CCNA ITN Lab 2 **Instruction** **Deadline: 11.12.2020**

Name: Rubaiya Kabir Pranti

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

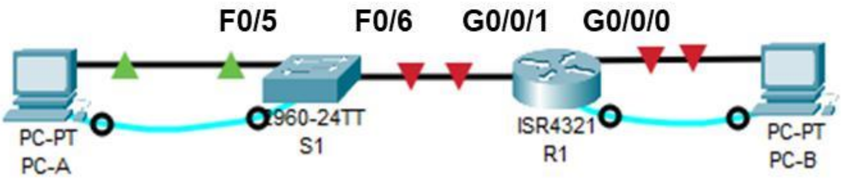
NP Course **NP Chapter 4-5**

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	192.168.0.62	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 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? **12.2**

```
Switch   Ports  Model            SW Version       SW Image
------   -----  -----            ----------       ----------
*    1   26     WS-C2960-24TT    12.2             C2960-LANBASE-M
```

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?

Answer: **The privileged EXEC mode password is shown as encrypted as shown below-**

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
```

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? **27**

(including 24 Fast Ethernet interfaces, 2 Gigabit Ethernet interfaces and one VLAN interface.)

Step 9:

Record the interface status for the following interfaces.

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.

For switch 1 (S1):

Interface	Status	Protocol
F0/5	YES manual up	yes
F0/6	YES manual down	down
VLAN 1	YES manual administratively down	down

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>
```

After above command:

```
Vlan1                  192.168.0.29     YES manual up                    up
S1#
```

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

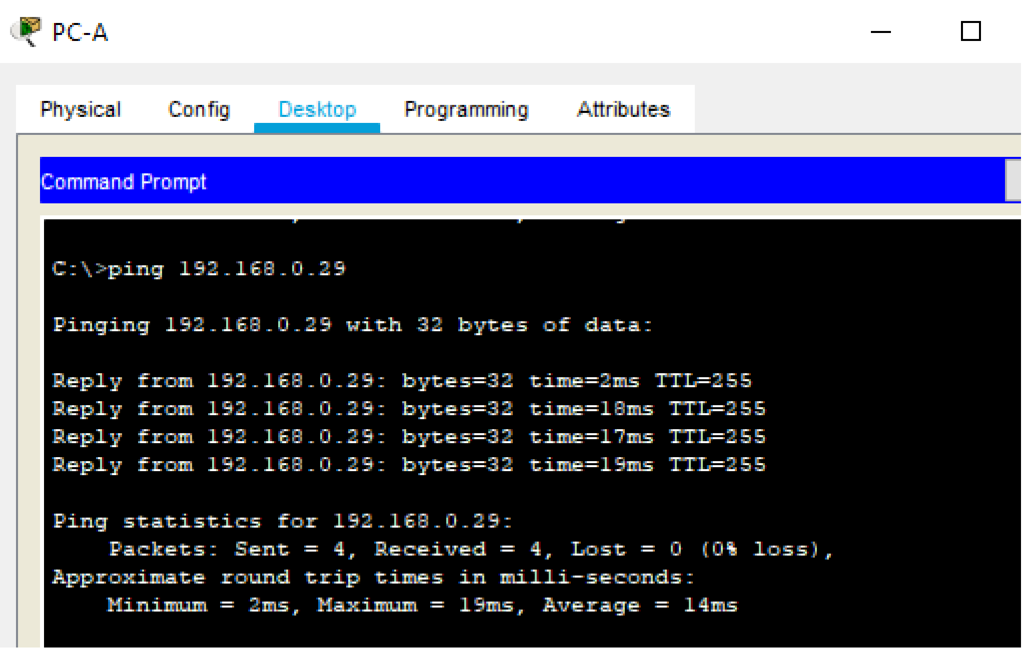
The running-configuration is held in the DRAM of a network device, but for save operation it should be saved to the startup-configuration in the non-volatile RAM, from where is restored during warm start or cold start.

