ETN LAB INTERNAL

Title - SSH: Basic Cisco Device Configuration Configure

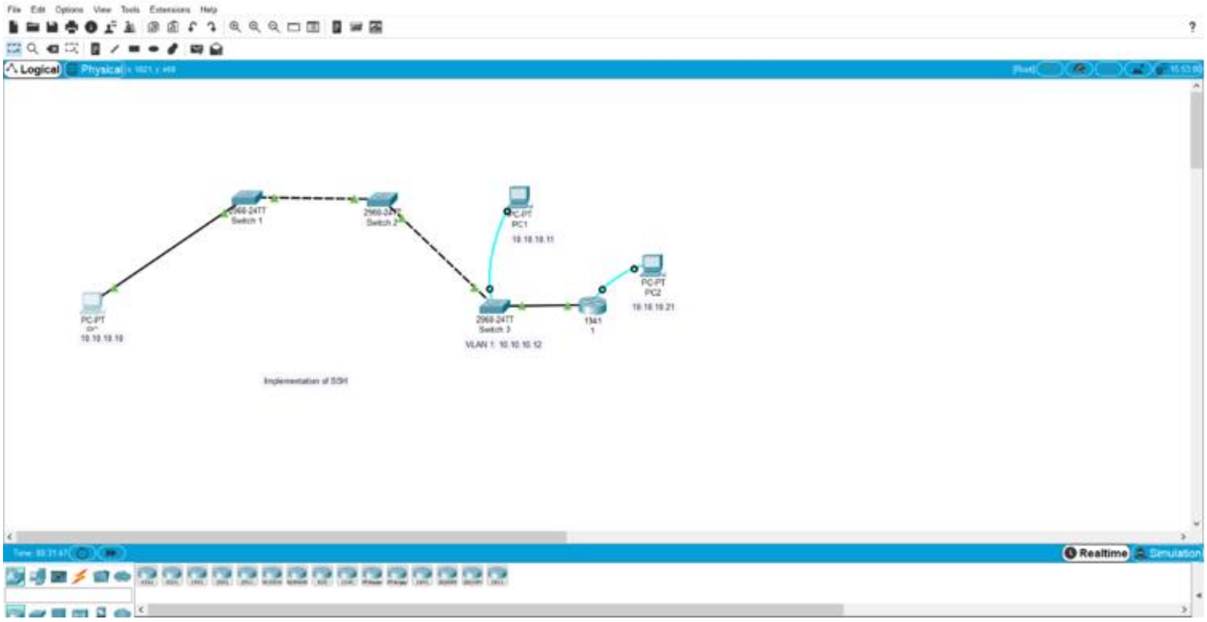
Objective -
Hardware/Software Used – Cisco Packet Tracer
Step by step config-

- Basic Cisco Device Configuration Configure Cisco router global configuration settings.
- Configure Cisco router interfaces.
- Save the router configuration file.
- Configure a Cisco switch Assign a device name to the router based on the topology and Addressing Table. Disable DNS lookup.
- Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
- Assign class as the privileged EXEC encrypted password. 7. Assign cisco as the console password and enable console login access. Encrypt clear text passwords.
- Create a domain name of cisco.com for SSH access. Create a user named admin with a secret password of cisco for SSH access.
- Generate a RSA modulus key. Use 1024 for the number of bits. Configure VTY line access.
- Use the local database for authentication for SSH. Enable SSH only for login access.

implment and configure ssh on router:
connect switch and router on gigabit ethernet 0/0
set ip for pc-4

```
(config)#enter global config mode
interface gigabitEthernet 0/0
ip address 10.10.10.20 255.0.0.0
no shutdown
(config)#change hostname of router
(config)#ip domain-name cisco.com
(config)#crypto key generate rsa  (it is used to generate 2 keys for 2 diff parties)
how many bits in the module(512): 1024
(config)#ip ssh version 2
(config)#line vty 0 4
(config-line)#transport input ssh
(config-line)#login local
(config-line)#username admin passowrd ....
ssh -l admin 10.10.10.20
```

Outcome -



Title-Implementation of telnet.

Objective:

Examining a Route Use the route command to modify a Windows computer routing table. Use a Windows Telnet client command telnet to connect to a Cisco router. Examine router routes using basic Cisco IOS commands. TELNET

Resources :

1- I am using packet tracer
2- I am using windows 10

Step by step:

Step 1- Open packet tracer.
Step 2- take 3 switch from 3 different cities.
Step 3- take 2 computer .

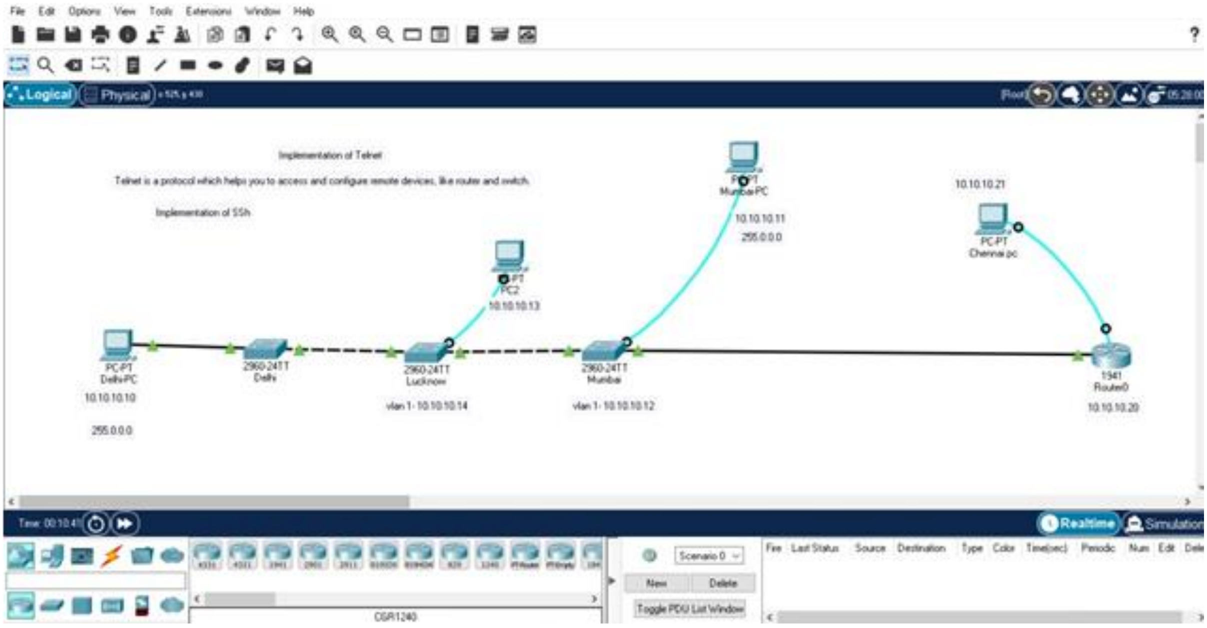
Step 4- connect one pc to switch using copper straight through.
Step 5- Connect switch to switch connect with copper cross over
Step 6- First we have to configure telnet procedure in switch.
Step 7- Take one more pc.
Step 8- with the help of console cable we connect
to Mumbai switch
Step 9- open pc 1 desktop ip-10.10.10.10
Step 10- open pc 2 desktop ip-10.10.10.11

