Practical – Week 12

Objectives:

The aim of this week's practical is:

- Consolidate your understanding of IPv6 addressing
- Configure IPv4 and IPv6 addressing and test connectivity

Tasks:

Accordingly, you will need to complete the following two tasks in this week's practical class:

1. Lab - IPv6 Addresses
2. Lab - Build a Switch and Router Network (with IPv4 and IPv6)

Instructions of the labs are on next pages, and the worksheet for this practical (to be completed and submitted) is in a separate word document in Week 12 Practical folder.

Assessment:

This week's Practical is assessed in class, and it is worth 3% of the total score of the course.

Notes:

- To be awarded marks for this Practical, a student must:
  - attend week 12 Practical class. Being absent from the class will result in zero marks for week 12's practical, and
  - complete the labs and submit the following two files in week 12 practical class using the "Practical-Week 12-Submission" link in Week 12 section of Learnonline course site:
    1. The completed lab worksheet, and
    2. The Packet Tracer file (a .pkt file) for Lab 2 - Build a Switch and Router Network (with IPv4 and IPv6)

    If you cannot finish the labs in class time, you need to let your tutor know before leaving the class and submit the above required two files by Sunday 11:59 pm of Week 12. Late submission will result in zero marks for week 12's practical.

Lab – IPv6 Addresses

Reminder:

1. Please read the lab instruction carefully (including the background and notes) and strictly follow the instruction to complete the steps.
2. Type your answers to the questions in the worksheet provided.

Objectives

Part 1: Identify the Different Types of IPv6 Addresses

Part 3: Practice IPv6 Address Abbreviation

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types, and in Part 3, you will practice IPv6 address abbreviation.

Part 1: Identify the Different Types of IPv6 Addresses

In Part 1, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

Step 1: Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits (4 x 32 = 128). A non-abbreviated IPv6 host address is shown here:

2001:0DB8:0001:0000:0000:0000:0000:0001

A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

An IPv4 address is 4 octets and is commonly written or displayed in decimal notation.

255.255.255.255

An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation.

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

In an IPv4 address, each individual octet is 8 binary digits (bits). Four octets equals one 32-bit IPv4 address.

11111111 = 255

11111111.11111111.11111111.11111111 = 255.255.255.255

In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address.

1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.
1111111111111111.1111111111111111.1111111111111111.1111111111111111 =
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

0000:0000:0000:0000:0000:0000:0000:0001 = loopback address

::1 = loopback address abbreviated

As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address.

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address

FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated

Study the chart below to help you identify the different types of IPv6 address based on the numbers in the first hextet.

First Hextet (Far Left)	Type of IPv6 Address
0000 to 00FF	Loopback address, any address, unspecified address, or IPv4-compatible
2000 to 3FFF	Global unicast address (a routable address in a range of addresses that is currently being handed out by the Internet Assigned Numbers Authority [IANA])
FE80 to FEBF	Link-local (a unicast address which identifies the host computer on the local network)
FC00 to FCFF	Unique-local (a unicast address which can be assigned to a host to identify it as being part of a specific subnet on the local network)
FF00 to FFFF	Multicast address

There are other IPv6 address types that are either not yet widely implemented, or have already become deprecated, and are no longer supported. For instance, an **anycast address** is new to IPv6 and can be used by routers to facilitate load sharing and provide alternate path flexibility if a router becomes unavailable. Only routers should respond to an anycast address. Alternatively, **site-local addresses** have been deprecated and replaced by unique-local addresses. Site-local addresses were identified by the numbers FEC0 in the initial hextet.

In IPv6 networks, there are no network (wire) addresses or broadcast addresses as there are in IPv4 networks.

Step 2: Match the IPv6 address to its type.

Match the IPv6 addresses to their corresponding address type. Notice that the addresses have been compressed to their abbreviated notation and that the slash network prefix number is not shown. Some answer choices must be used more than once.

IPv6 Address	Answer (Select correct answer from the choices given on the right –use the letter eg a,b,c,d,e,)
2001:0DB8:1:ACAD::FE55:6789:B210	a b c d e
::1	a b c d e
FC00:22:A:2::CD4:23E4:76FA	a b c d e
2033:DB8:1:1:22:A33D:259A:21FE	a b c d e
FE80::3201:CC01:65B1	a b c d e
FF00::	a b c d e
FF00::DB7:4322:A231:67C	a b c d e
FF02::2	a b c d e

Answer Choices

a. Loopback address

b. Global unicast address

c. Link-local address

d. Unique-local address

e. Multicast address

Part 2: Practice IPv6 Address Abbreviation

In this part of the lab, you will study and review rules for IPv6 address abbreviation to correctly compress and decompress IPv6 addresses.

