Data Communication and Computer Networks

EEE314

Lab Manual

Name	
Registration Number	
Class	
Instructor's Name	

Lab # 01: Introduction to Networks and Networking Commands in Windows and Introduction to Packet Tracer

1. Objective:

The lab is intended to familiarize the students with the networking commands used in windows environment for debugging network related issues.

At the end of the lab the student must know:

- Local Loop Address and its purpose
- How to find IP address of a machine's NIC
- How to find MAC (Physical) address of machine's NIC
- Name Server lookup
- How to display arp table
- How to display routing table
- How to list the machines on the network
- How to find MAC address of a remote machine IP address
- How to find MAC address of a remote machine from host name

2. PreLab

2.1 OSI Model:

Open Systems Interconnection model (OSI model)l has a layered architecture. Model defines 7 layers. Each layer performs its specific task, hiding the details and complexities of its layer from other layers. Division of the bigger task into smaller subtasks makes it manageable and flexible. Protocol at any layer can be changed without affecting the other layers. Each layer takes and provides services to/from adjacent upper and lower layers.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing (IP-Address)
	Frame	2. Data link	Physical addressing (MAC-address)
	Bit	1. Physical	Media, signal and binary transmission

Figure 1. 1 OSI Model

2.2. Internet Protocol

The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (also known as network packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. It has the task of delivering datagrams from the source host to the destination host solely based on the addresses. For this purpose, IP defines datagram structures that encapsulate the data to be delivered. The first major version of IP, now referred to as Internet Protocol Version 4 (IPv4) is the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is in active, growing deployment worldwide.

2.3. IP Address:

An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6). The role of IP address has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates ho to get there."In IPv4 an address consists of 32 bits which limits the address space to 4294967296 (232) possible unique addresses.

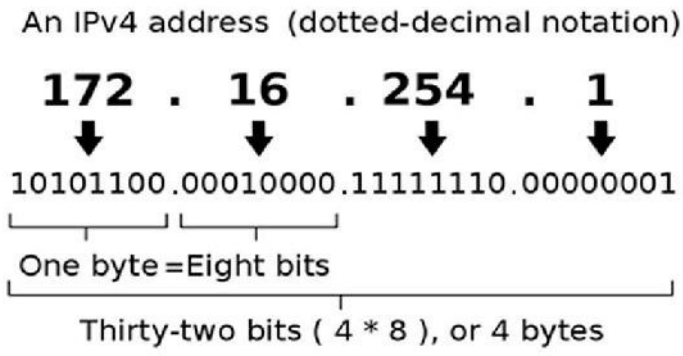


Figure 1. 2

This next generation of the Internet Protocol intended to replace IPv4 is IPv6 with 128 bits or 16 octets. That is 2128 or about 3.403×1038 unique addresses.

2.4. MAC Address:

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address or adapter address. A network node may have multiple NICs and will then have one unique MAC address per NIC. The standard (IEEE 802) format for printing MAC addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab). Another convention used by networking equipment uses three groups of four hexadecimal digits separated by dots (.) (e.g. 0123.4567.89ab).

2.5. Routing:

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network, electronic data networks (such as the Internet), and transportation (transport) networks in this course we are concerned primarily with routing in electronic data networks. Here routing is the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes; typically hardware devices called routers, bridges, gateways, or switches. Ordinary computers with multiple network cards can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the routers' memory, becomes very important for efficient routing.

2.6. Address Resolution Protocol:

In computer networking, the Address Resolution Protocol (ARP) is the method for finding a host's link layer (hardware) address when only its Internet Layer (IP) or some other Network Layer address is known. It is a request and reply protocol. It can be used to resolve many different network layer protocol addresses to interface hardware addresses, although, due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses.

2.7. Loop-back Address:

The term loopback (sometimes spelled loop-back) is generally used to describe methods or procedures of routing electronic signals, digital data streams, or other flows of items, from their originating facility quickly back to the same source entity without intentional processing or modification. This is primarily intended as a means of testing the transmission or transportation infrastructure. It is a virtual network interface implemented in software only and not connected to any hardware, but which is fully integrated into the computer system's internal network infrastructure. Any traffic that a computer program sends to the loopback interface is immediately received on the same interface. Correspondingly, the Internet Protocol (IP) specifies a loopback network. The most commonly used IP address on the loopback device is 127.0.0.1 for IPv4, although any address in the range 127.0.0.0 to 127.255.255.255 is mapped to it. IPv6 designates only a single address for this function, 0:0:0:0:0:0:0:1 (also written as ::1). The standard, officially reserved, domain name for these addresses is localhost. On Unix-like systems, the loopback interface usually has the device name lo or lo0.

3. Lab Task

Students are required to explore these commands. Through these commands students can accomplish the goals mentioned in section: “Objective”. Use the command prompt in windows or terminal window in linux.