- Switch in second layer device
  we cant configure any ip address
- However who access switch who performed telnet its compulsory to assign ip address
- We can configure more than one ip address on switch in VLAN

Step 11- Compulsory to assign ip address
who connet to Mumbai pc
Step 12- compulsory assign ip address who connect to Mumbai in pc 2 terminal command
enable, configure,configure terminal, interface VLAN1,ip address 10.10.10.12 subnet mask 255.0.0.0, no shutdown

Step 13- line VTY 0 4, password cisco,login,exit

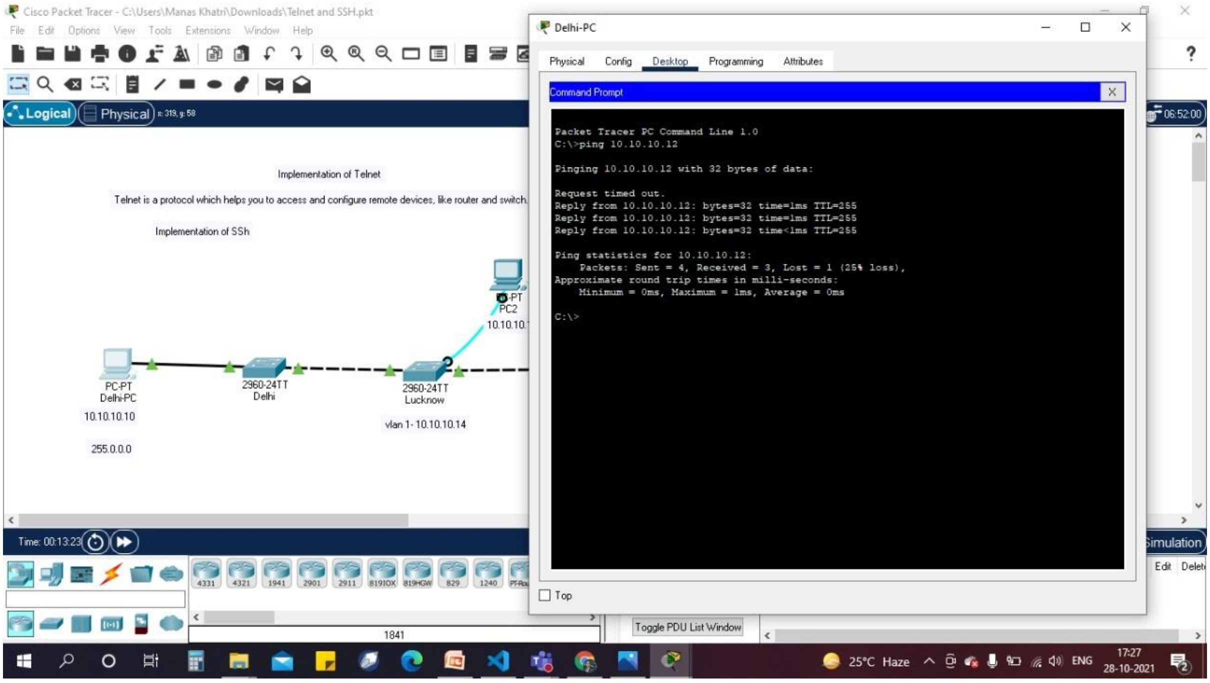
Step 14- Go to delhi pc(pc1) telnet 10.10.10.12, password cisco , hostname packet



Implementation of Telnet

Telnet is a protocol which helps you to access and configure remote devices, like router and switch.

Implementation of SSh



Implementation of Telnet

Telnet is a protocol which helps you to access and configure remote devices, like router and switch.

Implementation of SSh

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.12

Pinging 10.10.10.12 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.12: bytes=32 time=1ms TTL=255
Reply from 10.10.10.12: bytes=32 time=1ms TTL=255
Reply from 10.10.10.12: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Lab– IPv4 Address Subnetting Scenario

1. Objectives:-

- The subnet address of this subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet

- The maximum number of subnets for this subnet mask
- The number of hosts for each subnet
- The number of subnet bits
- The number of this subnet

192.168.10.0/27

2. Required Hardware and software

- Device with Internet access
- Optional: IPv4 address calculator
- Cisco packet Tracer

1. Identify network/host, subnet mask and network address.

In Part 1, you will be given several examples of IPv4 addresses and will complete tables with appropriate information.

1. Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

The first two rows show examples of how the table should be completed.

Key for table:

N = all 8 bits for an octet are in the network portion of the address
n = a bit in the network portion of the address
H = all 8 bits for an octet are in the host portion of the address
h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network, H,h = Host	Subnet Mask	Network Address
192.168.10.0/27	N.N.N.nnnhhhhh	255.255.255.224	192.168.10.0

2. Analyze the table below and list the range of host and broadcast addresses given a network/prefix mask pair.

The first row shows an example of how the table should be completed.

