

CSE 4512 [Computer Networks Lab]

Lab # 02

1. Objectives:

- Understand the basics of IP Subnetting
- Learn to subnet a network following given specifications
- Understand Variable Length Subnet Mask (VLSM) addressing scheme
- Learn to design and implement VLSM in a network
- Get to know Secure Shell (SSH) and Telnet basics

2. Theory:


This lab assumes that you know binary arithmetic operations and have basic knowledge about IPv4 addressing scheme. If not, you're requested to go through your class lectures and online reference materials understand these concepts.


IP Subnetting:

In the early days of networking, organizations could only use one network from the class A, B or C address space that were allocated to them. This resulted in a huge wastage of address space and newer demands for IP address could not be met properly. To overcome this problem, IP subnetting concept was introduced which enables splitting already existing larger networks into smaller networks. Use of subnetting freed up unnecessary allocation of IPv4 addresses and also made network management easier.

Now, let's see how this subnetting actually works in practice. You know a IPv4 address consists of two portions: a Network part and a Host part. A *class A* address will have 8 bits for its network portion and rest 24 bits for its host portion. What we do in subnetting is we take some bits from the host portion and designate them as **subnetwork** portion and the rest of the bits are used for host addressing. Then the number of bits in the subnetwork portion (raised to the power of 2) will define the number of possible subnets. A bit-mask known as **subnet mask** is used to differentiate between the subnetwork and host portion. A subnet mask is a 32-bit mask which contains 1's in its most significant bits equal to the number of bits in the network+subnetwork portion of an address. The remaining bits in the subnet mask are zero. Put in another way, the number of 0's in a subnet mask is equal to the number of hosts in each subnet. A concrete example of IP subnetting is given below.

Let's consider the network with IP address *172.16.0.0*. This is a *class B* IP address and we know for a class B address, first 16 bits are the Network portion and rest 16 bits are host portion. Now, let's say, we want to have 2 subnets out of this bigger network. We'll then take 1 bit (as $2^1=2$) from 16 bits host portion. Then host portion will have 15 bits in total which means each subnet will have $(2^{15})-2 = 32,768-2 = 32,766$ hosts. And the subnet mask will be *255.255.128.0*.

172.16.0.0 - 10101100 00010000 00000000 00000000  Network Address

255.255.128.0 - 11111111 11111111 10000000 00000000  Subnet Mask

Note that, a different notation known as CIDR (Classless Inter-Domain Routing) notation is also used to specify a subnet mask. This is basically the number of bits in network portion (including the subnetwork portion) of an IP address and is written with a / in front of it. So, for our running example, it would be written as 172.16.0.0/17 as there are 17 bits in network portion. For remainder portion of this lab handout, we will use this CIDR notation.

So, continuing on the above example, the two subnets will be 172.16.0.0/17 (subnet A) and 172.16.128.0/17 (subnet B). Each subnet will now function as an independent network. So, at the cost of reducing total number of hosts in a network, we've added another level of network to ease management and reduce IP address wastage. In a similar way, a bigger network can be subnetted to meet the number of host requirement. Now, that we've an understanding of how IP subnetting works, we are ready to understand VLSM (Variable Length Subnet Mask) addressing scheme which is a special form subnetting.

VLSM:

Though we stated that subnet masking reduces IP address wastage, this is partially true. Subnetting scheme demonstrated above also suffers from IP address wastage albeit in a reduced manner than without subnetting. This is because in case of normal subnetting the same subnet mask is applied to all the subnets which results in same number of hosts in each subnet. This is not an efficient solution as some networks might have number of host requirements that don't *exactly* match the number of hosts obtained after applying same subnet masks in all subnets. All subnets might not utilize all hosts that result in address wastage.

To counter this issue, a subnet is further divided into more subnets and this method is known as variable length subnet masking because each subnet would have a different subnet mask (variable length) unlike what we saw in previous section. Now, let's consider a concrete example.

