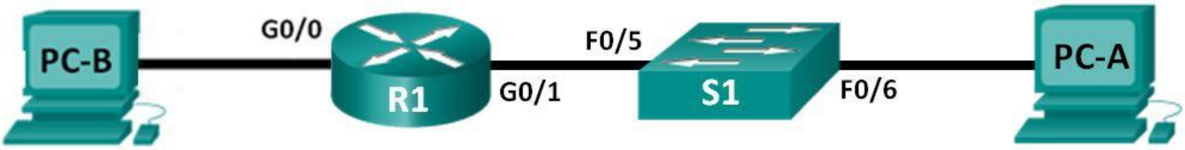
**CCNA** **ITN Lab 2**

**Names:** : **Sanjida Shamin, Febin Chollapra, Rubaiya Kabir Pranti**

**Team-No.:04**

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



## Lab Preparations

ITN Assessments: Modules 4-7: Ethernet Concepts Exam (partly Refresher)
Modules 8-10: Communicating Between Networks Exam
Modules 11 - 13: IP Addressing Exam

NP Course: NP Chapter 3-5

Cisco IOS Commands

IPv4 Subnetting

IPv6 Addressing

## Lab Instructions

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

## Deliverables and List of Due Dates

# Preparation

## Part 1: Cisco IOS Basic Configuration Commands

a. Read the Lab Instructions of this Lab

b. Check the IOS Command List, provided for the Labs.

c. Which IOS commands are necessary to configure the following tasks?

- Enter the privileged mode from startup mode. **Router> - enable**
- Enter the configuration (EXEC) mode from terminal. **Router# configure terminal**
- Set the hostname to R1. **Router(config)# hostname R1**
- Disable DNS lookup. **R1(config)# no ip domain-lookup**
- Assign **class** the EXEC encrypted password **R1(config)# enable secret class**
- Configure global password encryption. **R1(config)# service-password encryption**
- Return from configuration (EXEC) mode: **R1(config)# exit**
- Assign **cisco** the console password and enforce login and set **logging synchronous** to prevent console messages from interrupting command entry.

```
R1(config)#  line con 0

R1(config-line)#  password cisco

R1(config-line)#  login

R1(config-line)#  logging synchronous

R1(config-line)#exit
```

- Use vty (Telnet) lines 0-4, assign **cisco** as the vty (Telnet) password and enforce login.

```
R1(config)#  line vty 0 4

R1(config-line)#  password cisco

R1(config-line)# login

R1(config-line)# exit
```

- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd $ unauthorized access prohibited ! $
```

- Save the running configuration to the startup configuration file.

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

- Display the **running configuration**. **R1(config)#** - **show running config/sh run**

Display the status of all **interfaces** in brief. **R1(config)# show ip interface brief/sh ip int br**

## Part 2: Calculate IPv4 Subnets

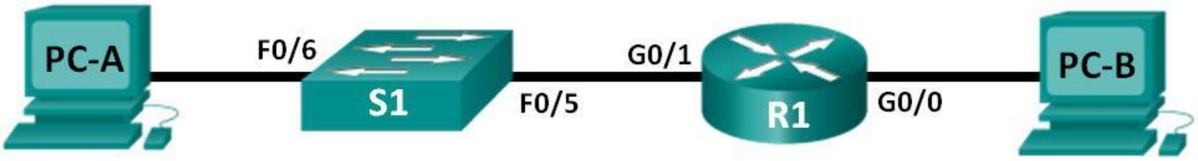
### Step 1: Network Topology A

Given is the following network topology.

PC-A is in subnet A with **208 hosts** in total.

PC-B is in subnet B with **98 hosts** in total.

Calculate the appropriate minimum sized subnets.



a. How many IP subnets are given in the topology in total? **two**

b. Which subnet mask is used in network A? **/24 or 255.255.255.0**

c. Which subnet mask is used in network B? **/25 or 255.255.255.128**

Plan the subnets with private IP addresses in the **IP address range of 192.168.0.0 / 16**. Design your subnet addressing scheme (decimal) starting with network A. The network addresses shall be consecutive without any gap in the used address space.

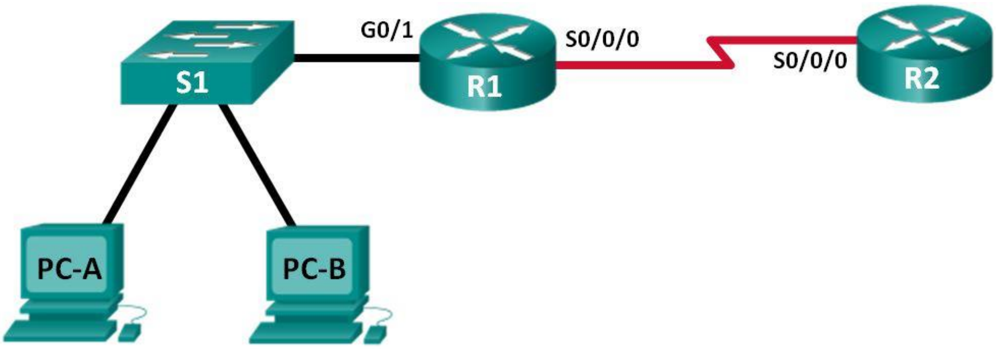
| Subnet Number | Subnet IP Address | First Usable Host IP Address | Last Usable Host IP Address | Broadcast IPAddress |
|---|---|---|---|---|
| 1 | 192.168.0.0 | 192.168.0.1 | 192.168.0.254 | 192.168.0.255 |
| 2 | 192.168.1.0 | 192.168.1.1 | 192.168.1.126 | 192.168.1.127 |
| | | | | |
| | | | | |

### Step 2: Network Topology B

Given is the following network topology. You have been given the private IP address space **172.16.0.0/24**.

PC-A and PC-B are in a subnet with **48 hosts**.

The subnet between the router R1 and R2 has **no additional hosts**.



Plan your subnets with the following rules:

- Subnets shall have a minimum size needed to support all IP addresses in that subnet

- Subnets shall be planned form the largest to the smallest one
- Subnet addresses shall be consecutive without any address space gap

a. How many IP subnets are in the topology in total? **2**

b. How many "0" bits in the subnet mask are needed for the largest subnet? **6**

c. Which subnet mask is used in the largest subnet (decimal)? **255.255.255.192**

d. How many "0" bits in the subnet mask are needed for the second largest subnet? **2**

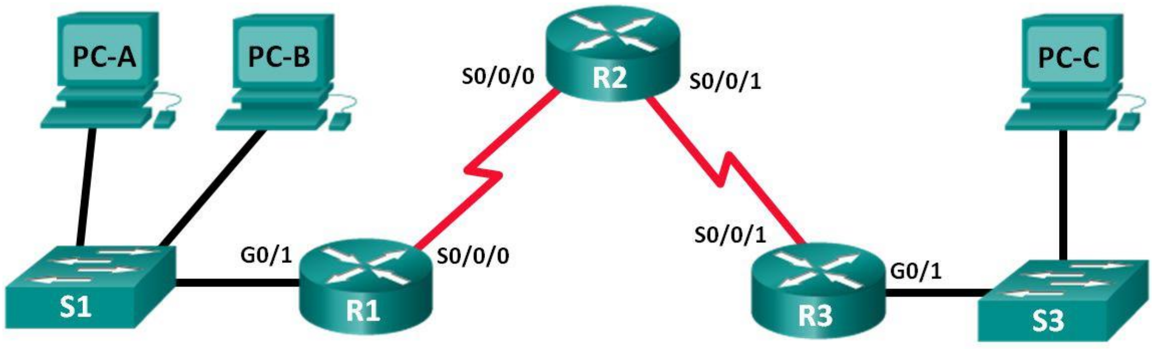
e. Which subnet mask is used in that subnet (decimal)? **255.255.255.252**

Design your subnet addressing scheme (decimal).

| Subnet Number | Subnet IP Address | First Usable Host IP Address | Last Usable Host IP Address | Broadcast IP Address |
|---|---|---|---|---|
| 1 | 172.1.0.0 | 172.16.0.1 | 172.16.0.62 | 172.16.0.63 |
| 2 | 172.16.0.64 | 172.16.0.65 | 172.16.0.66 | 172.16.0.67 |
| | | | | |
| | | | | |

### Step 3: Network Topology C

The network topology C is illustrated in the following topology. Use the **192.168.10.0/24** network address range to provide addresses to the network devices, and then design a new addressing scheme to support the additional network requirement.



a. How many IP subnets are in the topology in total? **4**

b. In the following table you find the number of host IP addresses per subnet.

| Subnet | Number of hosts | Number of router IPs | Subnet mask | Maximum hosts IP addresses |
|---|---|---|---|---|
| Subnet PC-A, PC-B | 101 | **1** | **255.255.255.128** | **125** |
| Subnet PC-C | 42 | **1** | **255.255.255.192** | **61** |
| Subnet R1-R2 | 0 | **2** | **255.255.255.252** | **0** |
| Subnet R2-R3 | 0 | **2** | **255.255.255.252** | **0** |

c. Plan your subnets according to the following rules:

- Subnets shall have a minimum size needed to support all IP addresses in that subnet
- Subnets shall be planned form the largest to the smallest one
- Subnet addresses shall be consecutive without any address space gap

Fill the following table with the subnet information:

| Subnet Number | Subnet IP Address | First Usable Host IP Address | Last Usable Host IP Address | Broadcast IP Address |