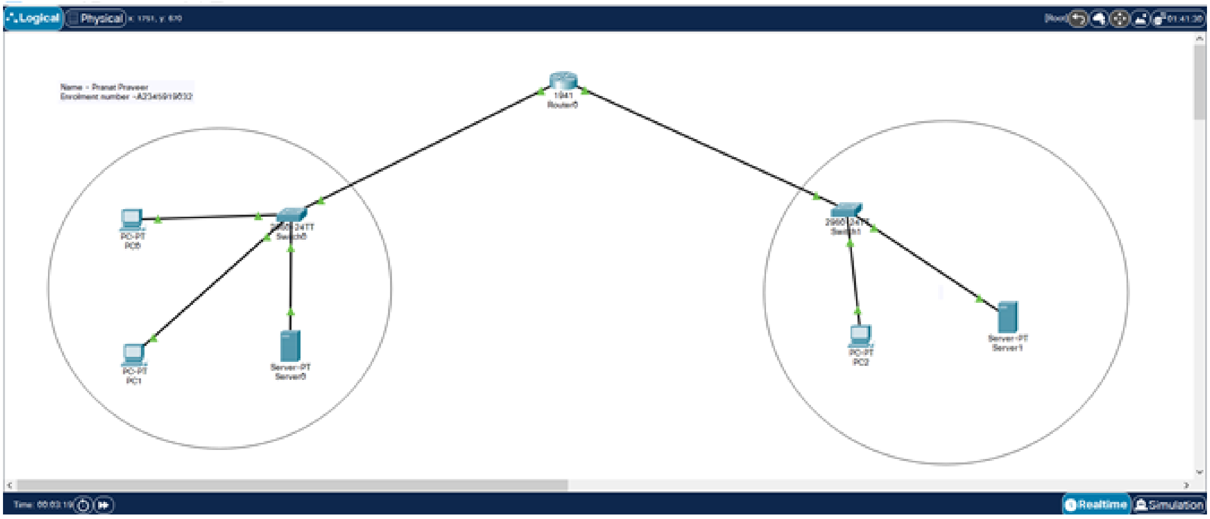
IP Address/Prefix	First Host Address	Last Host Address	Broadcast Address
192.168.10.0/27	192.168.10.1	192.168.10.254	192.168.10.255

2. IPv4 Address type

In Part 2, we will identify and classify several examples of IPv4 addresses.

IP Address	Subnet Mask	Address Type
192.168.10.0	255.255.255.224	host

Output:-



2. Objectives

Part 1: Examine Network Requirements

Part 2: Design the VLSM Address Scheme

Part 3: Cable and Configure the IPv4 Network

3. 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 172.16.128.0/17 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.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this 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.

4. Required Resources

- 3 routers (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 PC (with terminal emulation program, such as Tera Term, to configure routers)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet (optional) and serial cables, as shown in the topology
- Windows Calculator (optional)

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 172.16.128.0/17 network address.

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

How many host addresses are available in a /17 network? __

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

How many subnets are needed in the network topology?

2. Determine the largest subnet.

What is the subnet description (e.g. BR1 G0/1 LAN or BR1-HQ WAN 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 172.16.128.0/17 network address to support this subnet? ____

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

____

Use the first network address for this subnet.

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 two network addresses that would result from this subnetting?

____

Use the first network address for this subnet.

4. Determine the next 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 two network addresses that would result from this subnetting?

____

____

Use the first network address for this subnet.

5. **Determine the next 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 two network addresses that would result from this subnetting?

____

____

Use the first network address for this subnet.

6. **Determine the next 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 two network addresses that would result from this subnetting?

____

____

Use the first network address for this subnet.

7. **Determine the next 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 two network addresses that would result from this subnetting?

____

____

Use the first network address for this subnet.

8. **Determine the subnets needed to support the serial links.**

How many host addresses are required for each serial subnet link? ______

What subnet mask can support that many host addresses?

____

a. Continue subnetting the first subnet of each new subnet until you have four /30 subnets. Write the first three network addresses of these /30 subnets below.

____

____

____

b. Enter the subnet descriptions for these three subnets below.

____

____

____

2. Design the VLSM Address Scheme

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
HQ G0/0	16,000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8,000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4,000			
BR1 G0/0	2,000			
BR2 G0/1	1,000			
BR2 G0/0	500			
HQ S0/0/0 – BR1 S0/0/0	2			
HQ S0/0/1 – BR2 S0/0/1	2			
BR1 S0/0/1 – BR2 S0/0/0	2			

2. Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. HQ should be given the first host address on the Serial links to BR1 and BR2. BR1 should be given the first host address for the serial link to BR2.

Device	Interface	IP Address	Subnet Mask	Device Interface
HQ	G0/0	172.16.128.1	255.255.192.0	16,000 Host LAN
	G0/1	172.16.192.1	255.255.224.0	8,000 Host LAN
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	2,000 Host LAN
	G0/1	172.16.224.1	255.255.240.0	4,000 Host LAN
	S0/0/0	172.16.254.9	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0
BR2	G0/0	172.16.252.1	255.255.254.0	500 Host LAN
	G0/1	172.16.248.1	255.255.252.0	1,000 Host LAN
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

3. Cable and Configure the IPv4 Network

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

1. Cable the network as shown in the topology.

2. Configure basic settings on each router.

a. Assign the device name to the router.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

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

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

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

f. Encrypt the clear text passwords.

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

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. Set the clocking rate on all DCE serial interfaces to 128000.

```
HQ(config-if)# clock rate 128000
```

d. Activate the interfaces.

4. Save the configuration on all devices.

5. Test Connectivity.

a. From HQ, ping BR1’s S0/0/0 interface address.

b. From HQ, ping BR2’s S0/0/1 interface address.

c. From BR1, ping BR2’s S0/0/0 interface address.

d. Troubleshoot connectivity issues if pings were not successful.

Note: Pings to the GigabitEthernet interfaces on other routers will not be successful. The LANs defined for the GigabitEthernet interfaces are simulated. Because no devices are attached to these LANs they will be in down/down state. 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. These interfaces will remain in a down/down state until a device is connected to the other end of the Ethernet interface cable. The focus of this lab is on VLSM and configuring the interfaces.

5. Reflection

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

____
____
____
____
____
____
____
____

6. Router Interface Summary Table

Router Interface Summary				
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)

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. 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.

7.

ETN INTERNAL LAB ASSESSMENT
Experiment 2

Title : Implementation of ARP Table.

Objective : Implement and show the working of ARP. (Build your own topology). Assign a device name to the router based on the topology and Addressing Table. Disable DNS lookup. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited. Assign class as the privileged EXEC encrypted password. Assign cisco as the console password and enable console login access. Encrypt clear text passwords.

The Address Resolution Protocol (ARP) feature performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses. ARP is part of all Cisco systems that run IP.