Step 1: Study and review the rules for IPv6 address abbreviation.

Rule 1: In an IPv6 address, a string of four zeros (0s) in a hextet can be abbreviated as a single zero.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:0404:0001:1000:**0**:**0**:0EF0:BC00 (abbreviated with single zeros)

Rule 2: In an IPv6 address, the leading zeros in each hextet can be omitted, trailing zeros cannot be omitted.

2001:**0**404:**000**1:1000:0000:0000:**0**EF0:BC00

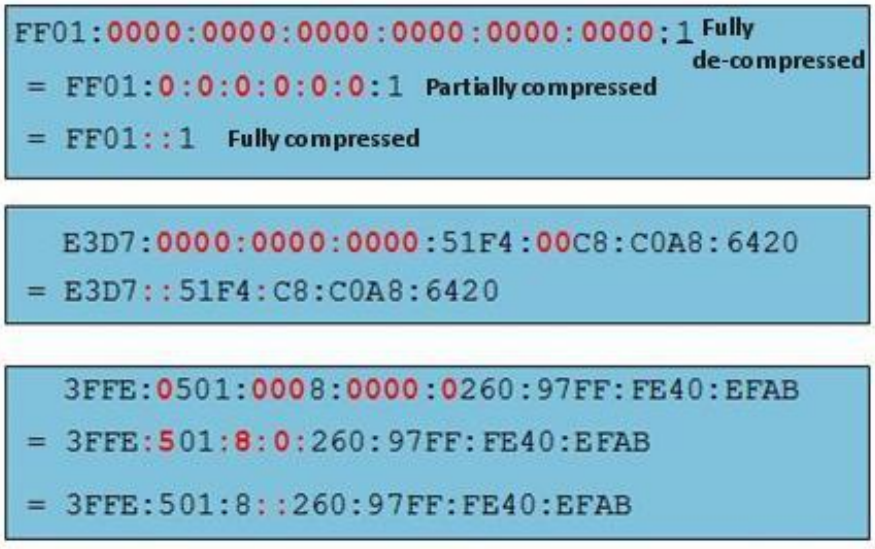
2001:404:1:1000:0:0:EF0:BC00 (abbreviated with leading zeros omitted)

Rule 3: In an IPv6 address, a single continuous string of four or more zeros can be abbreviated as a double colon (::). The double colon abbreviation can only be used one time in an IP address.

2001:0404:0001:1000**:0000:0000:**0EF0:BC00

2001:404:1:1000**::**EF0:BC00 (abbreviated with leading zeroes omitted and continuous zeros replaced with a double colon)

The image below illustrates these rules of IPv6 address abbreviation:



NOTE how the Ipv6 **fully** compressed or fully decompressed addresses look

Step 2: Practice compressing and decompressing IPv6 addresses.

Using the rules of IPv6 address abbreviation, either FULLY compress or FULLY decompress the following addresses: [the fully means apply ALL the applicable rules given above]

1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

_____

2) FE80:0000:0000:0001:0000:60BB:008E:7402

_____

3) FE80::7042:B3D7:3DEC:84B8

_____

4) FF00::

_____

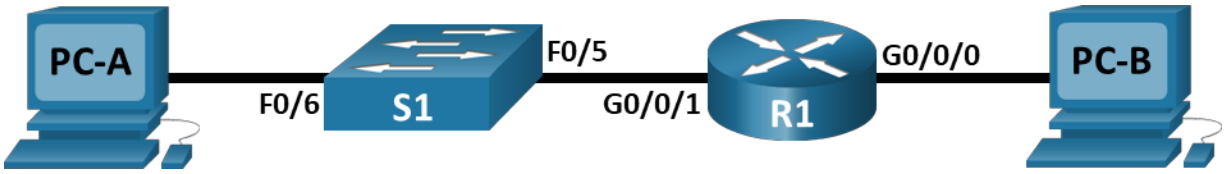
5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

_____

Lab - Build a Switch and Router Network

Reminder:
1. Start Packet Tracer, set up your User Profile (go to Packet Tracer menu, Options->User Profile)
2. Follow instructions given below to build and configure the network.
3. Save the network as a **.pkt** file and submit the file as part of your practical submission for this week.

