

LAB TWO – SINGLE SEGMENT

In this lab, you will learn how to use Wireshark, a software package to monitor link activity. You will also learn about ARP and how to configure the PCs. This lab uses the network configuration shown in Figure 2.2 for all parts.

Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 2.1. Configure the IP addresses for the PCs as shown in Table 2.1.

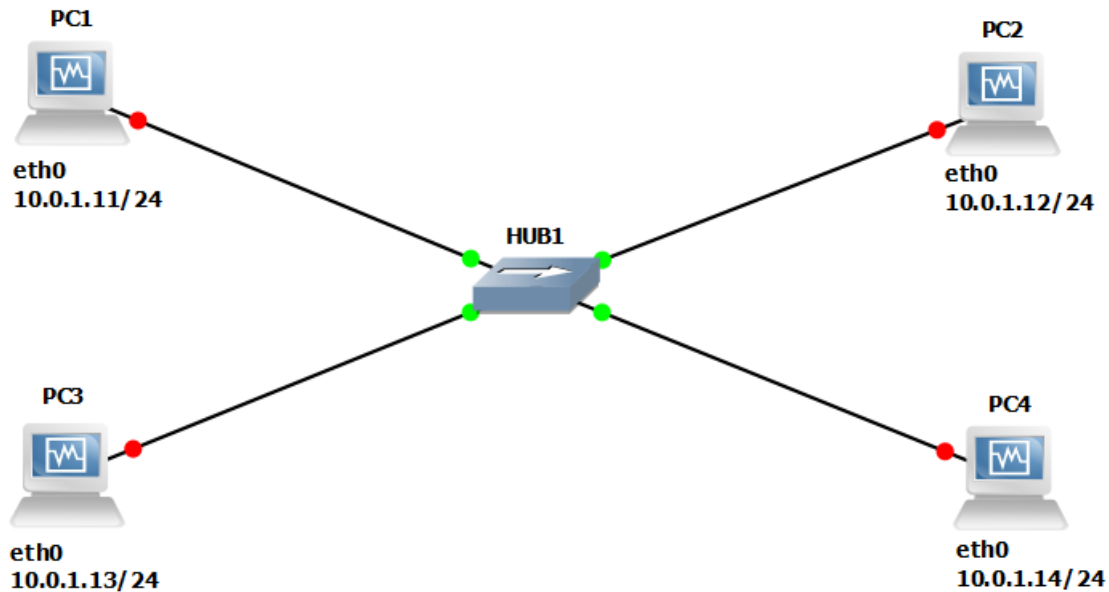


Figure 2.1 - Network Configuration for Lab 2.

VMS	IP Addresses of Ethernet Interface eth0
PC1	10.0.1.11 / 24
PC2	10.0.1.12 / 24
PC3	10.0.1.13 / 24
PC4	10.0.1.14 / 24

Table 2.1 - IP Addresses for Lab 2



Tip: Recall the following command to help you set up the IP addresses.

```
ifconfig interface_name A.B.C.D/XX
```

PART 1. Starting WIRESHARK

During the GNS3 installation process in Lab 1, you will automatically have installed Wireshark. For windows you do not need to download Wireshark. It comes automatically with the GNS3 installation. For Macs you are required to download it from the web ([here](#)). For Macs you also are required to download [X11](#). Wireshark will not work on a Mac without the X11 environment.

Make sure Wireshark is properly working by opening the Wireshark application on your computer. If Wireshark is not in your application folder, please download the appropriate version for your OS from the Internet.

- You have to set up four VMs on VirtualBox Manager if you haven't done so already. To do this, simply refer to Lab 1 (PART 3, Ex 3(A) Step 7-8). Make sure to have four VMs as shown in Figure 2.2.