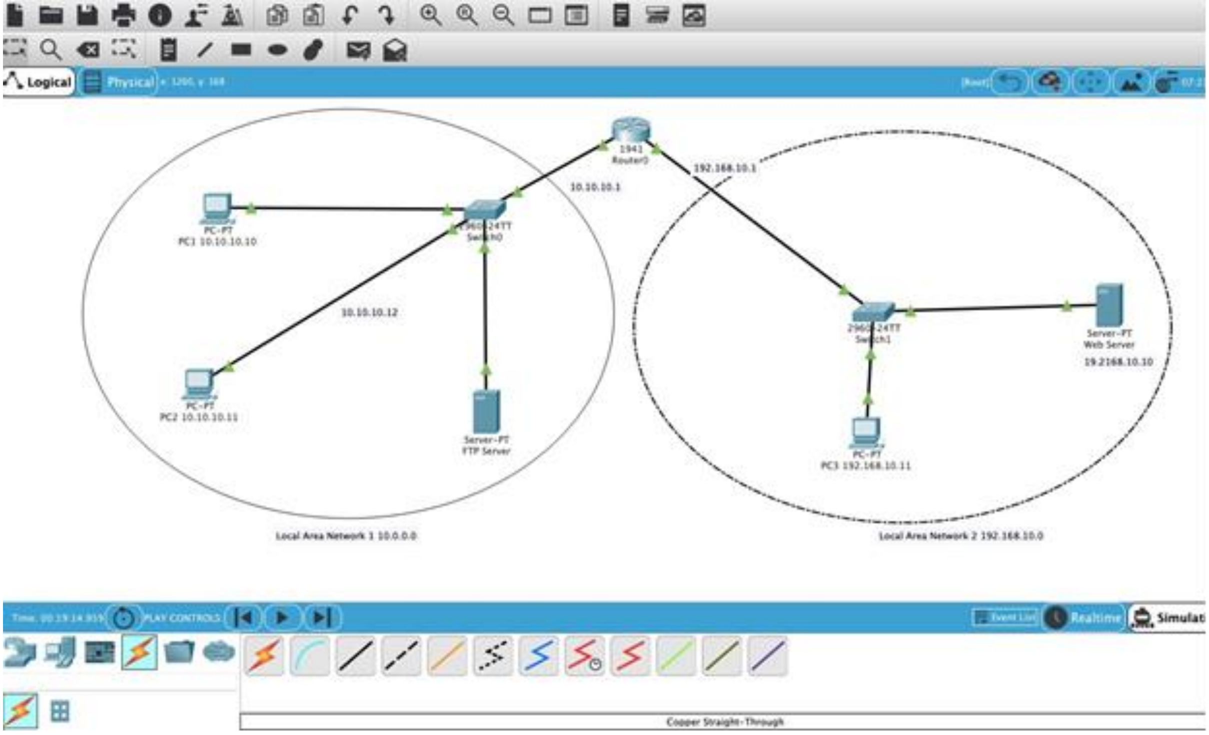
Software/Hardware used: 3 PC, 2 server, 2 switch, 1 router, Cisco Packet Tracer

Step by Step Configurations:

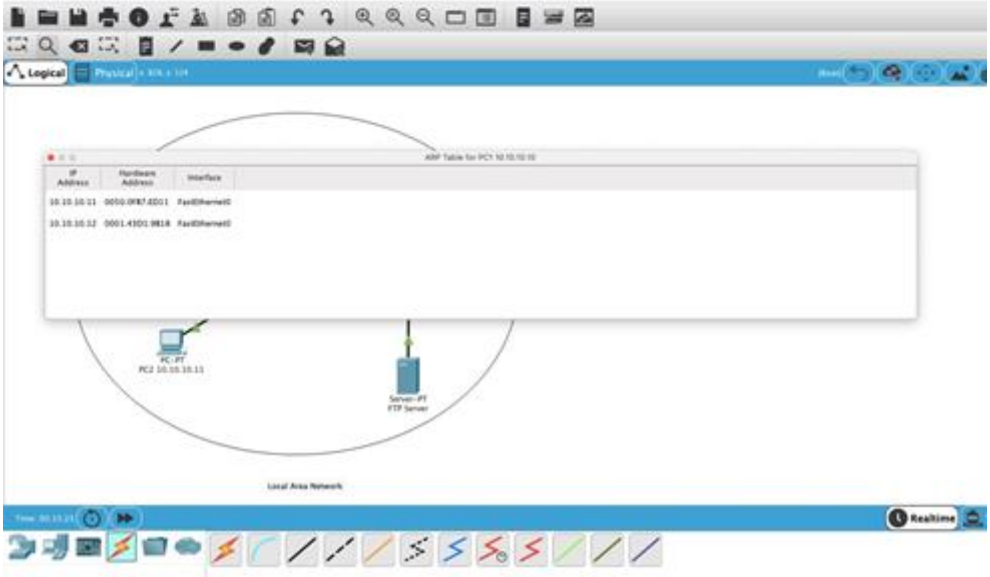
1. Connect all the devices creating two local area networks.
2. Assign ip addresses to all the devices except switch.
3. Connect both the local area networks using router and assign network ip address, RIP (routing protocols - network address) in it and make sure to turn it on in while assigning ip addresses.
4. Follow the commands to Assign cisco as the console password and enable console login access.

Result:

1. Output of connection of all the devices.



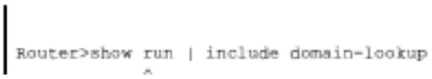
2. ARP Table :