3.1. Task1:

Run these commands and find out which command performs which of the above listed task

3.2. Task2:

Explore these commands and find out at least 5 new command options (switches)On your PCs open the command prompt (start - - run - and type cmd) and type the commands

1. ipconfig

Purpose: _____

Observation: _____

2. ipconfig / all

Purpose: _____

Observation: _____

3. ping <IP> e.g (C:\>ping 192.168.10.5)

Purpose: _____

Observation: _____

4. arp-a

Purpose: _____

Observation: _____

5. netstat -a

Purpose: _____

Observation: _____

6. net view

Purpose: _____

Observation: _____

7. tracert <hostname> e.g (C:\>tracert www.facefook.com)

Purpose: _____

Observation: _____

8. netstat -r

Purpose: _____

Observation: _____

9. nslookup

Purpose: _____

Observation: _____

10. nbtstat -n

Purpose: _____

Observation: _____

Hints:

- Use Windows Help (Press F1) or search the internet for more info about commands
- Add a question mark (?) after any command to get more info about it.
- If you are stuck in a command either type “exit” or press Ctrl+Break
- Replace <arguments> with actual values.

- **Part-2: Introduction to Packet Tracer**

Purpose:

The lab is intended to familiarize the students with a network classes and packet tracer simulator used to develop a network

Introduction to Packet Tracer:

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This "e-doing" capability is a fundamental component of learning how to configure routers and switches from the command line.

Steps to use Packet Tracer 5.1

After downloading you can install the software on your PC.

- **Step 1 - Start Packet Tracer And have A Look At The Interface**

The bottom left-hand corner of the Packet Tracer screen displays eight icons that represent device categories or groups, such as Routers, Switches, or End Devices.

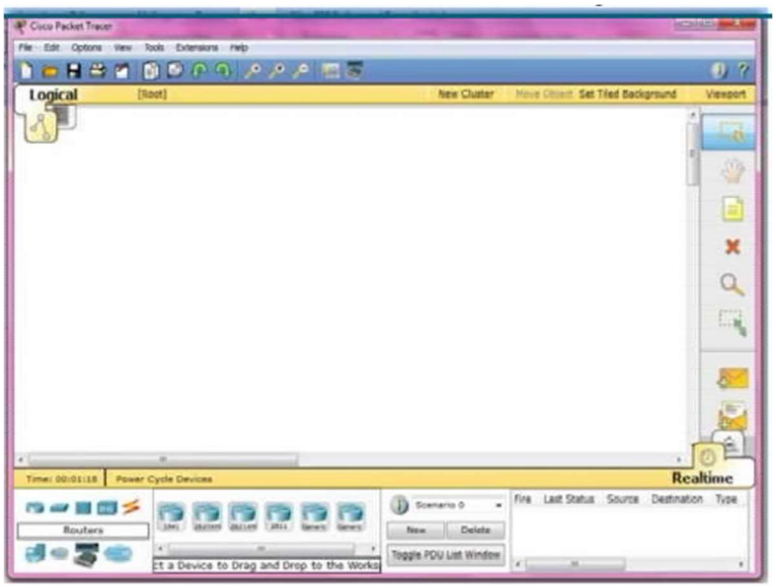


Figure 1. 3

Moving the cursor over the device categories will show the name of the category in the box. To select a device, first select the device category. Once the device category is selected, the options within that category appear in the box next to the category listings. Select the device option that is required. Select End Devices from the options in the bottom left-hand corner. Drag and drop two generic PCs onto the design area.

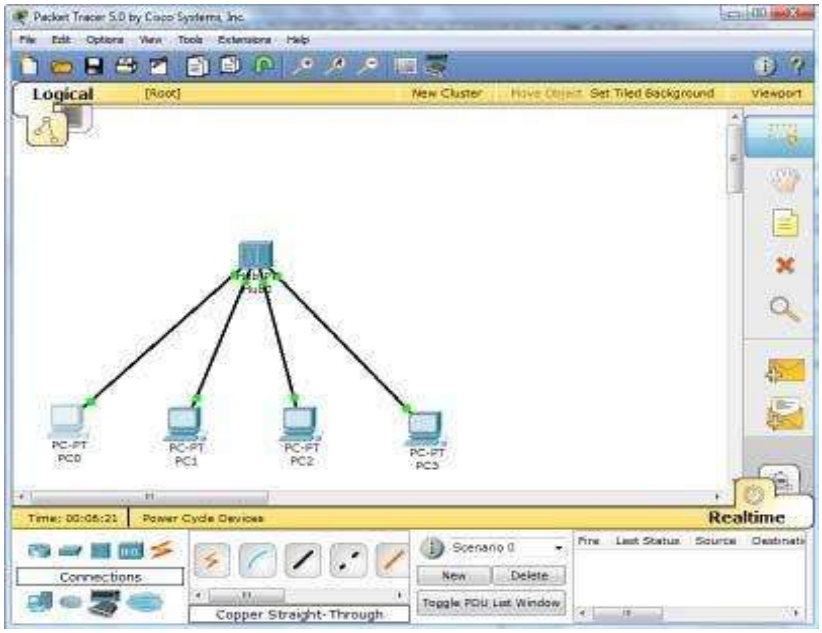


Figure 1. 4

- **Step 2 - Create A Logical Network Diagram With Four PCs And A Hub**

Select Hubs from the options in the bottom left-hand corner. Add a hub to the prototype network by dragging and dropping a generic hub onto the design area.