Suppose, we have been asked to subnet the network with address 204.15.5.0/24 to meet the following host requirements:

- netA: must support 14 hosts
- netB: must support 28 hosts
- netC: must support 2 hosts
- netD: must support 7 hosts
- netE: must support 28 host

The way to create subnets using VLSM technique is to take the largest host requirement first and assign it the appropriate subnet mask. Let's take netB first. It requires 28 hosts, so a subnet mask of /27 would meet its needs. Because /27 leaves 5 bits for host addressing that gives us $2^5 = 32$ hosts. Note that, we always need to choose the nearest block that meets the given host requirement. In this case, a subnet mask of /28 would give us $2^4 = 16$ host addresses which would fail to meet the given requirement and a mask of /26 would result in address wastage. So, if we follow similar approach as above for the other networks (in descending order of host requirements), we would reach the final subnetting as shown below:

netB: 204.15.5.0/27 host address range 1 to 30

netE: 204.15.5.32/27 host address range 33 to 62

netA: 204.15.5.64/28 host address range 65 to 78

netD: 204.15.5.80/28 host address range 81 to 94

netC: 204.15.5.96/30 host address range 97 to 98

Remember to increment the host portion of the calculated network addresses accordingly. So, following this technique, we can meet any kind of host specification with very little address wastage.

Telnet and SSH:

Telnet is an application protocol for communication between two end devices which enables virtual access to a remote device. It's a bi-directional client-server protocol i.e., both sides can communicate interactively with one another. The standard TCP port for Telnet is 23. A user can log in to a remote server and interact with it using this protocol. Major drawback of this protocol is that all the communication happens in plain text which enables an attacker to see through any telnet communication by intercepting the packets and makes it possible to capture the password and get access to the remote device. For more on Telnet, you can further read [here](#).

Secure Shell Protocol (SSH) have now become the application protocol of choice for communicating with remote resources as it provides an encrypted channel between the two ends. It also provides remote authentication and allows for remote administration. The standard TCP port for SSH is 22. In order for SSH to work, both the parties must agree on a common encryption technique. Further communication happens based on the agreed encryption technique. You can read more on SSH [here](#).

3. Tasks:

- I. You need to subnet a network following the given network specification and configure the devices properly following proper IP addressing. The task description is provided in the ***Task-1_subnet-an-ipv4-network*** pdf. You're also given a .pka file for this task.
- II. The task description for this task is provided in the ***Task-2_VLSM*** pdf. You'll have to subnet a given network topology following the network description provided in the pdf. You'll need to create the network topology by yourself as there's no .pka file provided for this task.
- III. Create a copy of your completed .pka file from task I and rename it as "**Task3_ZZZ**" where *ZZZ* denotes last 3 digits of your student ID. Then following the steps in *Basic Telnet and SSH configuration* in section 3, configure ssh in the *CustomerRouter* device. You just need to customize one thing while doing this task. Change the **domain name** of the router to **ZZZ.com** where *ZZZ* is last 3 digits of your student ID.

Packet Tracer – Subnet an IPv4 Network

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
CustomerRouter	G0/0			N/A
	G0/1			
	S0/1/0	209.165.201.2	255.255.255.252	
LAN-A Switch	VLAN1			
LAN-B Switch	VLAN1			
PC-A	NIC			
PC-B	NIC			
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

Objectives

Part 1: Design an IPv4 Network Subnetting Scheme

Part 2: Configure the Devices

Part 3: Test and Troubleshoot the Network

Background / Scenario

In this activity, you will subnet the Customer network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the table by filling in the missing host and interface IP addresses, you will configure the host PCs, switches and router interfaces.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

Instructions

Part 1: Subnet the Assigned Network

Step 1: Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network technician assigned to install a new network for a customer. You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

- a. The first subnet is the LAN-A network. You need a minimum of 50 host IP addresses.
- b. The second subnet is the LAN-B network. You need a minimum of 40 host IP addresses.
- c. You also need at least two additional unused subnets for future network expansion.

Note: Variable length subnet masks will not be used. All of the device subnet masks should be the same length.

- d. Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

How many host addresses are needed in the largest required subnet?

What is the minimum number of subnets required?