|---|---|---|---|---|
| **1** | **192.168.10.0** | **192.168.10.1** | **192.168.10.128** | **192.168.10.127** |
| **2** | **192.168.10.128** | **192.168.10.129** | **102.168.10.190** | **192.168.10.191** |
| **3** | **192.168.10.192** | **192.168.10.193** | **192.168.10.194** | **192.168.10.195** |
| **4** | **192.168.10.196** | **192.168.10.197** | **192.168.10.198** | **192.168.10.199** |

How many IP addresses from the given IP address range 192.168.10.0/24 have not been assigned to any subnet? **56**

## Part 3: IPv6 Addressing

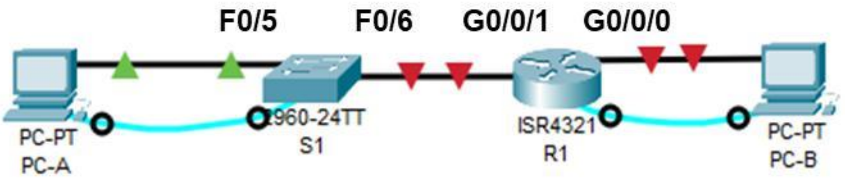
a. Which 2 types of IPv6 addresses must be configured on an IPv6 interface?

b. Given is the IPv6 global prefix **2001:638:402:1303 / 64** and the IPv6 host address **::100 / 64** Create the global unicast IPv6 address and the link-local unicast IPv6 address for that interface:

Global unicast: **2001:638:402:1303::100 /64**
Link-local unicast: **FE80::100**

# 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 | **192.168.0.62** | **255.255.255.224** | N/A |
|  | G0/0/1 | **192.168.0.30** | **255.255.255.224** | N/A |
| S1 | VLAN 1 | **192.168.0.29** | **255.255.255.224** | **192.168.0.30** |
| PC-A | NIC | **192.168.0.1** | **255.255.255.224** | **192.168.0.30** |
| PC-B | NIC | **192.168.0.33** | **255.255.255.224** | **192.168.0.62** |

## Part 2: Set Up Network Topology

### 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.

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?
**Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)**

## 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 '#',`<br>`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?

**Answer: The privileged EXEC mode password is shown as encrypted as shown below-**
**enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1**
**But the console password is not encrypted. It is in plain text.**

### 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?

**Answer: in total 26 interfaces (24 FastEthernet, 2 GigabitEthernet)**

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

| | S1 | |
|---|---|---|
| **Interface** | **Status** | **Protocol** |
| F0/5 | **YES manual up** | **up** |
| F0/6 | **YES manual down** | **down** |
| VLAN 1 | **administratively 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.

### 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
- Enter configuration mode
- Assign a device name **R1** to the router
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names
- Assign **class** as the privileged EXEC encrypted password
- Assign **cisco** as the console password and enable login
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited

### 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**

(**Note:** Adjust configuration errors until these tests are working.)

## 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
   **Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)**
2. Record the size of NVRAM (non-volatile RAM) memory.
   **32768K bytes of non-volatile configuration memory.**
3. Record the size of local Flash memory
   **3223551K bytes of flash memory at bootflash:**

### 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?
   **CLCL is observed which denotes L-Local and C-Connected**
   **C expresses g0/0/0 and g0/0/1 interfaces are directly connected.**
2. How many networks are directly connected to the router?
   **In total, two networks or two subnets are connected to the two interfaces of router.**

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

1. Record the operational status of the G0/0/1 interface.
   **GigabitEthernet0/0/1 is up, line protocol is up (connected)**
2. Record the Media Access Control (MAC) address of the G0/0/1 interface.
   **MAC address of G0/0/1 interface: Hardware is Lance, address is 0050.0f48.7302 (bia 0050.0f48.7302)**

### Step 4: Use the most useful show ip interface brief command to display the status of each interface.

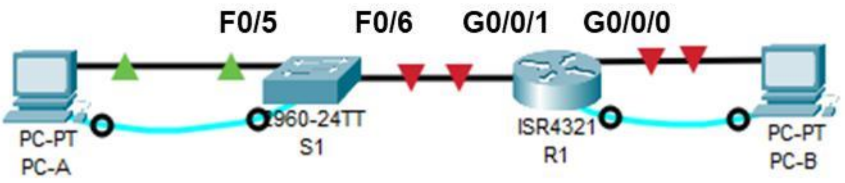
1. If the G0/0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