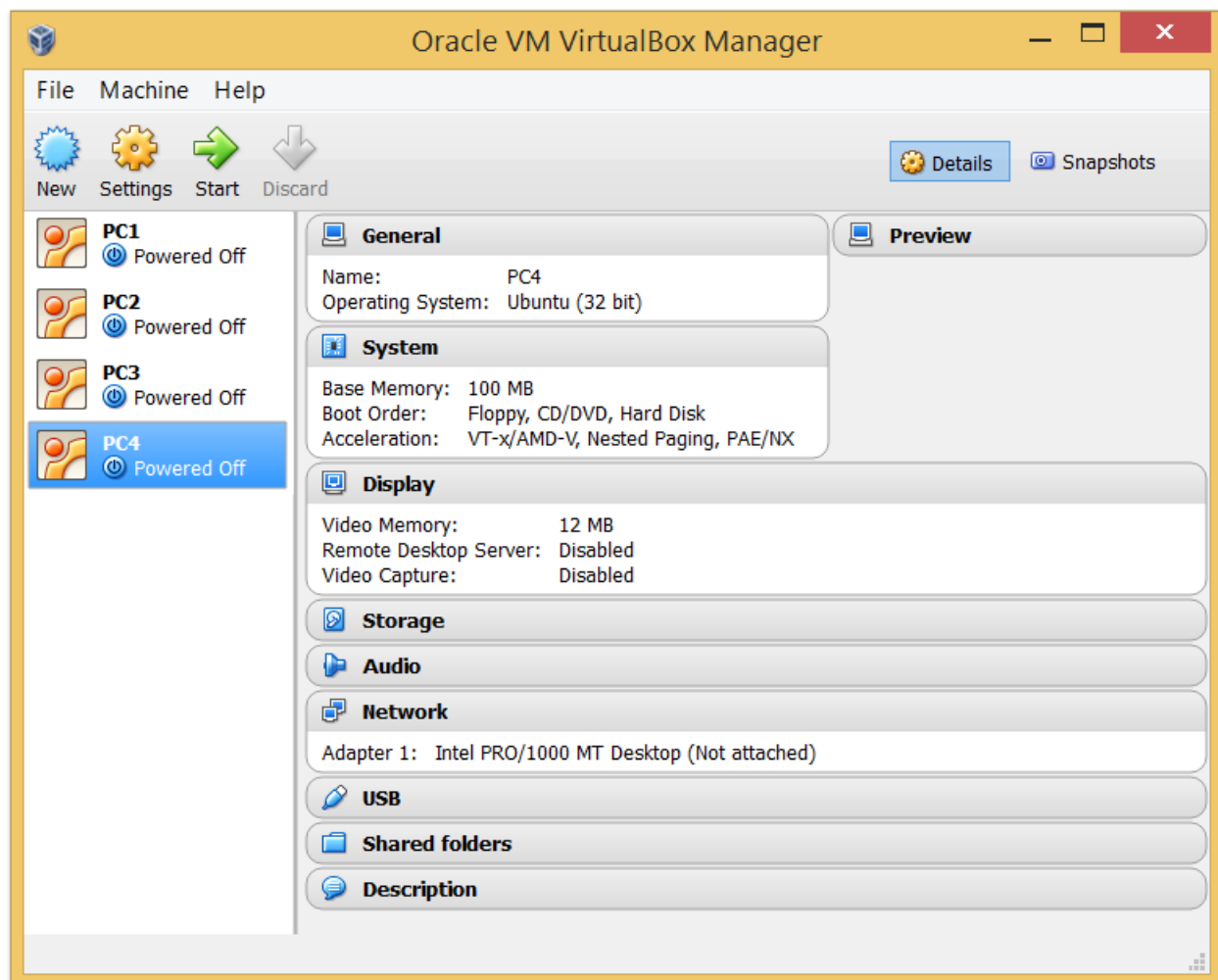


Figure 2.2 – VMs on VirtualBox Manager.

PART 2. Capturing Traffic using WIRESHARK

In this part of the lab, you experiment with filter expressions within the Wireshark application. The filtering capabilities and options of Wireshark are described under the help tab in Wireshark.

Exercise 1. Display filters and traffic capture with Wireshark

This exercise is mostly about the traffic capture process using Wireshark. You are introduced to the notion of capture filters.