The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?

- e. The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.

In the network mask, what do the ones represent?

In the network mask, what do the zeros represent?

- f. To subnet a network, bits from the host portion of the original network mask are changed into subnet bits. The number of subnet bits defines the number of subnets.

Given each of the possible subnet masks depicted in the following binary format, how many subnets and how many hosts are created in each example?

Hint: Remember that the number of host bits (to the power of 2) defines the number of hosts per subnet (minus 2), and the number of subnet bits (to the power of two) defines the number of subnets. The subnet bits (shown in bold) are the bits that have been borrowed beyond the original network mask of /24. The /24 is the prefix notation and corresponds to a dotted decimal mask of 255.255.255.0.

- 1) (/25) 11111111.11111111.11111111.**10000000**

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

- 2) (/26) 11111111.11111111.11111111.11000000

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

- 3) (/27) 11111111.11111111.11111111.11100000

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

- 4) (/28) 11111111.11111111.11111111.11110000

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

- 5) (/29) 11111111.11111111.11111111.11111000

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

- 6) (/30) 11111111.11111111.11111111.11111100

Dotted decimal subnet mask equivalent:

Number of subnets? Number of hosts?

Considering your answers above, which subnet masks meet the required number of minimum host addresses?

Considering your answers above, which subnet masks meets the minimum number of subnets required?

Considering your answers above, which subnet mask meets both the required minimum number of hosts and the minimum number of subnets required?

When you have determined which subnet mask meets all of the stated network requirements, derive each of the subnets. List the subnets from first to last in the table. Remember that the first subnet is 192.168.0.0 with the chosen subnet mask.

Subnet Address	Prefix	Subnet Mask

Step 2: Fill in the missing IP addresses in the Addressing Table

Assign IP addresses based on the following criteria: Use the ISP Network settings as an example.

- a. Assign the first subnet to LAN-A.
 - 1) Use the first host address for the CustomerRouter interface connected to LAN-A switch.
 - 2) Use the second host address for the LAN-A switch. Make sure to assign a default gateway address for the switch.
 - 3) Use the last host address for PC-A. Make sure to assign a default gateway address for the PC.
- b. Assign the second subnet to LAN-B.
 - 1) Use the first host address for the CustomerRouter interface connected to LAN-B switch.
 - 2) Use the second host address for the LAN-B switch. Make sure to assign a default gateway address for the switch.
 - 3) Use the last host address for PC-B. Make sure to assign a default gateway address for the PC.

Part 2: Configure the Devices

Configure basic settings on the PCs, switches, and router. Refer to the Addressing Table for device names and address information.

Step 1: Configure CustomerRouter.

- a. Set the enable secret password on CustomerRouter to **Class123**
- b. Set the console login password to **Cisco123**.
- c. Configure **CustomerRouter** as the hostname for the router.
- d. Configure the G0/0 and G0/1 interfaces with IP addresses and subnet masks, and then enable them.
- e. Save the running configuration to the startup configuration file.

Step 2: Configure the two customer LAN switches.

Configure the IP addresses on interface VLAN 1 on the two customer LAN switches. Make sure to configure the correct default gateway on each switch.

Step 3: Configure the PC interfaces.

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

Part 3: Test and Troubleshoot the Network

In Part 3, you will use the **ping** command to test network connectivity.

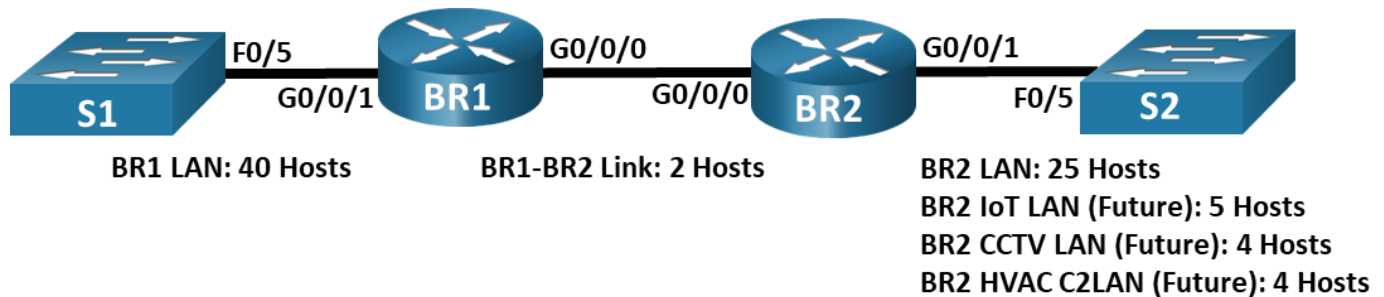
- a. Determine if PC-A can communicate with its default gateway. Do you get a reply?