• Select End Devices from the options in the bottom left-hand corner. Add four PC:s to the prototype network by dragging and dropping them onto the design area.

• Select Connections from the bottom left-hand corner. Choose a Copper Straight-through cable type. Click the first host, PC0, and assign the cable to the FastEthernet connector. Click the hub, Hub0, and select a connection port, Port 0, to connect to PC0.

• Repeat the same steps for the second PC, PC1, to connect the PC to Port 1 on the hub.

• Repeat the same steps for the third PC, PC2, to connect the PC to Port 2 on the hub.

• Repeat the same steps for the last PC, PC3, to connect the PC to Port 3 on the hub.

There should be green dots at both ends of each cable connection. If not, check the cable type selected.

Step 3 - Configure The Hosts Attached To The Hub

• Configure host names and IP addresses on the PCs by clicking the PC0-icon. A PC0 window will appear.

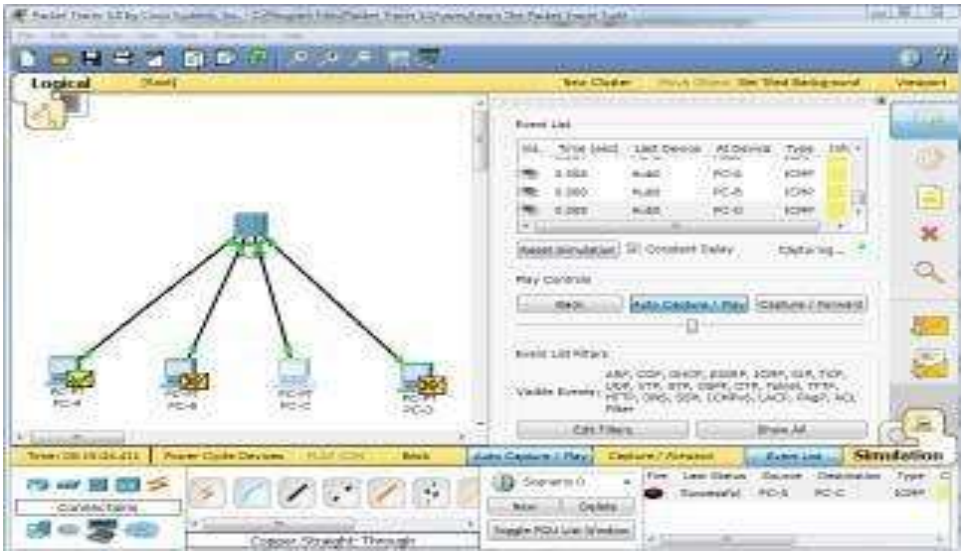


Figure 1

• From the PC0 window, select the Config tab. Change the PC Display Name to PC-A.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.1 and subnet mask of 255.255.255.0.

• Close the PC-A configuration window by selecting the x in the upper right-hand corner.

• Continue and configure PC1 by clicking on the PC1-icon.

• Select the Config tab. Change the PC Display Name to PC-B.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.2 and subnet mask of 255.255.255.0.

• Continue and configure PC2 by clicking on the PC2-icon.

• Select the Config tab. Change the PC Display Name to PC-C.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.3 and subnet mask of 255.255.255.0.

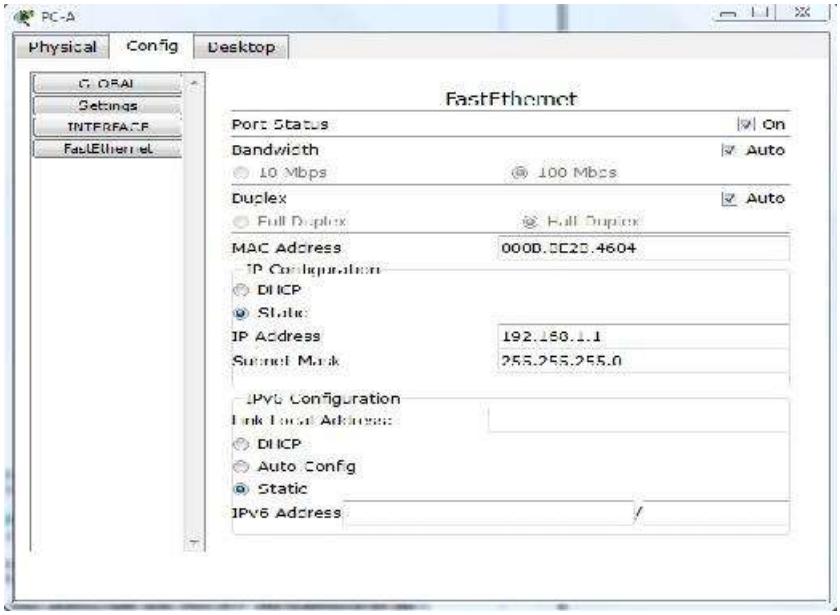
• Continue and configure PC3 by clicking on the PC3-icon.

• Select the Config tab. Change the PC Display Name to PC-D.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.4 and subnet mask of 255.255.255.0.

Step 4 - Run a Simulation of ICMP (ping)

• Switch to Simulation mode by selecting the tab that is partially hidden behind the Realtime tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.