1. Configure the network topology as shown in Figure 2.1 and configure the VMs' IP addresses with the values shown in Table 2.1.
2. Mouse right click on the link that connects PC1 and the Ethernet Hub and select "Start capture". **NOTE: Please choose the HUB side of the link for capturing, not the PC side.** Choose option Wireshark. It will initiate Wireshark and capture traffic on the link.
1. Please make sure that the Packet Capture settings are set to Wireshark Live Traffic Capture from Packet capture preferences section.

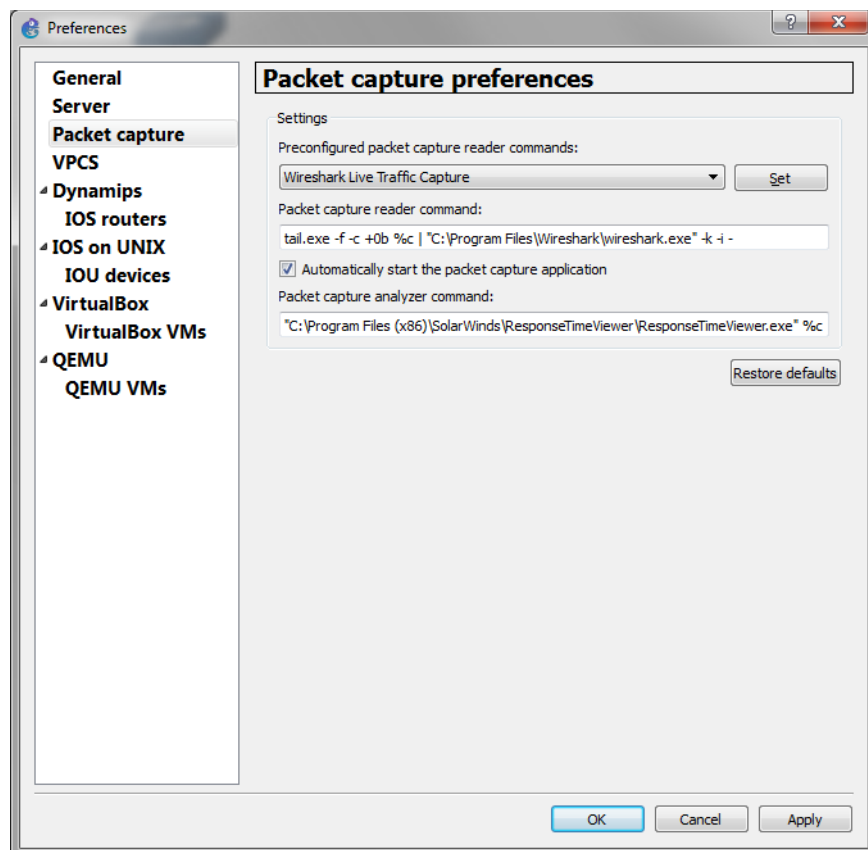


Figure 2.3 Packet capture Preferences

2. For Mac users the Wireshark does not open the capture file automatically, you need to open the \$HOME/GNS3/project folder. Then find the corresponding .pcap file in the *captures* folder. The initial size of this file will be 0. Once you start sending traffic the file will grow in size. You can open the file in Wireshark and it will keep refreshing the capture window while traffic is being captured.
3. **Setting a display filter:** From the command “Display Filters...” under the “Analyze” menu, you can set a display filter so that only the traffic that matches the filter is displayed. Set a filter so that all packets that contain the IP address of PC2 (10.0.1.12) are captured. Press “Enter/Return” after typing the filter.

