	
PC-A	NIC	192.168.0.3/27	255.255.255.224	192.168.0.1
PC-B	NIC	192.168.1.2/27	255.255.255.224	192.168.1.1

Part 2: Set Up Network Topology and Initialize Devices

Step 1: Build topology in Packet Tracer.

COVID-19 Version: Build topology in **Packet Tracer**. Use and re-label the following devices:

a. Build the network with ISR4321 router, 2960 switch, and 2 PCs in Packet Tracer. Rename the devices.

b. Cable the network according to the topology with straight-through TP cables .

c. Connect the rollover console cable from PC-A serial port RS-232 to switch S1 console port.

d. Connect the rollover console cable from PC-B serial port RS-232 to router R1 console port.

Part 3: Configure Switch via Console Cable

Step 1: Access Network Devices through the Serial Console Port

a. Use a **Terminal** from Desktop at PC-A to configure the switch S1. The default settings for the serial console port: **9600 baud, 8 data bits, no parity, 1 stop bit, no flow control**.

b. When you can see the switch terminal output `>switch`, you are ready to configure a Cisco switch. The following console example displays the terminal output of the switch while it is loading.

Important Note: In case you reload the device, **always bypass** the initial configuration dialog and **terminate** the autoinstall section.

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Step 2: Display the switch IOS image version.

a. While you are in the user EXEC mode, display the IOS version for your switch. The IOS operating system is a binary file (.bin) stored in the flash memory of your switch.
Note: You may use the question mark (**?**) to help with the correct sequence of parameters needed to execute commands, e.g. **`Switch>show ?`**

```
Switch> show version
```

Which IOS image version is currently in use by your switch?
Version 12.2(25r)FX

Step 3: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command (shortcut **en**).

```
Switch> enable
Switch#
```

Step 4: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode (shortcut **conf t**).

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

Step 5: Perform some basic Switch configurations

Provide hostname:	`S1(config)# hostname S1`
Prevent DNS domain lookup:	`S1(config)# no ip domain-lookup`
Use enable secret "**class**":	`S1(config)# enable secret class`
Create Motto-of-the-Day:	`S1(config)# banner motd # Enter TEXT message. End with the character '#', e.g. banner motd # Restricted Access. #`

Step 6: Enter local console password

To prevent unauthorized access to the switch, passwords must be configured. Privileged EXEC mode password is **class** (step 5), terminal login password is **cisco**.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
```

To leave your context type "**`exit`**" to move one step up or "**`end`**", which ends configuration mode.

Step 7: Save and display the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM) (shortcut **copy run start**).

```
S1# copy running-config startup-config

Destination filename [startup-config]? [Enter]
```

The **show running-config** command (shortcut **sh run**) displays the entire running configuration, one page at a time. Use the spacebar to advance paging. The commands configured in Steps 1 – 8 are highlighted below.

```
S1# show running-config
```

Check whether your local passwords stored in the running-config are encrypted or not? yes

Step 8: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command (shortcut **sh ip int br**). Press the spacebar to advance to the end of the list.

```
S1# show ip interface brief
```

How many switch interfaces (NIC) are built into your switch? fastEthernet/24

Step 9: Record the interface status for the following interfaces.

Interface	S1	
	Status	Protocol
F0/5	up	up
F0/6	down	down
VLAN 1	down	down

Remark:

The FastEthernet **port status** is up when cables have physical connectivity unless the ports were manually shutdown by the administrator.

The **protocol status** is up when the layer 2 protocol is working and peers are negotiating.

Note: VLAN 1 is a logical interface, used to address the switch. Only virtual switch interfaces might have an IP address and MAC address. Not set mac address:00D0.FF2D.A237

Step 10: Switch Virtual Interface

To make the switch reachable by its IP address, a virtual interface must be configured. We use VLA1 interface.

```
S1(config)# interface vlan1
S1(config-if)# ip address <your ip address> <your network mask>
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway <ip address of router R1 G0/0/1>
```

Part 4: Router Settings

Step 1: Run the following tasks and insert the necessary command

Access router R1 through the Serial Console Port and repeat the configuration known from switch S1.

- Enter the privileged EXEC mode enable
- Enter configuration mode config terminal
- Assign a device name **R1** to the router hostname R1
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names no ip domain-lookup
- Assign **class** as the privileged EXEC encrypted password enable secret class
- Assign **cisco** as the console password and enable login line console 0 #password cisco #login
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited

Banner motd #Restricted Access#

Step 2: Assign cisco as the Telnet (VTY) password and enable login

Configure inband access by Telnet for 5 vty lines 0-4

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

Step 3: Encrypt the clear text passwords in the configuration file

```
R1(config)# service password-encryption
```

Step 4: Configure and activate router interfaces

Do not forget to configure an interface description for each interface indicating network is connected.

Note: While switch interfaces are powered-on when they are physically connected, router interfaces must be switched on actively.