• Click the Edit Filters button in the Event List Filters area. Clicking the Edit Filters button will create a popup window.

• In the pop-up window, click the Show All/None box to deselect every filter. Select just the ARP and ICMP filters.

• Select a Simple PDU by clicking the closed envelope on the right vertical toolbar.

• Move your cursor to the display area of your screen. Click PC-A to establish the source.

• Move your cursor to PC-C and click to establish the destination.

Notice that two envelopes are now positioned beside PC-A. One envelope is ICMP, while the other is ARP. The Event List in the Simulation Panel will identify exactly which envelope represents ICMP and which represents ARP.

• Select Auto Capture / Play from the Play Controls area of the Simulation Panel. Below the Auto Capture / Play button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging it to the left will slow down the simulation.

• Choose the Reset Simulation button in the Simulation Panel. Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries. The ARP request is not necessary to complete the ping command because PC-A already has the MAC address in the ARP table.

• Choose the Capture / Forward button. The ICMP envelope will move from the source to the hub and stop. The Capture / Forward button allows you to run the simulation one step at a time.

• Continue selecting the Capture / Forward button until you complete the event.

• Choose the Power Cycle Devices button on the bottom left, above the device icons.

An error message might appear asking you to confirm reset. Choose Yes. Now both the ICMP and ARP envelopes are present again. The Reset Network button will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.

Step 5 - View ARP Tables on Each PC

• Choose the Auto Capture / Play button to repopulate the ARP table on the PCs. Click OK when the No More Events message appears.

• Select the magnifying glass on the right vertical tool bar.

• Click PC-A. The ARP table for PC-A will appear. Notice that PC-A does have an ARP entry for PC-c. View the ARP table for PC-C. Close all ARP table windows.

• Click Select Tool on the right vertical tool bar. (This is the first icon present in the toolbar.)

• Click PC-A and select the Desktop tab.

• Select the Command Prompt and type the command arp -a and press enter to view the ARP table from the desktop view. Close the PC-A configuration window.

• Examine the ARP tables for the other PCs.

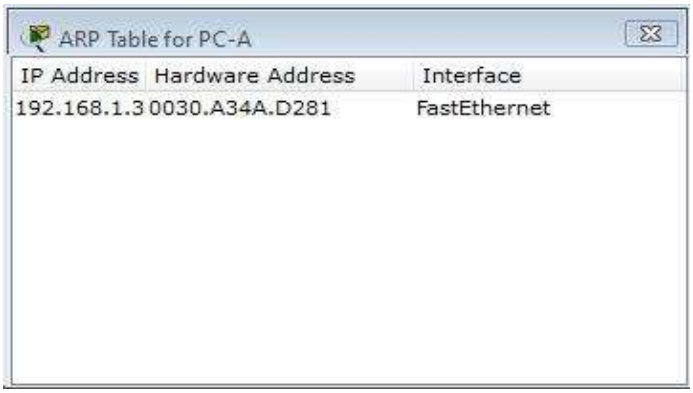
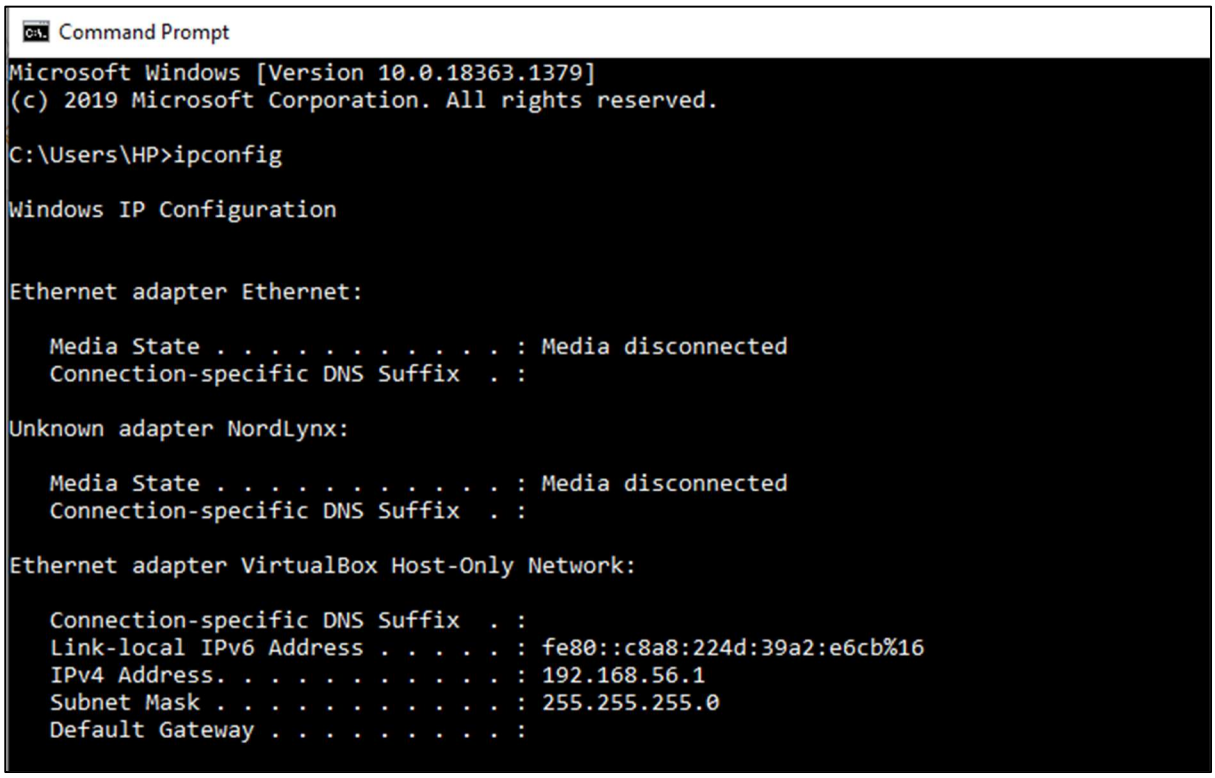