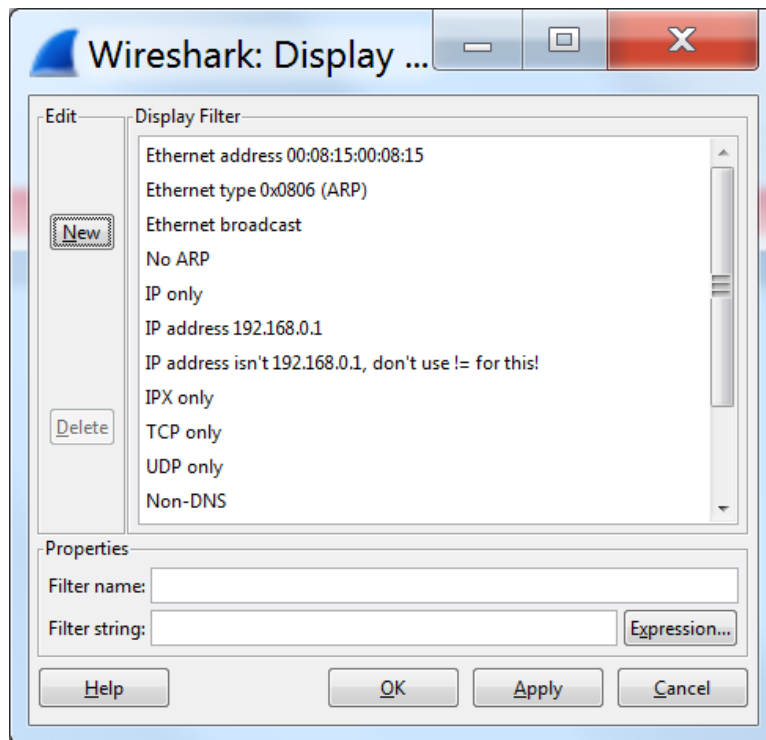


Figure 2.4 Display Filters command

4. You can also set a display filter by typing the desired display filter in the “Filter” box, which is found in the Wireshark main window as shown in Figure 2.5. Click the Clear button next to the filter box to clear any existing filter.



Figure 2.5 Filter box for setting display filters

5. In the terminal window of PC1, issue a ping command to PC2:

```
PC1% ping 10.0.1.12 -c 2
```

6. Stop the capture process.
7. **Saving captured traffic:** This is done by selecting the “Print” command in the “File” menu. Be sure Output to file option is checked. (Unless asked to save the details of captured frames, selecting the summary option is usually sufficient, uncheck Packet details unless you are required to display that.) See figure 2.6 below.