ARP Table for PC1 10.10.10.10

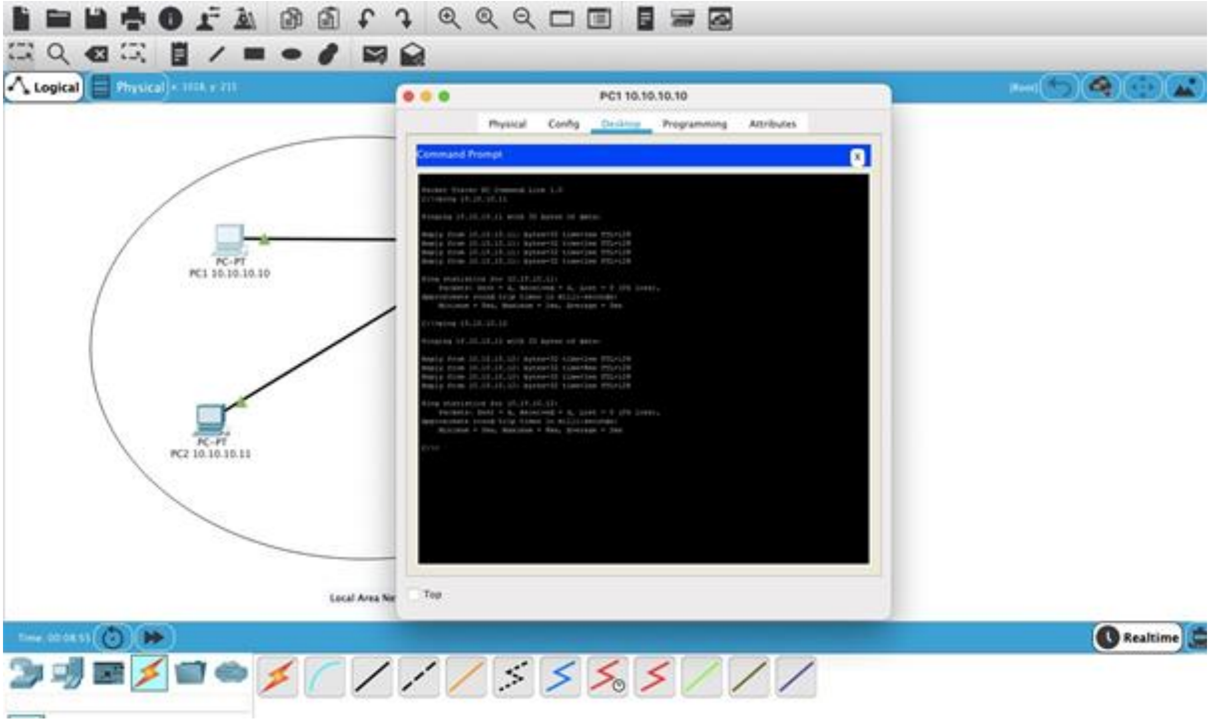
IP Address	Hardware Address	Interface
10.10.10.11	0050.0FB7.6D01	FastEthernet0
10.10.10.12	0001.43D1.9818	FastEthernet0

3. DNS lookup



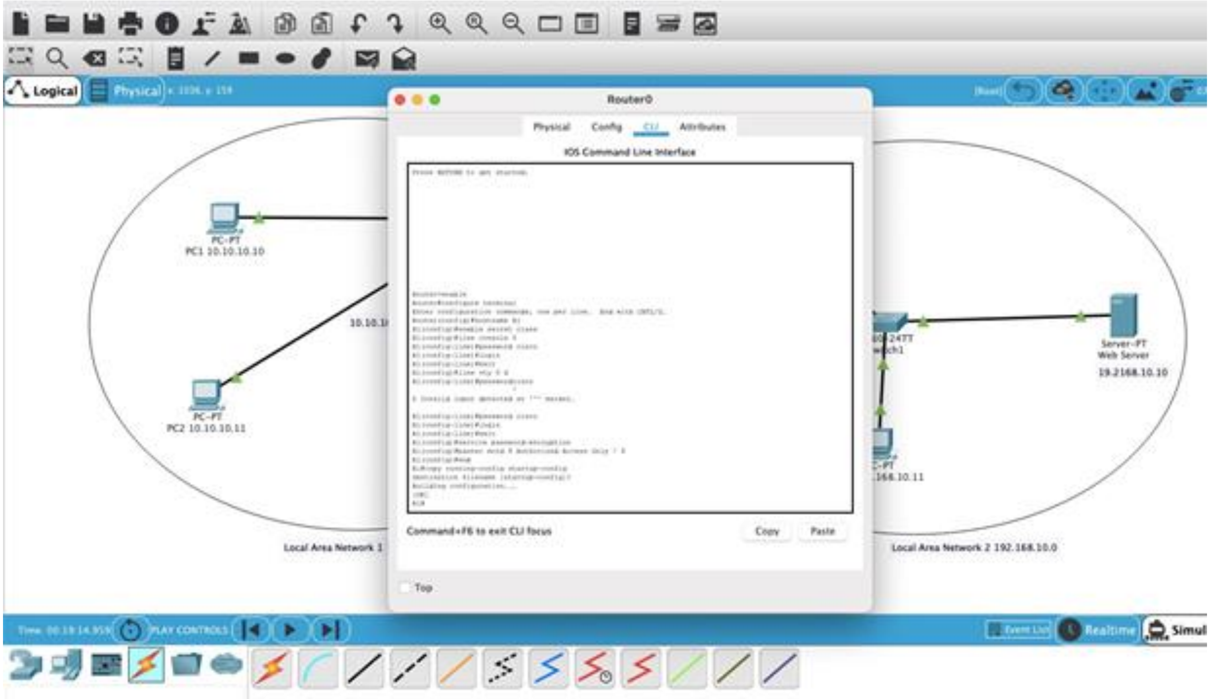
```
Router>show run | include domain-lookup
                ^
```

4. Connection working using ping command



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 [illegible] TTL=128
Reply from 10.10.10.11: bytes=32 [illegible] TTL=128
Reply from 10.10.10.11: bytes=32 [illegible] TTL=128
Reply from 10.10.10.11: bytes=32 [illegible] TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

C:\>ping 10.10.10.12

Pinging 10.10.10.12 with 32 bytes of data:

Reply from 10.10.10.12: bytes=32 [illegible] TTL=128
Reply from 10.10.10.12: bytes=32 [illegible] TTL=128
Reply from 10.10.10.12: bytes=32 [illegible] TTL=128
Reply from 10.10.10.12: bytes=32 [illegible] TTL=128

Ping statistics for 10.10.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

C:\>
```

5. Assign cisco as the console password and enable console login access



```
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#passwordcisco
                        ^
% Invalid input detected at '^' marker.

R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd # Authorized Access Only ! #
R1(config)#end
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

TITLE :

Examining a Device's Gateway Understand and explain the purpose of a gateway address.

OBJECTIVE :

- Assign a device name to the router based on the topology and Addressing Table.
- Disable DNS lookup.
- Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
- Assign class as the privileged EXEC encrypted password.
- Assign cisco as the console password and enable console login access.
- Encrypt clear text passwords.