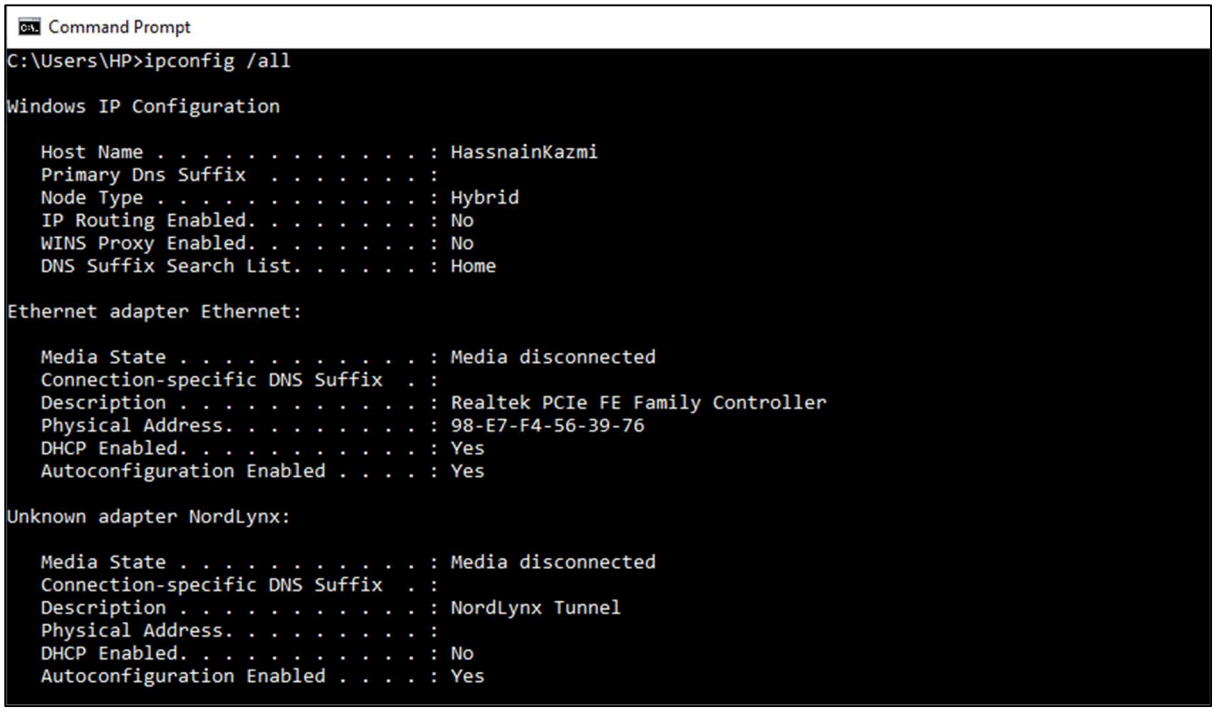
Figure 2

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Task 1:


Command Prompt
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\HP>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Unknown adapter NordLynx:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VirtualBox Host-Only Network:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c8a8:224d:39a2:e6cb%16
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :


Command Prompt
C:\Users\HP>ipconfig /all
Windows IP Configuration
Host Name . . . . . : HassnainKazmi
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Home
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe FE Family Controller
Physical Address. . . . . : 98-E7-F4-56-39-76
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Unknown adapter NordLynx:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : NordLynx Tunnel
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

```
C:\Users\HP>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\HP>arp -a

Interface: 192.168.1.2 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.1           f0-8c-fb-38-71-44     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x10
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
```

```
C:\Users\HP>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:445            HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:5040           HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:7070           HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:38000          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:39000          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49664          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49665          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49666          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49667          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49668          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49669          HassnainKazmi:0        LISTENING
  TCP    0.0.0.0:49675          HassnainKazmi:0        LISTENING
```

```
C:\Users\HP>net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
```

```
C:\Users\HP>tracert www.google.com

Tracing route to www.google.com [172.217.19.4]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2    34 ms    33 ms    33 ms  182.176.0.121
  3    36 ms    35 ms    34 ms  10.253.20.78
  4    49 ms    37 ms    33 ms  10.253.12.84
  5    58 ms    63 ms    66 ms  10.253.4.18
  6    80 ms    69 ms    63 ms  10.253.4.8
  7    73 ms    73 ms    71 ms  74.125.118.170
  8    73 ms    72 ms    73 ms  172.253.51.205
  9    72 ms    72 ms    72 ms  209.85.249.155
 10    72 ms    72 ms    72 ms  fjr02s08-in-f4.1e100.net [172.217.19.4]

Trace complete.
```

```
C:\Users\HP>netstat -r
===========================================================================
Interface List
 21...98 e7 f4 56 39 76 ......Realtek PCIe FE Family Controller
  9...........................NordLynx Tunnel
 16...0a 00 27 00 00 10 ......VirtualBox Host-Only Ethernet Adapter
 19...00 ff b4 32 73 76 ......TAP-NordVPN Windows Adapter V9
 22...30 e3 7a 22 66 32 ......Microsoft Wi-Fi Direct Virtual Adapter
 11...32 e3 7a 22 66 31 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...30 e3 7a 22 66 31 ......Intel(R) Dual Band Wireless-AC 3168
  1...........................Software Loopback Interface 1
===========================================================================
```