```
R1#show ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.0.62 YES manual up up
GigabitEthernet0/0/1 192.168.0.30 YES manual up up
Vlan1 unassigned YES unset administratively down down
```

   **GigabitEthernet0/0/1 is already up manually.**
   **If it was administratively down, the I will use no shutdown command to turn the interface(G0/0/01 interface).**

# 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 1: 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::20C:CFFF:FE8A:9C30**

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::201:97FF:FE51:877B**

Record the displayed IPv6 global unicast address: **:: (It is not assigned yet.)**

### 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** to verify the correct IPv6 unicast address of each

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

**link local address of g0/0/01: FE80::250:FFF:FE48:7302**

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::250:FFF:FE48:7301**

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:
**all-nodes multicast group- FF02::1 and**
**Solicited nodes multicast group- 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
```

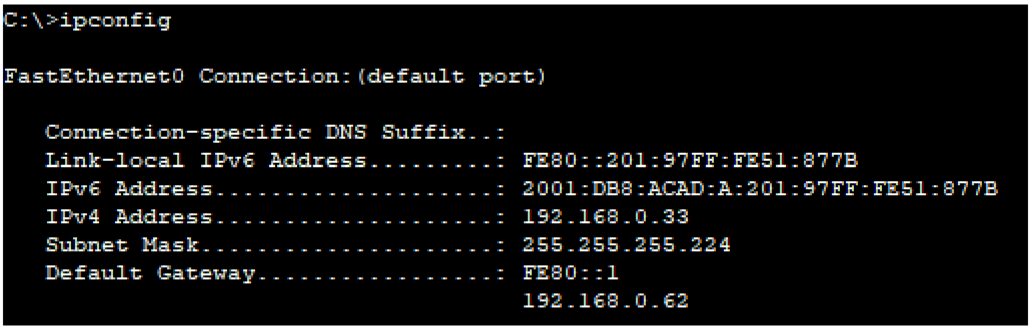
Re-check IPv6 on interface g0/0/0 with the **show ipv6 interface g0/0/0** command.

Did the multicast group addresses change?

**Yes. A new FF02::2 multicast group address has been added with old ones.**

For which purpose do we need the FF02::2 multicast group.
**We need the FF02::2 multicast group for getting the layer 2 data link-layer addresses of other nodesin Neighbor Discovery Protocol.**

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.