```
R1(config)# int g0/0/0
R1(config-if)# description Connection to PC -B (LAN B)
R1(config-if)# ip address <your ip address> <your
mask> R1(config-if)# no shut
R1(config-if)# int g0/0/1
            <continue for g0/0/1>
```

Step 5: Save the running configuration to the startup configuration file

The running-configuration is held in the DRAM of a network device, but for save operation it should be saved to the startup-configuration in the non-volatile RAM, from where is restored during warm start or cold start.

```
R1(config)# copy running-config startup-
          config (shortcut: copy run start)
```

Step 6: Test Connectivity

Assign static IP address, network mask and default gateway to the PC interfaces using **IP Configuration** of the **PC Desktop**. **Note**: Adjust configurations until all ping works.

From PC-A ping switch S1. Successful (y/n) yes

Test PC-A to PC-B connectivity by ping. Successful (y/n) yes

Part 5: Device Information

Step 1: Retrieve hardware and software information from router R1

1. Record the version of the IOS image that the router is running – `version 03.16.05`
2. Record the size of NVRAM (non-volatile RAM) memory. 689 byte(237588 bytes free)
3. Record the size of local Flash memory.

3.17338e+06K bytes of processor board System flash (Read/Write)

Step 2: Use show ip route to answer the following questions.

1. What code is used in the routing table to indicate a directly connected network? Code 'C'
2. How many networks are directly connected to the router?

2

Step 3: **Use** show interface g0/0/1 **to answer the following questions.**

1. Record the operational status of the G0/0/1 interface. up
2. Record the Media Access Control (MAC) address of the G0/0/1 interface.

00E0.F7C0.2502

Step 4: **Use the <u>most useful</u>** show ip interface brief **command to display the status of each interface.**

1. If the G0/0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

#Int g0/0/1
ip address 192.168.0.3 255.255.255.252

Task 2 - IPv6 Addresses at Network Devices and Hosts

Packet Tracer Topology

Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0/0	2001:DB8:ACAD:A::1	64	N/A
	G0/0/1	2001:DB8:ACAD:1::1	64	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	2001:DB8:ACAD:1::ff	64	FE80::1
PC-B	NIC	SLAAC		SLAAC

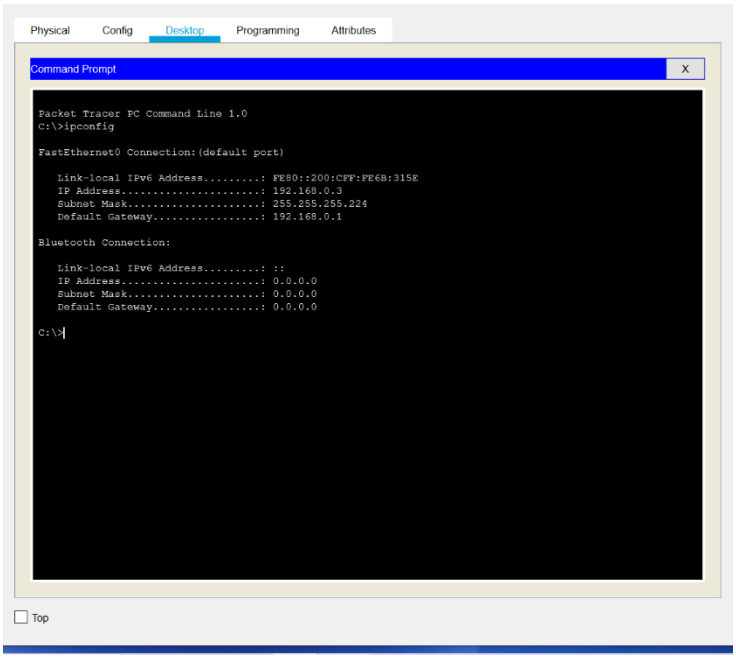
Use the topology of the previous lab and configure and inspect IPv6 addresses and IPv6 routing.

Part 6: Configure IPv6 Addresses

Step 1: Enable IPv6 addresses of PC-A and PC-B.

a. For PC-A, configure IPv6 global unicast address and the same host address for link local IPv6.

b. On a PC-A **command prompt**, enter the **ipconfig** command to examine IPv6 address information. Record the displayed IPv6 link local address: FE80::200:CFF:FE6B:315E

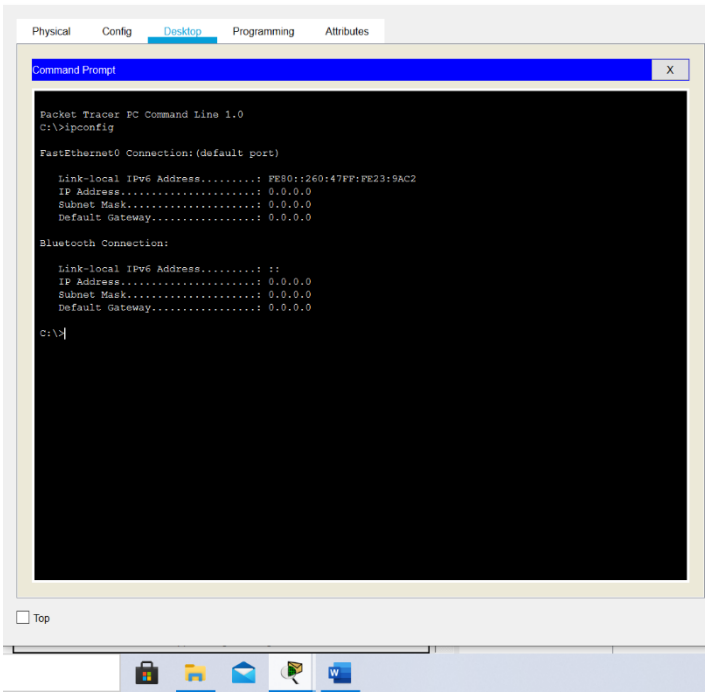


c. For PC-B, configure **automatic IPv6 configuration** (SLAAC).

d. On a PC-B **command prompt**, enter the **ipconfig** command to examine IPv6 address information.

Record the displayed IPv6 link local address: FE80::260:47FF:FE23:9AC2

Record the displayed IPv6 global unicast address: ::



Step 2: IPv6 addresses and IPv6 routing at router R1

a. Assign the IPv6 global unicast addresses, listed in the Addressing Table, to Ethernet interfaces on R1.