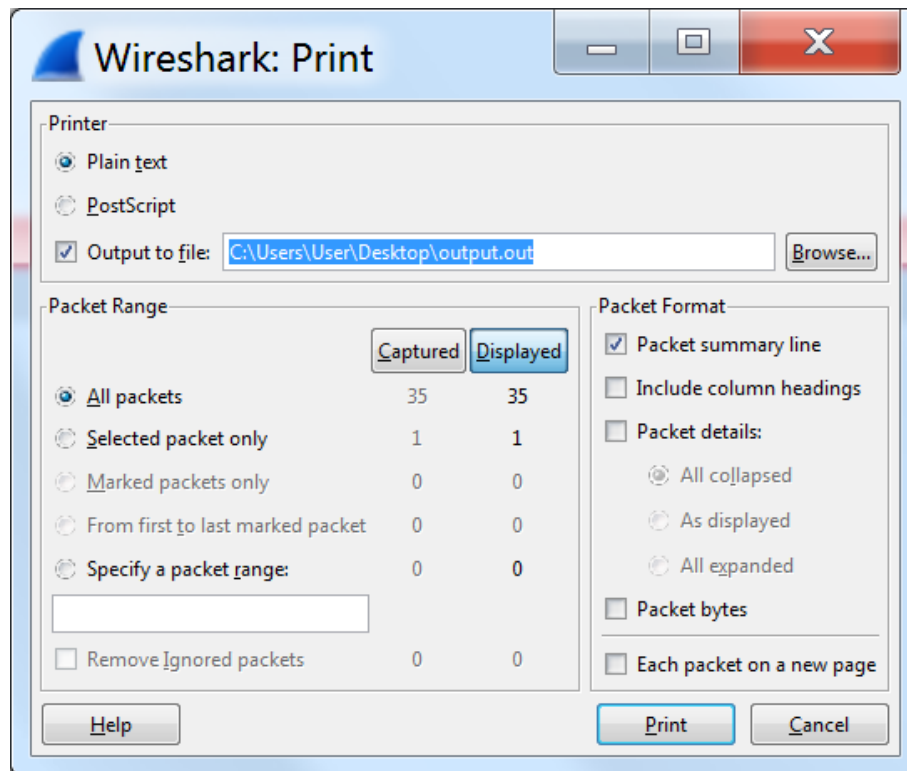


Figure 2.6 Print/Save Captured Traffic

PART 3. Address Resolution Protocol (ARP)

This part of the lab explores the operation of the Address Resolution Protocol (ARP) that resolves a MAC address for a given IP address. The lab exercises use the Linux command `arp`, for displaying and manipulating the contents of the ARP cache. The ARP cache is a table that holds entries of the form <IP address, MAC address>. The most common uses of the `arp` command are listed below.

COMMON USES OF THE ARP COMMAND

`arp -a`

Display the content of the ARP cache.

`arp -d IPaddress`

Deletes the entry with the IP address **IPaddress**.

`arp -s IPaddress MACaddress`

Adds a static entry to the ARP cache that is never overwritten by network events. The MAC address is entered as 6 hexadecimal bytes separated by colons.

Example: `arp -s 10.0.1.12 00:02:2D:0D:68:C1`



TIME-OUTS IN THE ARP CACHE

The entries in an ARP cache have a limited lifetime. Entries are deleted unless they are refreshed. The typical lifetime of an ARP entry is 2 minutes, but much longer lifetimes (up to 20 minutes) have been observed.



FLUSHING THE ARP CACHE

You also can clear the ARP cache with the following command

```
ip -s -s neigh flush all
```



REFRESHING THE ARP CACHE

In Linux you will observe that a host occasionally sends out ARP requests to interfaces that are already in the ARP cache.

Example: Suppose that a host with IP address 10.0.1.22 has an ARP cache entry:
`10.0.1.11 is at 08:00:27:53:63:1a`

Then, this host occasionally sends a unicast ARP Request to MAC
08:00:27:53:63:1a of the form:

`who has 10.0.1.11? Tell 10.0.1.22`

to verify that the IP address 10.0.1.11 is still present before deleting the entry from the ARP cache.

Exercise 3(A). A simple experiment with ARP

1. On PC1, view the ARP cache with `arp -a` and delete all entries with the `-d` option.
2. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address of PC2.
3. Issue a ping command from PC1 to PC2:

```
PC1% ping 10.0.1.12 -c 2
```

Observe the ARP packets in the Wireshark window. Explore the MAC addresses in the Ethernet headers of the captured packets.

Direct your attention to the following fields:

- The destination MAC address of the ARP Request packets.
 - The Type Field in the Ethernet headers of ARP packets and ICMP messages.
4. View the ARP cache again with the command `arp -a`. Note that ARP cache entries can get refreshed/deleted fairly quickly (~2 minutes).

```
PC1% arp - a
```

5. Save the results of Wireshark to a text file, using the “Packet details” option in “Print”.

Lab Questions

- What is the destination MAC address of an ARP Request packet?
- What are the different Type Field values in the Ethernet headers that you observed?
- Use the captured data to analyze the process in which ARP acquires the MAC address for IP address 10.0.1.12.

Exercise 3(B). Matching IP addresses and MAC addresses

Identify the MAC addresses of all the interfaces connected to the network, and enter them in Table 2.2. You can obtain the MAC addresses from the ARP cache of a PC by issuing a `ping` command from that host to every other host on the network. Alternatively, you can obtain the MAC addresses from the output of the `ifconfig` command in the console window of each PC.

VMS	IP Address of eth0	MAC address of eth0
PC1	10.0.1.11 / 24	
PC2	10.0.1.12 / 24	
PC3	10.0.1.13 / 24	
PC4	10.0.1.14 / 24	

Table 2.2. IP and MAC addresses.