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

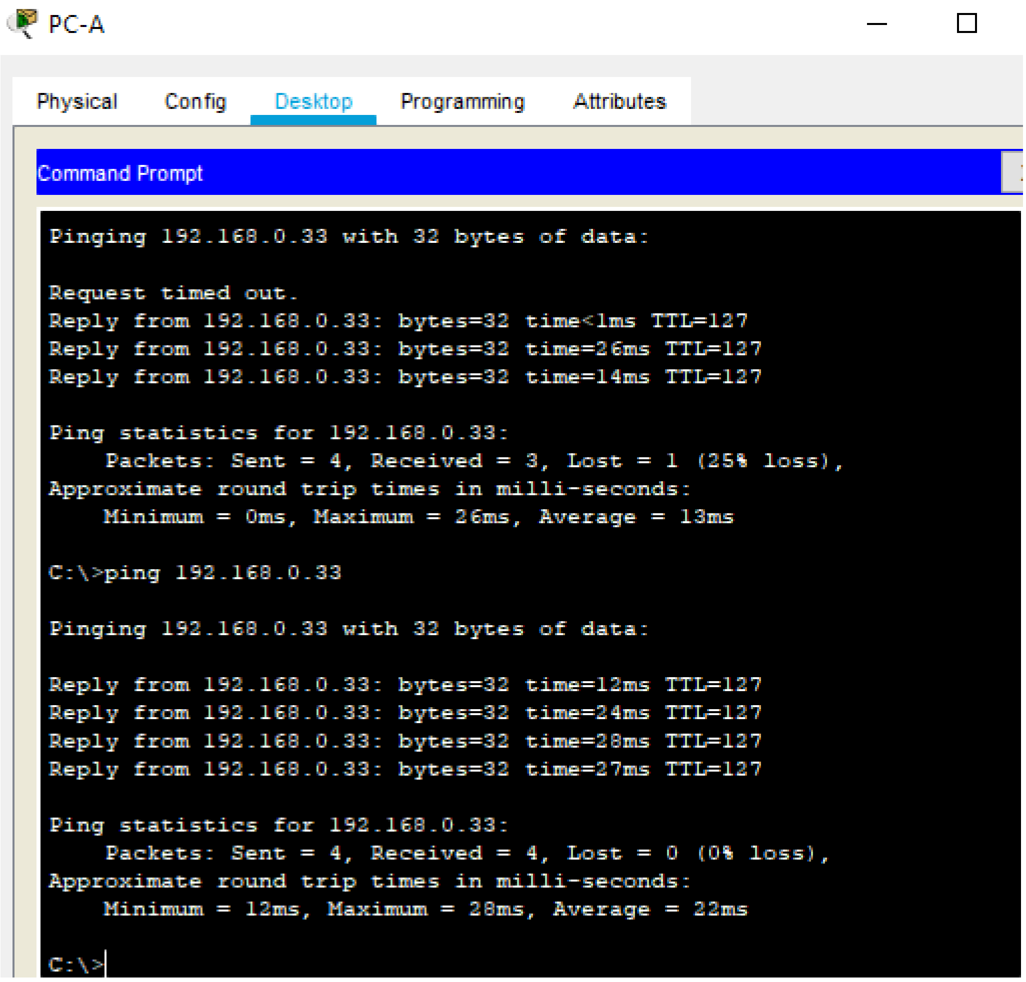
Step 6: Test Connectivity

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**



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 15.5**

```
R1#show version
Cisco IOS XE Software, Version 03.16.05.S - Extended Support Release
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**

```
cisco ISR4321/K9 (1RU) processor with 1687137K/6147K bytes of memory.
Processor board ID FLM2041W2HD
2 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.
```

3. Record the size of local Flash memory. **3223551K bytes**

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

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.0.0/27 is directly connected, GigabitEthernet0/0/1
L       192.168.0.30/32 is directly connected, GigabitEthernet0/0/1
C       192.168.0.32/27 is directly connected, GigabitEthernet0/0/0
L       192.168.0.62/32 is directly connected, GigabitEthernet0/0/0
```