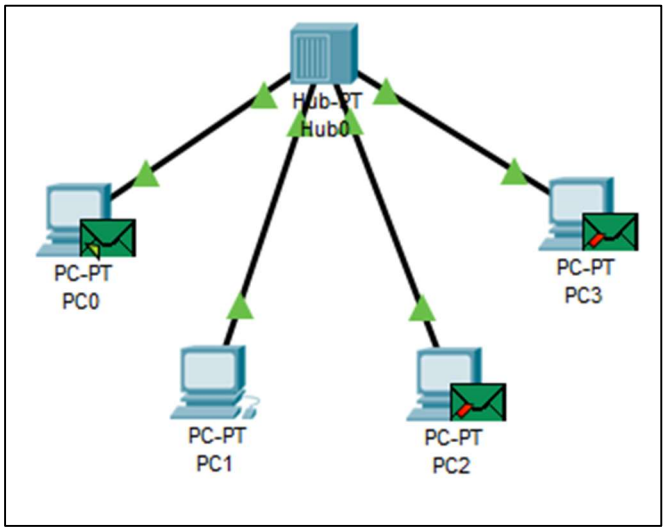
```
C:\Users\HP>nslookup
Default Server:  one.one.one.one
Address:  1.1.1.1

> www.youtube.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    wide-youtube.l.google.com
Addresses:  2a00:1450:400c:c0b::c6
          108.177.15.198
Aliases:  www.youtube.com
          youtube-ui.l.google.com
```

```
C:\Users\HP>nbtstat -n

Ethernet 3:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    HASSNAINKAZMI  <20>  UNIQUE      Registered