- b. Determine if PC-B can communicate with its default gateway. Do you get a reply?
- c. Determine if PC-A can communicate with PC-B. Do you get a reply?

If you answered “no” to any of the preceding questions, then you should go back and check your IP address and subnet mask configurations, and ensure that the default gateways have been correctly configured on PC-A and PC-B.

Lab - Design and Implement a VLSM Addressing Scheme

Topology



Objectives

Part 1: Examine Network Requirements

Part 2: Design the VLSM Address Scheme

Part 3: Cable and Configure the IPv4 Network

Background / Scenario

Variable Length Subnet Mask (VLSM) was designed to avoid wasting IP addresses. With VLSM, a network is subnetted and then re-subnetted. This process can be repeated multiple times to create subnets of various sizes based on the number of hosts required in each subnet. Effective use of VLSM requires address planning.

In this lab, use the 192.168.33.128/25 network address to develop an address scheme for the network displayed in the topology diagram. VLSM is used to meet the IPv4 addressing requirements. After you have designed the VLSM address scheme, you will configure the interfaces on the routers with the appropriate IP address information. The future LANS at BR2 will need to have addresses allocated, but no interfaces will be configured at this time.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

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

- Windows Calculator (optional)

Instructions

Part 1: Examine Network Requirements

In Part 1, you will examine the network requirements to develop a VLSM address scheme for the network displayed in the topology diagram using the 192.168.33.128/25 network address.

Note: You can use the Windows Calculator application and search the internet for an IP subnet calculator to help with your calculations.

Step 1: Determine how many host addresses and subnets are available.

How many host addresses are available in a /25 network?

What is the total number of host addresses needed in the topology diagram?

How many subnets are needed in the network topology?

Step 2: Determine the largest subnet.

What is the subnet description (e.g. BR1 LAN or BR1-BR2 link)?

How many IP addresses are required in the largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the 192.168.33.128/25 network address to support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 3: Determine the second largest subnet.

What is the subnet description?

How many IP addresses are required for the second largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 4: Determine the third largest subnet.

What is the subnet description?

How many IP addresses are required for the next largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Use the second network address for the CCTV LAN.

Use the third network address for the HVAC C2 LAN.

Step 5: Determine the fourth largest subnet.

What is the subnet description?

How many IP addresses are required for the next largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Part 2: Design the VLSM Address Scheme

Step 1: Calculate the subnet information.

Use the information that you obtained in Part 1 to fill in the following table.

Subnet Description	Number of Hosts Needed	Network Address /CIDR	First Host Address	Broadcast Address
BR1 LAN	40			
BR2 LAN	25			
BR2 IoT LAN	5			
BR2 CCTV LAN	4			
BR2 HVAC C2LAN	4			
BR1-BR2 Link	2			

Step 2: Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. BR1 should be assigned the first host address in the BR1-BR2 Link.

Device	Interface	IP Address	Subnet Mask	Device Interface
BR1	G0/0/0	192.168.33.249	255.255.255.252	BR1-BR2 Link
	G0/0/1	192.168.33.129	255.255.255.192	40 Host LAN
BR2	G0/0/0	192.168.33.250	255.255.255.252	BR1-BR2 Link
	G0/0/1	192.168.33.193	255.255.255.224	25 Host LAN

Part 3: Cable and Configure the IPv4 Network

In Part 3, you will cable the network to match the topology and configure the three routers using the VLSM address scheme that you developed in Part 2.