HARDWARE / SOFTWARE USED :

Cisco Packet Tracer

STEPS INVOLVED :

A default gateway address permits a network device to communicate with other devices on different networks. In essence, it is the door to other networks. All traffic destined to different networks must go through the network device that has the default gateway address.

Step 1: Configure a topology with atleast 2 switches so as to create two networks connected by a router

Step 2: Open a terminal window on a host computer.

Step 3: Use the ping command to verify connectivity with IP address 192.168.10.11.

a. Ping from PC-A to its default gateway (LOCAL's GigabitEthernet 0/1 interface).

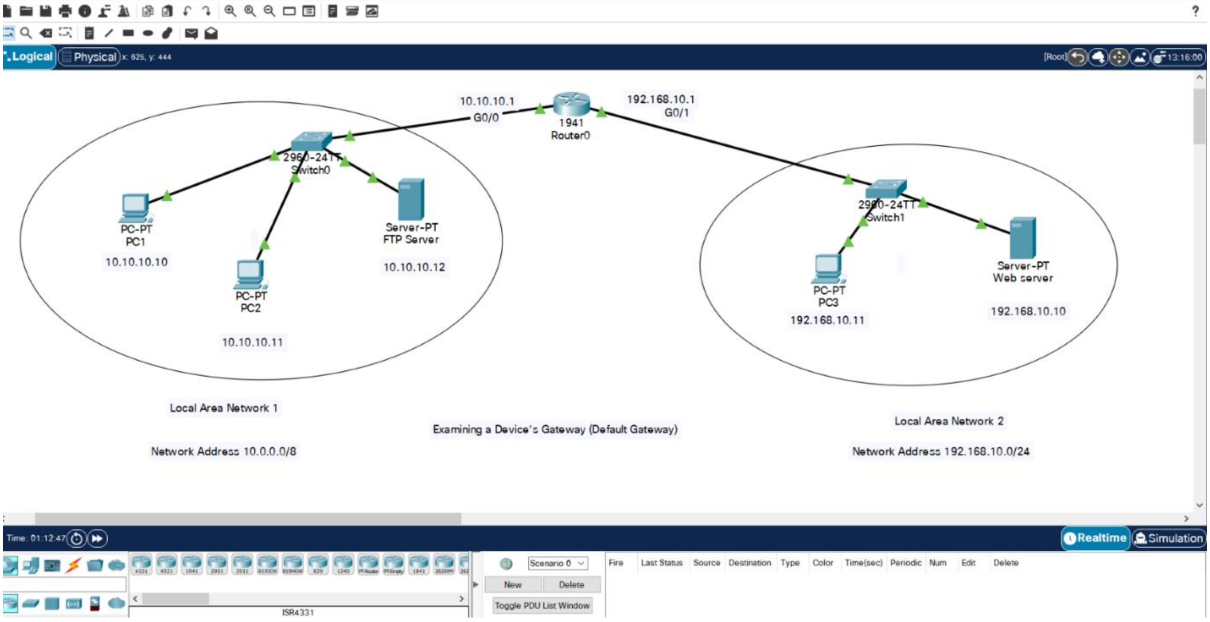
```
C:\Users\User1> ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

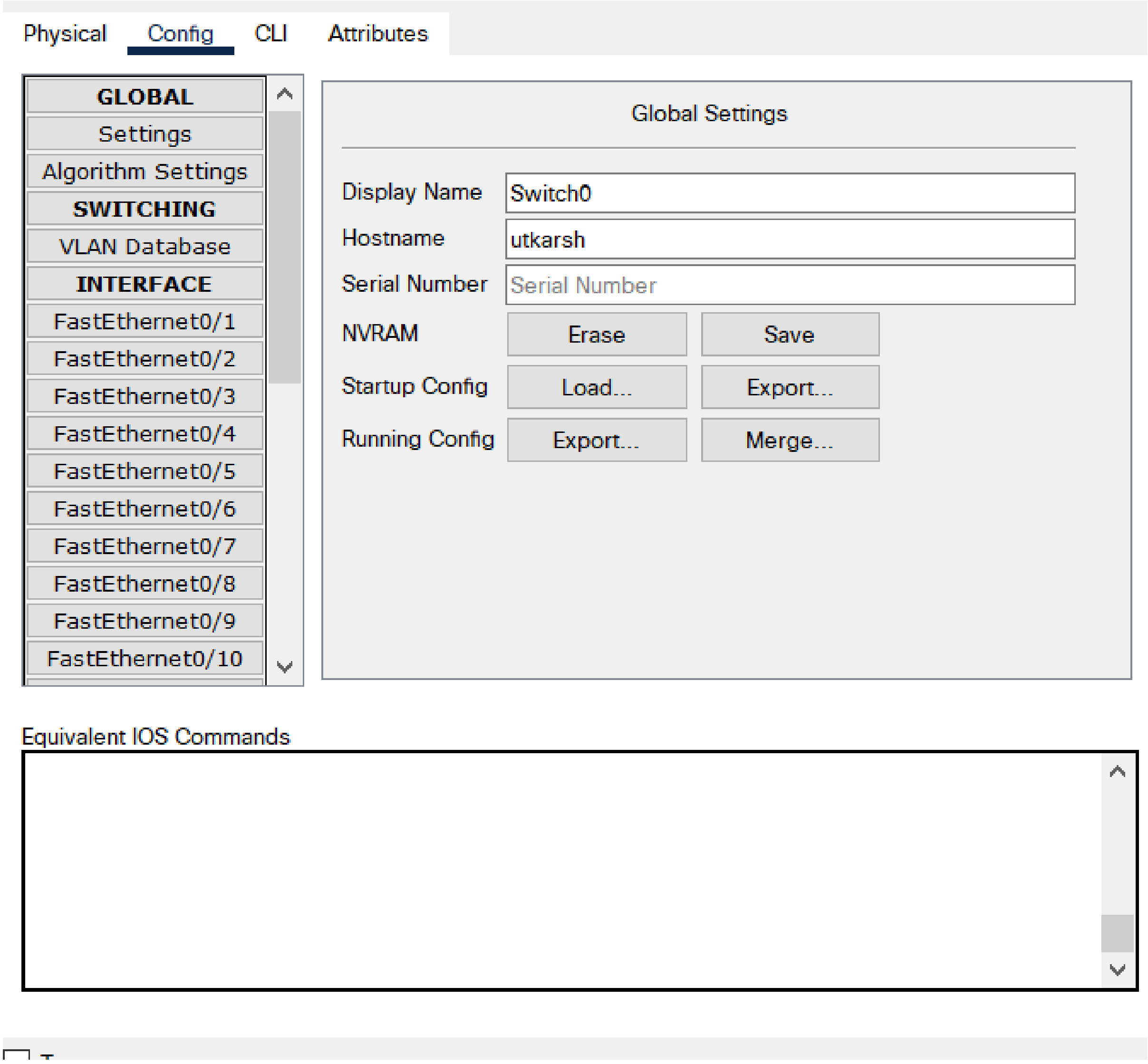
Step 4: Use the ping command to ping different IP addresses on the 192.168.10.0 network.