```
R1(config)# interface g0/0/0
R1(config-if)# ipv6 address
2001:db8:acad:a::1/64 R1(config-if)# no shutdown
R1(config-if)# interface g0/0/1 R1(config-if)#
ipv6 address 2001:db8:acad:1::1/64 R1(config-
if)# no shutdown
```

b. Issue the **show ipv6 interface brief** command to verify that the correct IPv6 unicast address is assigned to each interface.

Record g0/0/1 status and link local address.

Up/up ipv6 address 2001:db8:acad:a::1/64

c. Issue the **show ipv6 interface g0/0/0** command.

Note: Notice that the interface is listing two Solicited Nodes multicast groups, because the IPv6 link-local (FE80) Interface ID was not manually configured to match the IPv6 unicast Interface ID.

The link-local address displayed is based on EUI-64 addressing, which automatically uses the interface Media Access Control (MAC) address to create a 128-bit IPv6 link-local address.

Record R1 g0/0/0 link local address:

FE80::2E0:F7FF:FEC0:2501

g0/0/0 global unicast address:

2001:db8:acad:a::1/64

d. To get the link-local address to match the unicast address on the interface, manually enter the link-local addresses on each of the Ethernet interfaces on R1.

```
R1(config)# interface g0/0/0
R1(config-if)# ipv6 address fe80::1 link-
local
 R1(config-if)# interface g0/0/1
 R1(config-if)# ipv6 address fe80::1 link-
local
```

Note: Each router interface belongs to a separate network. Packets with a link-local address never leave the local network; therefore, you can use the same link-local address on both interfaces.

e. Re-issue the **show ipv6 interface g0/0/0** command.

Record the new g0/0/0 link local address: FE80::1

Record the g0/0/0 multicast group addresses: FF02::1
FF02::1:FF00:1

f. IPv6 routing must be enabled explicitly using the **IPv6 unicast-routing** command.