Exercise 3(C). ARP requests for a non-existing address

Observe what happens when an ARP Request is issued for an IP address that does not exist.

1. Start Wireshark on PC1-Hub1 link with a capture filter set to capture packets that contain the IP address of PC1.
2. Issue a ping command from PC1 to 10.0.1.22. (Note that this address does not exist in this network.)

```
PC1% ping 10.0.1.22 -c 10
```

3. Save the captured output.

Lab Questions

- Using the saved output, describe the time interval between each ARP Request packet issued by PC1. Observe the method used by ARP to determine the time between retransmissions of an unsuccessful ARP Request.
- Why are ARP Request packets not transmitted (i.e. not encapsulated) as IP packets?

PART 4. The NETSTAT Command

The Linux command `netstat` displays information on the network configuration and activity of a Linux system, including network connections, routing tables, interface statistics, and multicast memberships. The following exercise explores how to use the `netstat` command to extract different types of information about the network configuration of a host. This list shows four important uses of the `netstat` command.

```
netstat -i
    Displays a table with statistics of the currently configured network
    interfaces.

netstat -rn
    Displays the kernel routing table. The -n option forces netstat to
    print the IP addresses. Without this option, netstat attempts to
    display the host names.

netstat -an
netstat -tan
netstat -uan
    Displays the active network connections. The -a option display all
    active network connections, the -ta option displays only information on
    TCP connections, and the -tu option displays only information on UDP
    traffic. Omitting the -n option prints host names, instead of IP
    addresses.

netstat -s
    Displays summary statistics for each protocol that is currently running
    on the host.
```

Exercise 4. Using netstat commands

1. Display information on the network interfaces by typing

```
PC1% netstat -in
```

2. Display the content of the IP routing table by typing

```
PC1% netstat -rn
```

3. Display information on TCP and UDP ports that are currently in use by typing

```
PC1% netstat -a
```

4. Display the statistics of various networking protocols by typing

```
PC1% netstat -s
```

**NOTE**

The values of the statistics displayed by some of the `netstat` commands are reset each time a host is rebooted. Therefore, if you are doing this exercise immediately after rebooting the VM, the output of `netstat` may not be very useful.

Lab Questions

Using the `netstat` output, answer the following questions.

- What are the network interfaces of PC1 and what are the MTU (Maximum Transmission Unit) values of the interfaces?
- How many IP datagrams, ICMP messages, UDP datagrams, and TCP segments has PC1 transmitted and received since it was last rebooted.
- Explain the role of interface `lo`, the loopback interface. In the `netstat -in` output, why are the values of RX-OK (packets received) and TX-OK (packets transmitted) different for interface `eth0` but identical for interface `lo`?

PART 5. Configuring IP Interfaces in LINUX

The `ifconfig` command is used to configure parameters of network interfaces, including enabling and disabling interfaces and setting the IP address. The `ifconfig` command is usually run when a system boots up. In this case, the parameters are read from a file. Once the Linux system is running, the `ifconfig` command can be used to modify the network configuration parameters. This list shows how `ifconfig` is used to query the status of network interfaces.

```
ifconfig
    Displays the configuration parameters of all active interfaces.

ifconfig interface
    Displays the configuration parameters of a single interface. For
    example, ifconfig eth0 displays information on interface eth0.

ifconfig eth0 down
    Disables the eth0 interface. No traffic is sent or received on a
    disabled interface.

ifconfig interface up
    Enables an interface.

ifconfig eth0 10.0.1.8 netmask 255.255.255.0 broadcast 10.0.1.255
    Assigns interface eth0 the IP address 10.0.1.8/24 and a broadcast
    address of 10.0.1.255.
```

Exercise 5. Changing the IP address of an interface

1. On PC4, run `ifconfig` and screenshot the output.
2. Change the IP address of interface `eth0` of PC4 to `10.0.1.11/24`.
3. Run `ifconfig` again and screenshot the output.