```
C:\Users\User1> ping 192.168.10.0
Pinging 192.168.10.0 with 32 bytes of data:
Reply from 192.168.10.0: bytes=32 time=41ms TTL=125
Reply from 192.168.10.0: bytes=32 time=41ms TTL=125
Reply from 192.168.10.0: bytes=32 time=40ms TTL=125
Reply from 192.168.10.0 bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

While the network is functioning correctly, the **ping** command can determine whether the destination responded and how long it took to receive a reply from the destination. If a network connectivity problem exists, the **ping** command displays an error message.

Output





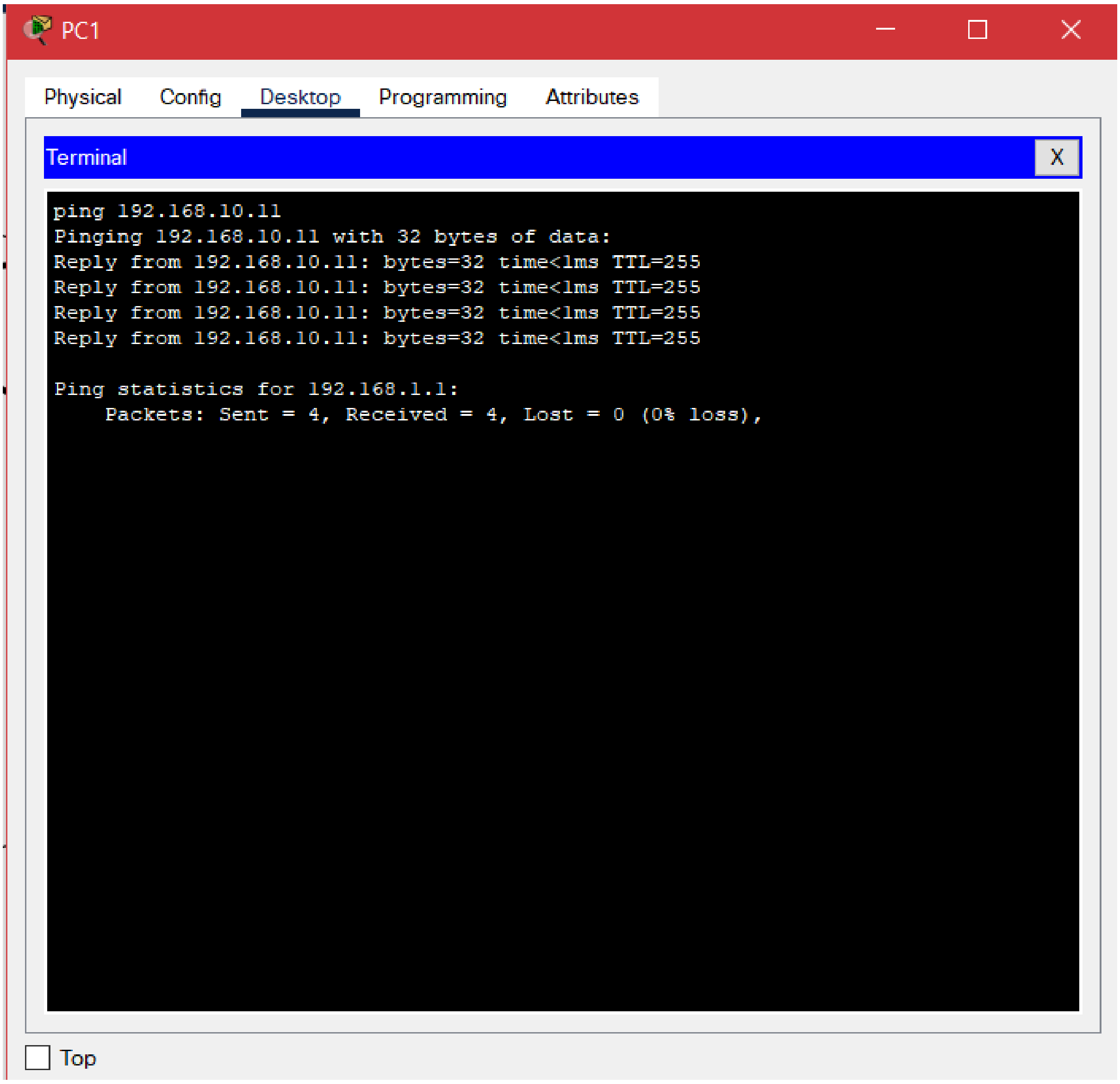
Global Settings

Display Name: Switch0

Hostname: utkarsh

Serial Number: Serial Number

Equivalent IOS Commands



```
ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255
Reply from 192.168.10.11: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Title:

Observing TCP and UDP using Netstat

Objectives:

Explain common netstat command parameters and outputs. Ping and Traceroute Use the ping command to verify simple TCP/IP network connectivity. Use the tracert/traceroute command to verify TCP/IP connectivity. (any topology). Perform basic settings also:

1. Assign a device name to the router based on the topology and Addressing Table.
2. Disable DNS lookup.
3. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
4. Assign **class** as the privileged EXEC encrypted password.
5. Assign **cisco** as the console password and enable console login access.

Encrypt clear text passwords.

Hardware/Software requirements: Cisco Packet Tracer

Procedure:

1. Create the topology with two PCs, one switch and a router.
2. Verify connectivity using net stat commands. Using *netstat –a* to see all available connections.
3. Ping PC B from PC A to verify connection using *ping 192.168.255.2*
4. *tracert 192.168.255.1* can be used to trace route to PC A from PC B
5. Assign a device name to the router based on the topology and Addressing Table. Using

hostname *Router* command

6. Disable DNS lookup. Using *no ip domain-lookup*
7. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited. Using *banner motd #Unauthorized access to this device is prohibited!#* in config mode.
8. Assign **class** as the privileged EXEC encrypted password. Using *enable password class* in config mode.
9. Assign **cisco** as the console password and enable console login access. Using *password cisco*

and then *login* in config mode.

10. Encrypt clear text passwords. Using *service password-encryption.*

Internal Assessment- ETN

Topic - Examining IPv4. Use Wireshark to capture and examine messages.

AIM: To capture packets using Wireshark and in that packet I will examine IPv4 protocol in Internet layer. My device is using TCP/IP protocol suite, So layer 3 will tell me about the Internet Protocol.