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:97FF:FE51:877B
   IPv6 Address....................: 2001:DB8:ACAD:A:201:97FF:FE51:877B
   IPv4 Address....................: 192.168.0.33
   Subnet Mask.....................: 255.255.255.224
   Default Gateway.................: FE80::1
                                     192.168.0.62
```

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

**Yes. IPv6 address** 2001:DB8:ACAD:A:201:97FF:FE51:877B **and default gateway** FE80::1 **has been added.**

Why did PC-B receive the Global Routing Prefix and Subnet ID that you configured on R1?

**With the help of FF02::2 all-nodes multicast group, now the IPv6 interfaces on R1 become the part of FF02::2. This multicast group permits the router to send information to every node in the LAN. That iswhy R1 send Global Routing Prefix and Subnet ID to all nodes. Thus, R1 sends fe80::1, default gateway address to PC-B as it is observed. Previously the IPv6 global unicast address through SLAAC and default gateway on PC-B were not visible in command prompt**. **Now device such as PC-B has received its IPv6 address and default gateway through SLAAC.**

## Part 2: Verify End-to-End Connectivity

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.

a. 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?

**The IPv6 address of g0/0/0 interface and IPv6 address of PC-A are given back.**

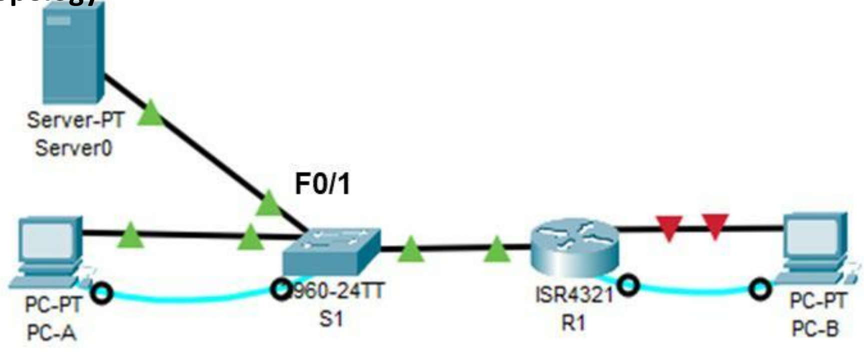
## Reflection

Why can the same link-local address, FE80::1, be assigned to both Ethernet interfaces on R1?

**Each router interface belongs to a separate network. Packets with a link-local address never leave the localnetwork. Therefore, same link-local address can be used on both interfaces g0/0/0 and g0/0/1.(from note)**

# 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**. **Second available IP: 192.168.0.2 from first table**

Record TFTP Server IP Address and Subnetz Mask:
**Second available IP: 192.168.0.2**
**Subnet mask: 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?

**flash:**

**(copy flash:  command)**

Which copy command saves the running-config?

**running-config**

**(copy running-config command)**

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?

**tftp: command**
**(copy flash: tftp: command)**

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.

e. Verify on TFTP Server, if the file has been transferred. File name at TFTP Server:
**Yes .File name is named as R1-confg.**

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

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

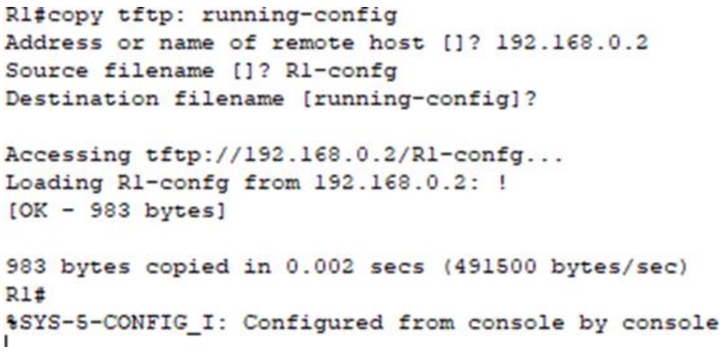
Reload the router and do NOT save the running config.
R1# reload

System configuration has been modified. Save? [yes/no]:n

Configure the G0/0/1 interface on the router with an IP address 192.168.0.30 /27 and switch on the interface. **After erasing and reloading, configuration on router with interface G0/0/1 is done.**

Verify connectivity between the router and TFTP Server**. As seen, connection has been established again after configuration between the router and TFTP Server.**
**By pinging g0/0/1 interface address from server side, it was successful.**

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



```
R1#copy tftp: running-config
Address or name of remote host []? 192.168.0.2
Source filename []? R1-confg
Destination filename [running-config]?

Accessing tftp://192.168.0.2/R1-confg...
Loading R1-confg from 192.168.0.2: !
[OK - 983 bytes]

983 bytes copied in 0.002 secs (491500 bytes/sec)
R1#
%SYS-5-CONFIG_I: Configured from console by console
!
```

Verify the router has updated by displaying the running-configuration.**Yes, after erasing and again copying from server, the running-configuration is showing as before.**

# Deliverables

## Lab Teams

This lab may be solved in teams of max. 3 students. All teams have to upload their deliverables in time.

Teams are grouped into 2 groups, which have different due dates and presentation dates.

## Module Group Exams

Each team member must solve the requested **Module Group Exams** before delivery date.

## Deliverables

Each teams uploads the following files:

- Create a PDF file One **PDF-File (.pdf)** with the completed and answered **Lab Preparations and Lab Instructions**. All tasks must be worked on and all questions must be answered.
- Save your **Packet Tracer file ITN-Lab2.pkt**
- Record the running configuration of router R1 (show run) in a text file **ITN-Lab2-R1.txt**.

## Due Dates

| Group 1 | Teams 1-10 | Due Date |
|---|---|---|
| | Module Group Exams 4-7, 8-10, 11-13 | 8.11. - EOB |
| | Upload Deliverables | 8.11. - EOB |
| | CCNA ZOOM Presentation | 10.11. - 16:45 ff. |

| Group 2 | Teams 11-20 | Due Date |
|---|---|---|
| | Module Group Exams 4-7, 8-10, 11-13 | 15.11. - EOB |
| | Upload Deliverables | 15.11. - EOB |
| | CCNA ZOOM Presentation | 17.11. - 16:45 ff. |

- Per team you load one solution in Ilias in time.
- Per team you book one timeslot for acceptance.