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.

```
R1#show interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0050.0f68.b702 (bia 0050.0f68.b702)
  Description: Connected to S1
  Internet address is 192.168.0.30/27
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is RJ45
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     16 packets input, 2048 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     15 packets output, 1920 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

2. Record the Media Access Control (MAC) address of the G0/0/1 interface.
   MAC address of G0/0/1 interface: 0050. 0f68. b702

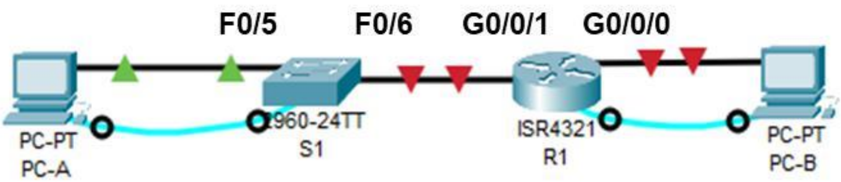
Step 4: Use the most useful show ip interface brief command to display the status of each interface.

1. If the G0/0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up? **No it is already up.**
   If it was seen administratively down, the I would use "no shutdown" command after IP addressing of G0/0/01 interface.

```
R1#sh 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
R1#
```

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

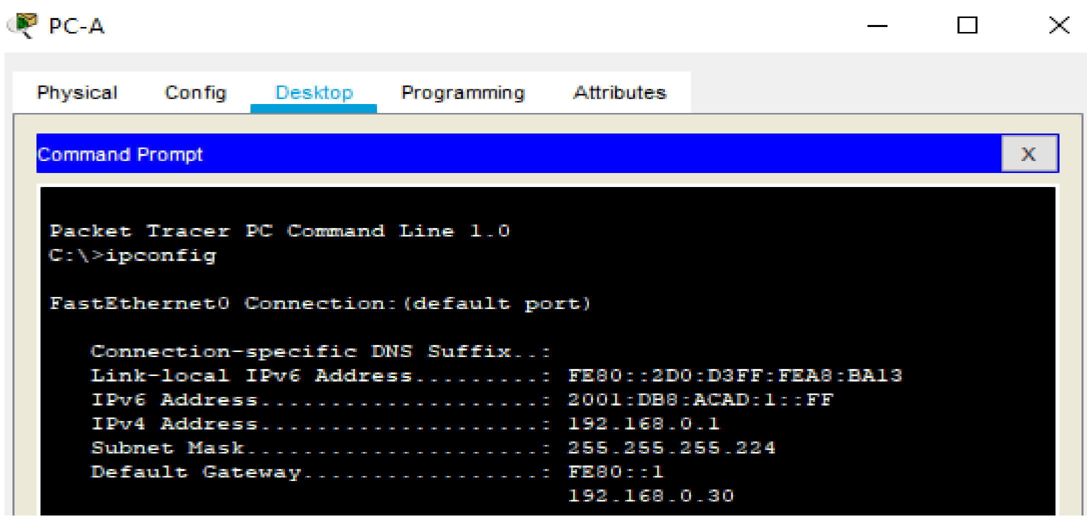
Use the topology of the previous lab and configure and inspect IPv6 addresses and IPv6 routing.

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::2D0:D3FF:FEA8:BA13**

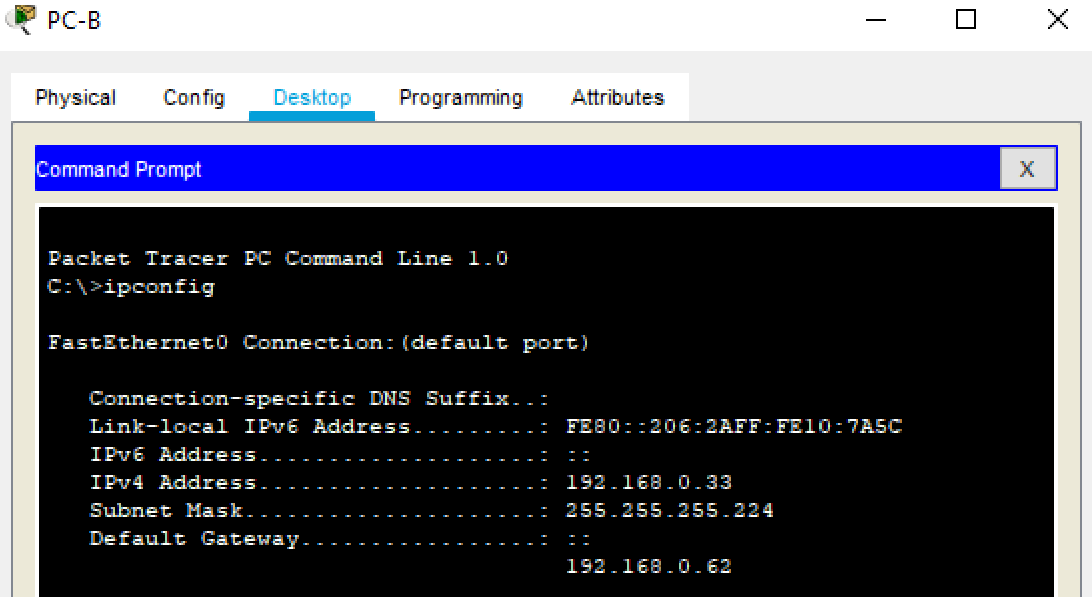


c. For PC-B, configure **automatic IPv6 configuration** (SLAAC).

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

Record the displayed IPv6 link local address: **FE80::206:2AFF:FE10:7A5C**

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** command to verify that the correct IPv6 unicast address is assigned to each interface.

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

Status is up

link local address of g0/0/01: FE80::250: FFF: FE68: B702