Tip: If you are not able to screenshot all the output on the screen (too much data), you should use the command `ifconfig interface` for each interface so that you can capture each one separately.

Lab Questions

- Explain the fields of the `ifconfig` output.

PART 6. DUPLICATE IP Addresses

In this part of the lab, you observe the effects of having more than one host with the same (duplicate) IP address in a network. After completing Exercise 5, the IP addresses of the Ethernet interfaces on the four PCs are as shown in table 2.3 below. Note that PC1 and P4 are assigned the same IP address.

VMS	IP Address of eth0
PC1	10.0.1.11 / 24
PC2	10.0.1.12 / 24
PC3	10.0.1.13 / 24
PC4	10.0.1.11 / 24

Table 2.3. IP addresses.

Exercise 6

1. Delete all entries in the ARP cache on all PCs.
2. Run Wireshark on PC3-Hub1 link and capture the network traffic to and from the duplicate IP address 10.0.1.11.
3. From PC3, issue a ping command to the duplicate IP address, 10.0.1.11, by typing

```
PC3% ping 10.0.1.11 -c 5
```

4. Stop Wireshark, save all ARP packets and screenshot the ARP cache of PC3 using the arp -a command:

```
PC3% arp - a
```

5. When you are done with the exercise, reset the IP address of PC4 to its original value as given in Table 2.1.

Lab Questions

- Explain how the ping packets were issued by the hosts with duplicate addresses.
- Did the ping command result in error messages?
- How can duplicate IP addresses be used to compromise the data security?
- Give an example. Use the ARP cache and the captured packets to support your explanation.

PART 7. Changing NETMASKS

In this part of the lab, you test the effects of changing the netmask of a network configuration. In the table below, two hosts (PC2 and PC4) have been assigned different network prefixes.

Exercise 7. Setting different IP address masks

1. Setup the interfaces of the hosts as follows:

VMS	IP Address of eth0	Network Mask
PC1	10.0.1.100 / 24	255.255.255.0
PC2	10.0.1.101 / 28	255.255.255.240
PC3	10.0.1.120 / 24	255.255.255.0
PC4	10.0.1.121 / 28	255.255.255.240

Table 2.4 IP addresses for Part 7.

2. Run Wireshark on PC1-Hub1 link and capture the packets for the following scenarios

- a. From PC1 ping PC3: `PC1% ping 10.0.1.120 -c 1`
- b. From PC1 ping PC2: `PC1% ping 10.0.1.101 -c 1`
- c. From PC1 ping PC4: `PC1% ping 10.0.1.121 -c 1`
- d. From PC4 ping PC1: `PC4% ping 10.0.1.100 -c 1`
- e. From PC2 ping PC4: `PC2% ping 10.0.1.121 -c 1`
- f. From PC2 ping PC3: `PC2% ping 10.0.1.120 -c 1`

3. Save the Wireshark output to a text file (using the “Packet Summary” option from “Print”), and save the output of the ping commands. Note that not all of the above scenarios are successful. Save all the output including any error messages.
4. When you are done with the exercise, reset the interfaces to their original values as given in Table 2.1. (Note that /24 corresponds to network mask 255.255.255.0. and /28 to network mask 255.255.255.240.)

Lab Questions

- Use your output data and ping results to explain what happened in each of the ping commands.
- Which ping operations were successful and which were unsuccessful? Why?

PART 8. Static Mapping of IP Addresses and Host Names

Since it is easier to memorize names than IP addresses, there are mechanisms to associate a symbolic name, called *hostname*, with an IP address. The term hostname is ambiguous on multi-homed systems, since a system can have one hostname for each network interface.

On the Internet, the resolution between hostnames and IP addresses is generally done by the Domain Name System (DNS), which is the topic of Lab 8. This experiment illustrates another, simpler method to map IP addresses and domain names using the host file `/etc/hosts`.