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1/64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	N/A
		200:db8:acad:1::1/64	
		fe80::1	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
PC-A	NIC	192.168.1.3 /24	192.168.1.1
		2001:db8:acad:1::3/64	fe80::1
PC-B	NIC	192.168.0.3 /24	192.168.0.1
		2001:db8:acad::3/64	fe80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing

table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. Test your knowledge by trying to configure the devices without referring to the content or previous activities. If you do have difficulties with the commands to use, refer to Week 4 Practical instruction PDF (for the lab titled Building a Switch and Router Network), and Week 12 slides for IPv6 related commands.

Required Resources

- 1 Router (Cisco 4321 or 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 4221 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Instructions

Part 1: Set Up Topology

Step 1: Cable the network as shown in the topology.

a. Select the correct devices as required in the above Required Resources section.

b. Cable the network according to the topology. Use the interfaces/ports as shown in the topology diagram.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to Addressing Table at the beginning of this lab for device names and address information. Note that in the following, if a device has both IPv4 and IPv6 addressing, you need to configure both of them according to the Addressing table and verify both IPv4 and IPv6 connectivity.

Step 1: Assign static IP information to the PC interfaces.

a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

c. Ping PC-B (IPv4 and IPv6 addresses respectively) from a command prompt window on PC-A by typing the following ping commands, one by one:

```
ping 192.168.0.3
```

```
ping 2001:db8:acad::3
```

Note that the command for pinging an IPv6 address is also “ping”.

Were the pings successful? Explain.

Step 2: Configure the router.

a. Console into the router and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name to the router.

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

e. Assign **class** as the privileged EXEC encrypted password.

f. Assign **cisco** as the console password and enable login.

g. Assign **cisco** as the VTY password and enable login.

h. Encrypt the plaintext passwords.

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

j. Configure and activate both interfaces on the router.

The following shows the command used to configure IPv4 AND IPv6 addresses on the g0/0/0 interface on the router. To configure the other interface g0/0/1, you need to change the interface name to g0/0/1 and use the addressing information for g0/0/1 as shown in the addressing table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad::1/64
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

k. Configure an interface description for each interface indicating which device is connected to it.

l. To enable IPv6 routing, enter the command ipv6 unicast-routing.

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

m. Save the running configuration to the startup configuration file.

n. Set the clock on the router.

Note: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command

o. Ping PC-B (IPv4 and IPv6 addresses respectively) from a command prompt window on PC-A by typing the following ping commands, one by one:

```
ping 192.168.0.3
ping 2001:db8:acad::3
```

Were the pings successful? Explain.

Step 3: Configure the switch.

In this step, you will configure the hostname, the VLAN 1 interface and its default gateway.

a. Console into the switch and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name to the switch.

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

e. Configure and activate the VLAN interface on the switch S1.

f. Configure the default gateway for the switch S1.

g. Save the running configuration to the startup configuration file.

Step 4: Verify connectivity end-to-end connectivity.

a. From PC-A, ping PC-B's IPv4 and IPv6 addresses respectively.

b. From S1, ping PC-B.

All the pings should be successful.

Part 3: Display Device Information

In Part 3, you will use **show** commands to retrieve interface and routing information from the router and switch.

Step 1: Display the routing table on the router.

a. Use the **show ip route** command on the router R1 to answer the following questions.

What code is used in the routing table to indicate a directly connected network?

How many route entries are coded with a C code in the routing table?

What interface types are associated to the C coded routes?

b. Use the **show ipv6 route** command on router R1 to display the IPv6 routes.

Step 2: Display interface information on the router R1.

a. Use the **show ip interface g0/0/1** to answer the following questions.

What is the operational status of the G0/0/1 interface?

What is the Media Access Control (MAC) address of the G0/1 interface?

How is the Internet address displayed in this command?

b. For the IPv6 information, enter the **show ipv6 interface *interface*** command.

Step 3: Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

a. Enter the **show ip interface brief** command on the router R1.

```
R1# show ip interface brief
```

b. To see the IPv6 interface information, enter the **show ipv6 interface brief** command on R1.

```
R1# show ipv6 interface brief
```

c. Enter the **show ip interface brief** command on the switch S1.

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