```
R1#sh ipv6 int br
GigabitEthernet0/0/0       [up/up]
    FE80::250:FFF:FE68:B701
    2001:DB8:ACAD:A::1
GigabitEthernet0/0/1       [up/up]
    FE80::250:FFF:FE68:B702
    2001:DB8:ACAD:1::1
Vlan1                      [administratively down/down]
    unassigned
```

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:FE68: B701

Record R1 g0/0/0 global unicast address:

2001:DB8:ACAD:A::1

```
R1#sh ipv6 int g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::250:FFF:FE68:B701
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF68:B701
```

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:
1. all-nodes multicast group- FF02::1 and
2. Solicited nodes multicast group- FF02::1: FF00:1

```
R1#sh ipv6 int g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    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.**

New FF02::2 multicast group address shows up with past ones.

```
R1#sh ipv6 int g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
```

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 nodes in 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.
Yes. IPv6 address and default gateway has been added.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::206:2AFF:FE10:7A5C
   IPv6 Address....................: 2001:DB8:ACAD:A:
206:2AFF:FE10:7A5C
   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? **No.**

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 is why 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 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

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:

Reply from FE80::1: bytes=32 time=25ms TTL=255
Reply from FE80::1: bytes=32 time=24ms TTL=255
Reply from FE80::1: bytes=32 time=21ms TTL=255
Reply from FE80::1: bytes=32 time=18ms TTL=255

Ping statistics for FE80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 25ms, Average = 22ms
```

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?

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

```
C:\>tracert 2001:db8:acad:1::ff

Tracing route to 2001:db8:acad:1::ff over a maximum of 30 hops:

  1   2 ms      14 ms     16 ms     2001:DB8:ACAD:A::1
  2   21 ms     20 ms     22 ms     2001:DB8:ACAD:1::FF