Before DNS became available, the `/etc/hosts` file was the only method to resolve hostnames in the Internet. All hosts on the Internet had to occasionally synchronize with the content of other `/etc/hosts` files.

Exercise 8. Associating names with IP addresses

In this exercise, you manipulate the static mapping of hostnames and IP addresses using the `/etc/hosts` file.

1. On PC1, inspect the content of file `/etc/hosts` with `vi`.

```
PC1% vi /etc/hosts
```

Linux has a wide variety of editors that can be used to modify text files. The native text editor for Ubuntu is `vi`. The UNIX `vi` editor has two modes of operation, **command** and **insert modes**. The command mode takes actions such as saving and quitting from a file, and the insert mode permits the insertion of characters. To get in the insert mode, press `i` and enter with the characters in the line, and to exit from the insert mode and enter in the command mode, press `esc` as long as the text editor is on insert mode.



Quitting from and saving a file

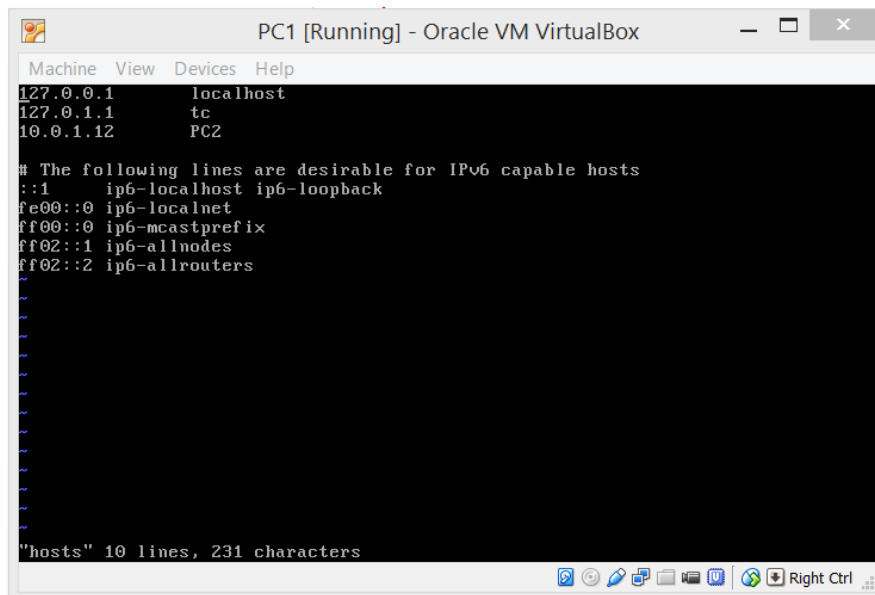
In command mode, type `:q!` to quit from a file and not to save any edits. Type in command mode `:wq` to save a file and exit from the text editor.

2. On PC1, issue a `ping` command to PC2.

```
PC1% ping 10.0.1.12 -c 5
```

3. Repeat Step 2, but use symbolic names instead of IP addresses (e.g., PC2 instead of 10.0.1.12). You should see that the symbolic name is unreachable at this point.

- On PC1, edit the file `/etc/hosts` and associate hostnames with the IP addresses of the 4 PC's and save the changes. Use the names PC1, PC2, etc., as used throughout this lab to refer to the PCs. For example, PC2 information should be inserted as shown in Figure 2.6.



```
127.0.0.1    localhost
127.0.1.1    tc
10.0.1.12    PC2

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

"hosts" 10 lines, 231 characters
```

Figure 2.7 How to insert PC2 information on `/etc/hosts` from PC1

- You should now be able to ping directly using PC2, PC3, and PC4, as in

```
PC1% ping PC2 -c 5
PC1% ping PC3 -c 5
PC1% ping PC4 -c 5
```

- Reset the `/etc/hosts` file to its original state. That is, remove the changes you have made in this exercise, and save the file.



Deleting characters on vi

On command mode, go to the character you want to delete and press `d` and then the right arrow `→` or the left arrow `←`. To delete the whole line press `d` two times.