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

Step 2: Configure basic settings on each router.

- Assign the device name to the routers.
- Disable DNS lookup to prevent the routers from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password for both routers.
- Assign **cisco** as the console password and enable login for the routers.
- Assign **cisco** as the VTY password and enable login for the routers.
- Encrypt the plaintext passwords for the routers.

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

Step 3: Configure the interfaces on each router.

- a. Assign an IP address and subnet mask to each interface using the table that you completed in Part 2.
- b. Configure an interface description for each interface.
- c. Activate the interfaces.

Step 4: Save the configuration on all devices.

Step 5: Test Connectivity.

- a. From BR1, ping BR2's G0/0/0 interface.
- b. From BR2, ping BR1's G0/0/0 interface.
- c. Troubleshoot connectivity issues if pings were not successful.

Note: Pings to the GigabitEthernet LAN interfaces on other routers will not be successful. A routing protocol needs to be in place for other devices to be aware of those subnets. The GigabitEthernet interfaces also need to be in an up/up state before a routing protocol can add the subnets to the routing table. The focus of this lab is on VLSM and configuring the interfaces.

Reflection Question

Can you think of a shortcut for calculating the network addresses of consecutive /30 subnets?

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device.

Lab - Design and Implement a VLSM Addressing Scheme

The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Basic Telnet and SSH configuration:

- I. Configure the vty line. Vty stands for virtual teletype. It's a virtual port and used for remotely accessing the device through telnet and ssh.

```
IUT(config)# line VTY 0 4
```

0 4 means allow 4 simultaneous connections to vty in ports 0 through 4.

```
IUT(config-line)# password class
```

class is the password.

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

This command enables password check at login time and verifies that the password is working.

The following commands define which protocol to allow through vty line connection.

```
IUT(config-line)# transport input telnet
```

It allows only telnet.

Or,

```
IUT(config-line)# transport input ssh
```

It allows only ssh.

Or,

```
IUT(config-line)# transport input all
```

It allows all supported protocols.

- II. Configure the Interfaces (FastEthernet or GigabitEthernet) (shown in Lab-1):

```
IUT(config)# interface fastEthernet 0/0
```

```
IUT(config-if)# ip address 192.168.10.1 255.255.255.0
```

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

```
IUT(config-if)# description LAN-NORTH-HALL
```

```
IUT(config)# interface gigabitEthernet 0/0
```

```
IUT(config-if)# ip address 192.168.11.1 255.255.255.0
```

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

```
IUT(config-if)# description LAN-SOUTH-HALL
```

```
IUT(config)# interface serial 0/0/0
```

```
IUT(config-if)# ip address 192.168.10.1 255.255.255.0
```

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

- III. Create Username and Password:

```
IUT(config)# username admin password IUT
```


IV. Configure SSH:

The following command will set the domain name for the Cisco router/switch. The SSH keys will be generated based on this domain name and also the host name.

```
IUT(config)# ip domain-name iut.com
```

The following command will generate RSA (a public-key cryptographic algorithm) key pairs for the device in use. Please make sure the domain name and hostname for the device is configured before issuing the command.

```
IUT(config)# crypto key generate rsa
```

How many bits in modulus [512]: **1024**

Note that, the longer the modulus the stronger is the key. But longer modulus will take more time to generate the key.

```
IUT(config)# line VTY 0 4
```

```
IUT(config-line)# login local
```

This command tells the Router to authenticate all incoming virtual terminal sessions via the local username database i.e., users created using the *username XXX password YYY* command in global configuration mode. Whereas, the login command that we used in step 1 is used to authenticate against the password set inside line console or vty configuration mode.

```
IUT(config-line)# transport input ssh
```

Now, you can use telnet and ssh from a desktop connected with this cisco device.

For login using telnet from Command Prompt:

```
> telnet 192.168.11.1
```

For login using SSH from Command Prompt:

```
> ssh -l admin 192.168.11.1
```