    HASSNAINKAZMI  <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

NordLynx:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

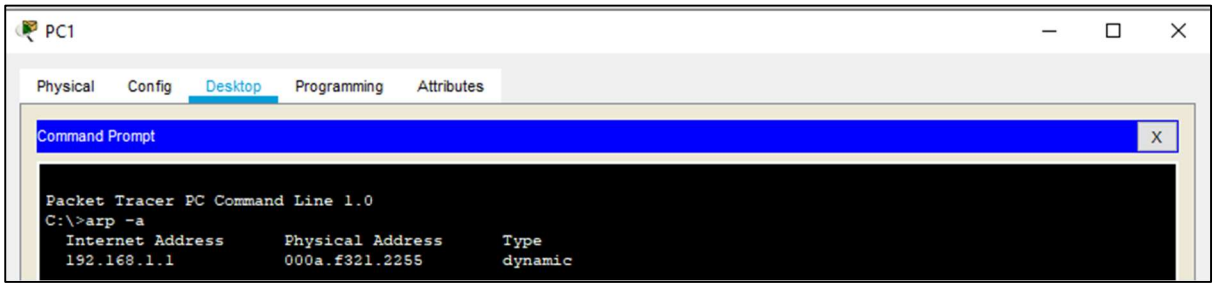
Task 2:

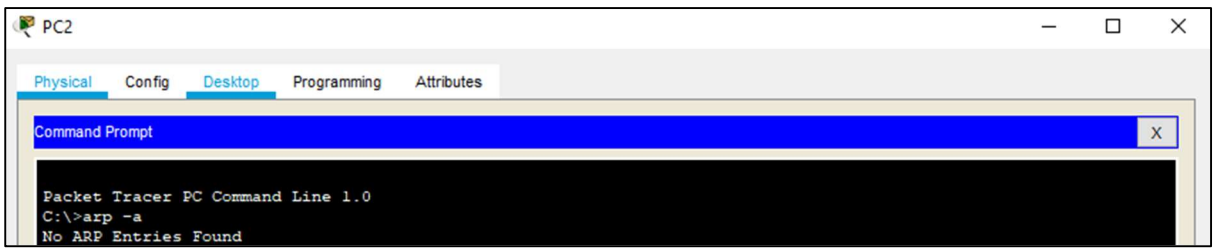
Source: PC0

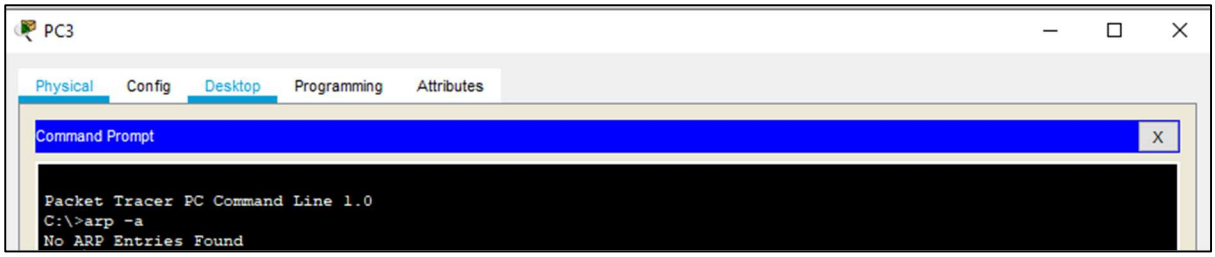
Destination: PC1



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC1	ICMP		0.000	N	0

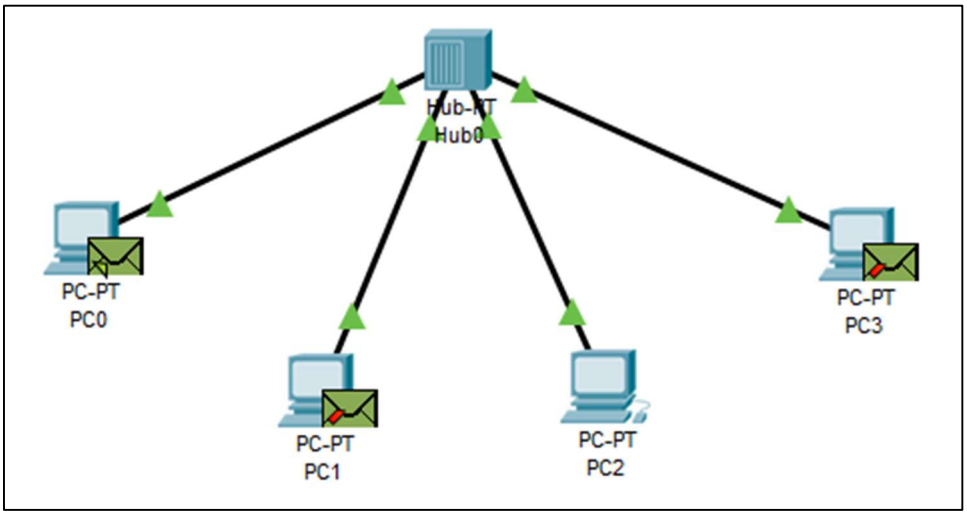




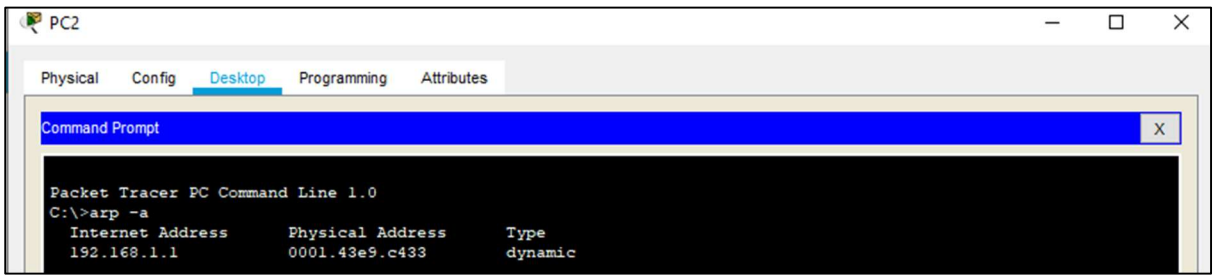


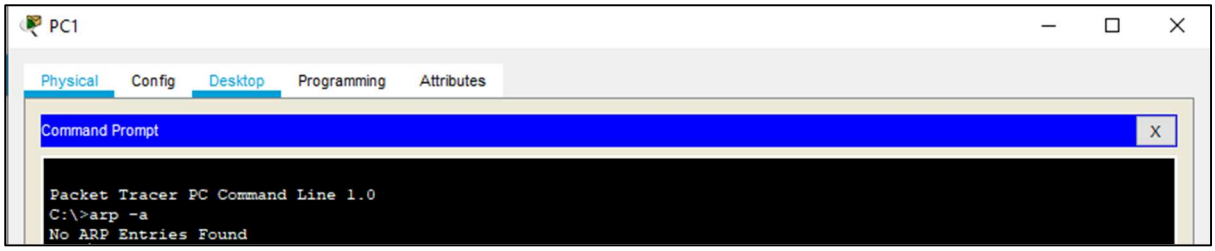