Trace complete.
```

Reflection

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

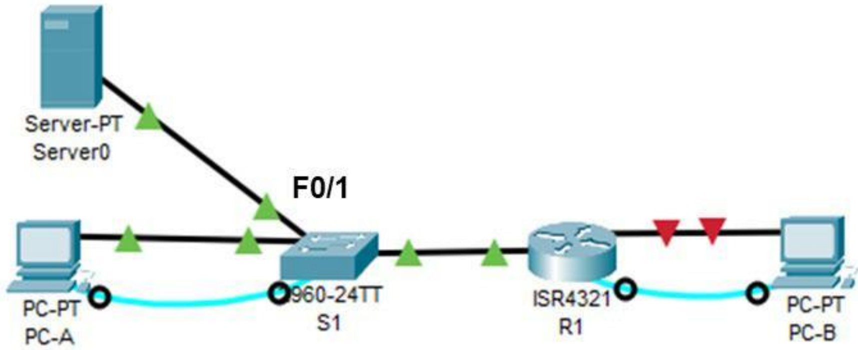
Each router interface belongs to a separate network. Packets with a link-local address never leave the local network. Therefore, same link-local address can be used on both interfaces g0/0/0 and g0/0/1.

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

Fourth hextet defines the Subnet ID of an IPv6 address having a prefix of /64. Here the 4th hextet contains <u>ab01 which has 16 bits.</u> So, the subnet ID is 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**. **Second available IP: 192.168.0.2 from first table**

Record TFTP Server IP Address and Subnet Mask:
Second available IP: 192.168.0.2
Subnet mask: 255.255.255.192 (for over 44 hosts this mask is taken)

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. Please check with your instructor for further assistance.

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

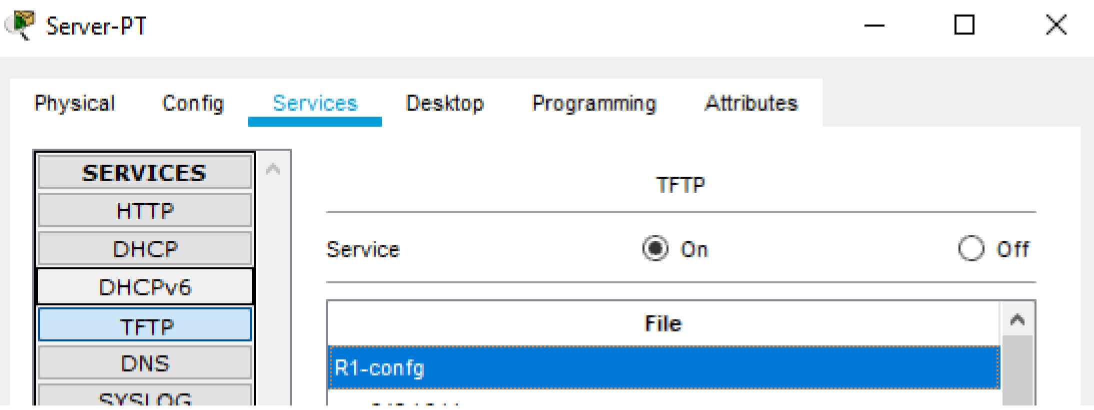
Yes transferred as seen from below.

File name is named as R1-confg.

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

Writing running-config...!!
[OK - 983 bytes]

983 bytes copied in 0.017 secs (57823 bytes/sec)
R1#
```



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.

After erasing and reloading, configuration on router with interface G0/0/1 is done.
Also at the last of step3-f part, I have switched on the other interface G0/0/0.

d. 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:

```
C:\>ping 192.168.0.30

Pinging 192.168.0.30 with 32 bytes of data:

Reply from 192.168.0.30: bytes=32 time=2ms TTL=255
Reply from 192.168.0.30: bytes=32 time=12ms TTL=255
Reply from 192.168.0.30: bytes=32 time<1ms TTL=255
Reply from 192.168.0.30: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

e. 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
```

f. 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.

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.