```
R1(config)# ipv6 unicast-
routing R1(config)# exit
```

Re-check IPv6 on interface g0/0/0 with the **show ipv6 interface g0/0**

command. Did the multicast group addresses change?yes

For which purpose do we need the FF02::2 multicast group. To access all the router in the net

g. Now that R1 is part of the all-router multicast group, re-issue the **ipconfig** command on PC-B. Examine the IPv6 address information.

Has an IPv6 unicast address been assigned to NIC on PC-B?yes

Why did PC-B receive the Global Routing Prefix and Subnet ID that you configured on R1? Cz pc B default gatway and router ip address are same

Part 7: Verify End-to-End Connectivity

a. From PC-A, **ping FE80::1**. This is the link-local address assigned to G0/0/1 on R1. Successful?yes

Note: You can also test connectivity by using the global unicast address, instead of the link-local address.

b. Use the **tracert** command on PC-B to verify that you have end-to-end connectivity to PC-A.

The IP addresses of which interfaces are given back by tracert?

Reflection

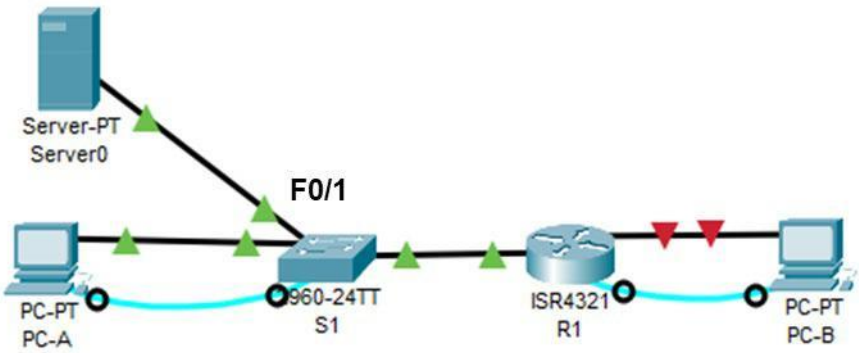
Why can the same link-local address, FE80::1, be assigned to both Ethernet interfaces on R1?
Packet of link-local address never leave the network

What is the Subnet ID of the IPv6 unicast address 2001:db8:acad:ab01::aaaa:1234/64?

Ab01

Task 3 - TFTP to Back Up and Restore a Running Configuration

Packet Tracer Topology



Part 1: Save and Restore Running Configuration with TFTP Server

Step 1: Extend Topology by TFTP Server

The TFTP application uses the UDP Layer 4 transport protocol, which is encapsulated in an IP packet. For TFTP file transfers to function, there must be Layer 1 and 2 (Ethernet, in this case) and Layer 3 (IP) connectivity between the TFTP client and the TFTP server.

a. Configure IPv4 connectivity for TFTP Server.

Select the **second** available IP address in its subnet and configure IP address of TFTP Server at **Desktop ➔ IP Configuration**.

Record TFTP Server IP Address and Subnetz Mask: 192.168.0.4 255.255.255.224

Step 2: Copy command on a Cisco device.

a. Clean TFTP configuration, if necessary

Some routers have preconfigured TFTP server interfaces.

```
R1# no ip tftp source-interface GigabitEthernet0
```

b. Enter **copy ?** to display the options for source or "from" location and other available copy options. You can specify **flash:** or **flash0:** as the source, however, if you simply provide a filename as the source, **flash0:** is assumed and is the default.

```
R1# copy ?
```

Which copy command uses the flash folder as a source?

Copy tftp:

Which copy command saves the running-config? Copy running-config

c. Use the **?** to display the destination options after a source file location is chosen. The **flash:** file system for R1 is the source file system.

```
R1# copy flash: ?
```

Which copy command uses the TFTP Server as a destination?
Copy flash: tftp:

d. From the privileged EXEC mode on the router, enter the copy command and provide the remote host address of the TFTP server.

```
R1# copy running-config tftp:
```

Note: Other issues, such as a firewall blocking TFTP traffic, can prevent the TFTP transfer. Please check with your instructor for further assistance.

e. Verify on TFTP Server, if the file has been transferred. File name at TFTP Server: file system

Step 3: Restore the running configuration file to the router.

a. Erase the startup-config file on the router.
```
R1# erase startup-config
```

b. Reload the router and do **NOT** save the running config.
```
R1# reload
System configuration has been modified. Save? [yes/no]:n
```

c. Configure the G0/0/1 interface on the router with an IP address 192.168.0.30 /27 and switch on the interface.

d. Verify connectivity between the router and TFTP Server.

e. Use the **copy** command to transfer the running-config file from the TFTP server to the router. Use **running-config** as the destination.

f. Verify the router has updated by displaying the running-configuration.

Checkout

When you successfully finished this Lab, record your solution.

Create a PDF file **ITN-Lab2-Result.pdf**, which includes these instructions completed by your answers.

Save your Packet Tracer file **ITN-Lab2-PT.pkt** and record the running configuration of router R1 (**show run**) as pdf file **ITN-Lab2-R1.pdf**.

Upload these 3 files in Ilias.