Resources:

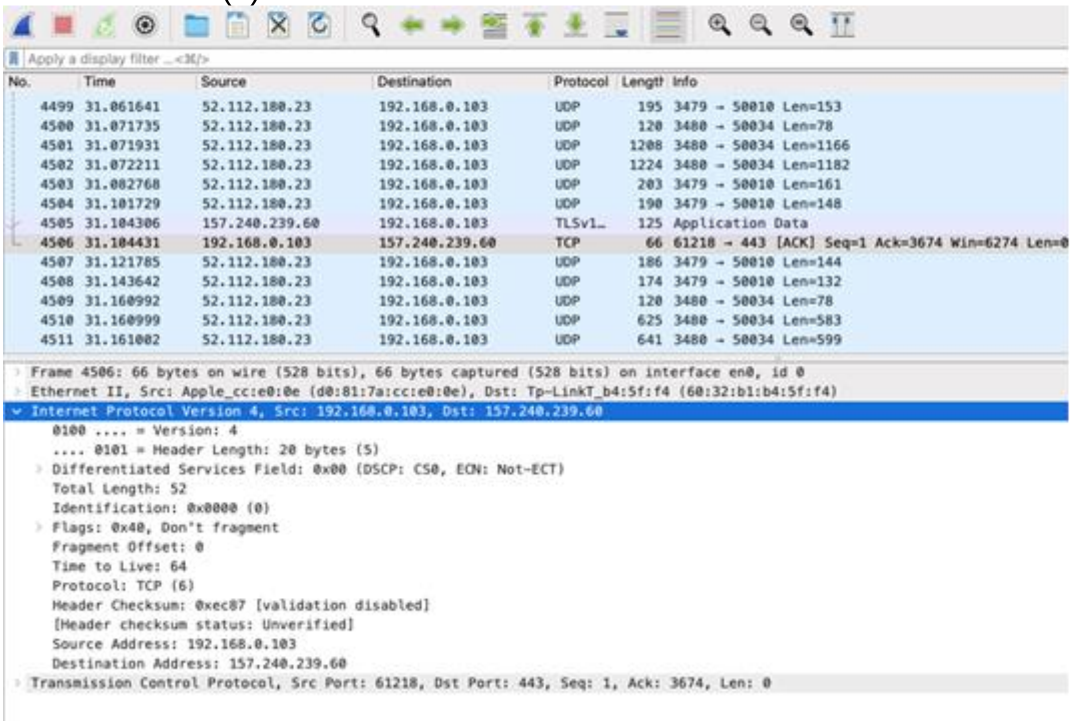
Software Used:

1- Wireshark version 3.4.8 (v3.4.8-0-g3e1ffae201b8) to capture packets/traffic on network.
2- macOS Big Sur
3- Processor:1.8 GHz Dual-Core Intel Core i5

Procedure/ step by step :
Step 1- Open Wireshark.
Step 2- Choose interface of which you want to capture. In my case it is Wi Fi en 0

Step 3- Open a packet and Annalise it.
Step 4- In layer 3 check internet protocol and Annalise it.

Result-
version= 0100 : Version 4
Source ip = 192.168.0.103
Destination ip=157.240.239.60
Header length= 0101 Version 4
Total length = 52
Identification= 0 X 0000(0)
Flags= 0X40, don’t fragment which means we don’t have to do fragmentation.
Fragment offset=0
Time to live or hop limit= 64
Protocol = TCP(6)



```
No.   Time       Source           Destination      Protocol Lengtł Info
 4499 31.061641  52.112.180.23    192.168.0.103    UDP       195 3479 → 50010 Len=153
 4500 31.071735  52.112.180.23    192.168.0.103    UDP       120 3480 → 50034 Len=78
 4501 31.071931  52.112.180.23    192.168.0.103    UDP      1208 3480 → 50034 Len=1166
 4502 31.072211  52.112.180.23    192.168.0.103    UDP      1224 3480 → 50034 Len=1182
 4503 31.082768  52.112.180.23    192.168.0.103    UDP       203 3479 → 50010 Len=161
 4504 31.101729  52.112.180.23    192.168.0.103    UDP       190 3479 → 50010 Len=148
 4505 31.104306  157.240.239.60   192.168.0.103    TLSv1…    125 Application Data
 4506 31.104431  192.168.0.103    157.240.239.60   TCP        66 61218 → 443 [ACK] Seq=1 Ack=3674 Win=6274 Len=0
 4507 31.121785  52.112.180.23    192.168.0.103    UDP       186 3479 → 50010 Len=144
 4508 31.143642  52.112.180.23    192.168.0.103    UDP       174 3479 → 50010 Len=132
 4509 31.160992  52.112.180.23    192.168.0.103    UDP       120 3480 → 50034 Len=78
 4510 31.160999  52.112.180.23    192.168.0.103    UDP       625 3480 → 50034 Len=583
 4511 31.161002  52.112.180.23    192.168.0.103    UDP       641 3480 → 50034 Len=599
```

```
> Frame 4506: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Apple_cc:e0:0e (d0:81:7a:cc:e0:0e), Dst: Tp-LinkT_b4:5f:f4 (60:32:b1:b4:5f:f4)
v Internet Protocol Version 4, Src: 192.168.0.103, Dst: 157.240.239.60
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xec87 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.103
    Destination Address: 157.240.239.60
> Transmission Control Protocol, Src Port: 61218, Dst Port: 443, Seq: 1, Ack: 3674, Len: 0
```

If there is no corruption, the result of summing the entire IP header, including checksum, should be zero. At each hop, the checksum is verified. Packets with checksum mismatch are discarded. The router must adjust the checksum if it changes the IP header (such as when decrementing the TTL)