Source: PC0

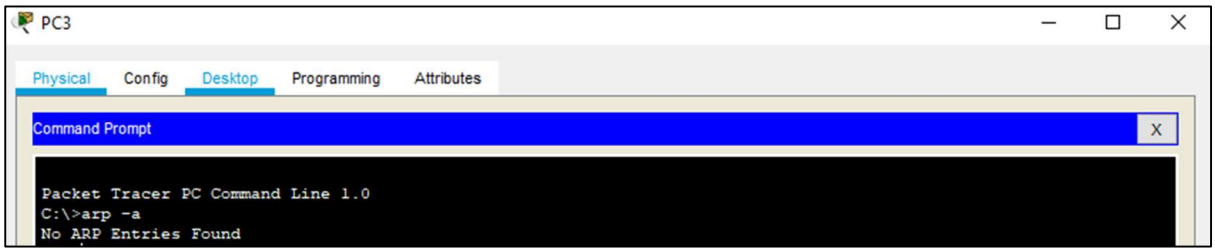
Destination: PC2



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC2	ICMP		0.000	N	0

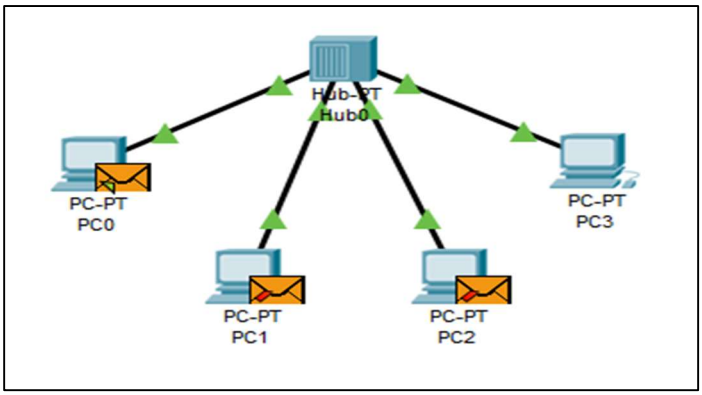




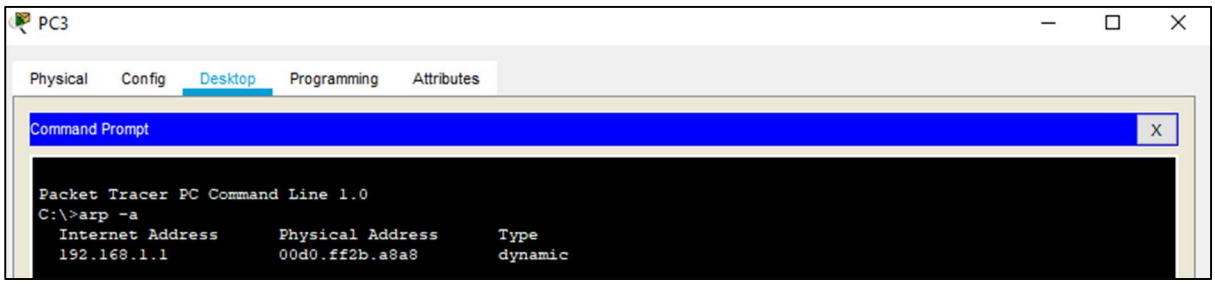


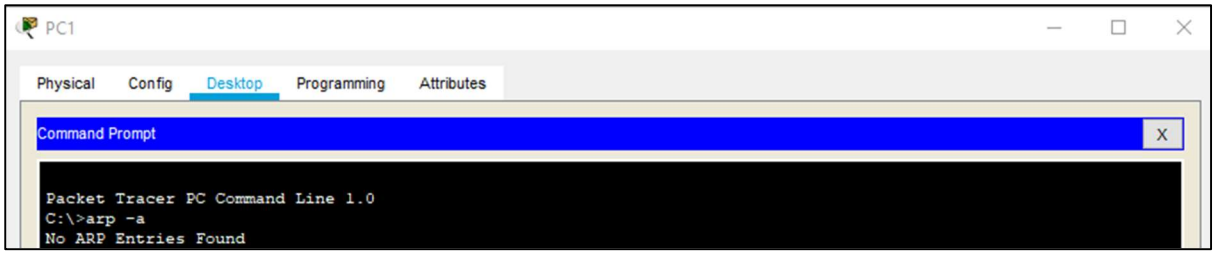
Source: PC0

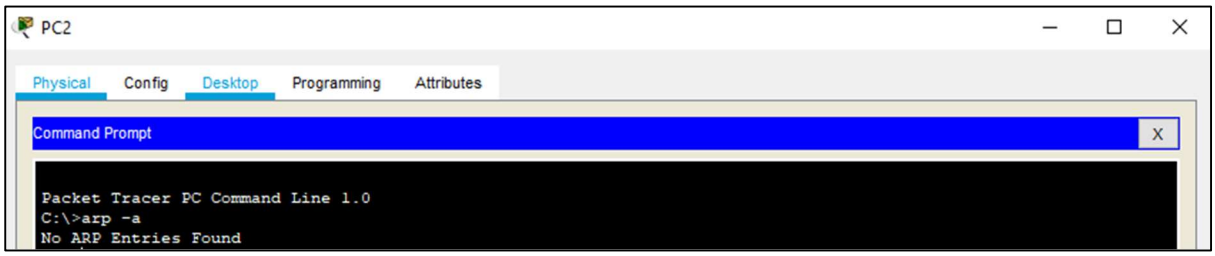
Destination: PC3



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC3	ICMP		0.000	N	0




PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found

Conclusion: