Transport and Network Layer Protocols Lab

TCP/IP

Name: ____

Date Experiment Performed: ______________________

Group Members:

____

____

____

PART I: Internet Protocol (IP)

Objective

Internet Protocols are the core of the Internet and it is necessary to understand how these protocols work together.

1. Understand the configuration of IP in LANs. Identify the IP address, physical address, subnet mask, the DHCP server that provide the IP address of a host computer, and to determine when the lease for that address was obtained and when it will expire.
2. Experiment with Domain Name Services; discover host names and DNS servers.
3. Experiment with ARP and IP Routing and understand the results with respect to network topology.

Descriptive overview

This document provides an overview to the laboratory experiment sessions for the TCP/IP lab. This overview and the suggested readings should be completed before beginning the lab since lab time is limited. We suggest that students bring the course textbook to the lab. Though our lab experiments will be carried out in Windows XP environment, most of the materials here should be independent of the operating system. Knowledge of basic Windows commands and features would be helpful.

IP header format

1				16
	IHL	Type of service	Total length	
Identification			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Option + Padding				
Data				

Exercise 1: Host IP configuration

This exercise focuses on basic IP configurations of a single host. Use the "**ipconfig**" utility to observe and list: Physical address (MAC address), IP address, Subnet Mask, Default Gateway, IP address of the DHCP server, when was the lease for the IP address obtained, when will the lease expire. Open a command window and type:

```
>ipconfig /all
```

Do it again on a different host on different subnets and fill out Table 1. Familiarize yourself with the topology of the lab network and draw a picture of the lab network; show how it is connected and what IP addresses are assigned to the network interfaces.

	Host on LAN1	**Host on LAN2**	**Host on LAN3**
MAC address			
IP address			
Subnet Mask			
Default Gateway IP address			
DHCP Server IP address			
Lease obtained			
Lease expires			

Table1: Using the ipconfig utility

Exercise 2: Network configuration and connection status

"**Ping**" is a utility that sends an ICMP echo message to another host on the network and receives a message back to let you know that your computer is communicating with other devices on the network. If a computer is not able to connect to a particular host or to another network, the ping utility is used as a troubleshooting tool to determine where the network communication is failing. You should see a message that tells you that the other computer is responding to your ping request. Use ping utility to check the connection status through the following steps:

On a command prompt type:

>ping *ip address or hostname*

The network IP address allocation will be drawn on the whiteboard.

1. Ping your own host.
2. Ping your neighbor on the same subnet
3. Ping one host on a different subnet
4. *Ping WebServer(10.1.1.4)*
5. Ping a host that is shut down (*20.20.20.20*)

Compare, analyze the result and explain every field of the output of **step 4** above in the space provided below.

Sent	**Received**	**Lost**	**Round trip times(ms)**		
			Min	**Max**	**Avg**

Table 2 Ping table

Exercise 3: Domain Name System (DNS)

The “**nslookup”** utility allows you to query DNS servers and display the mapping from IP addresses to hostnames. Before using this tool, you should be familiar with how DNS works. Nslookup works in interactive or non-interactive mode.

Determine the local hostname of your machine by typing the following:

>hostname

Write down your local hostname here: ________________

You can run nslookup in interactive mode by typing:

>nslookup

To query the DNS server, type the hostname on the nslookup command prompt.

Use **nslookup** to query different hosts and fill Table 3

DNS server name	Address

Table 3: Using the nslookup utility

Exercise 4: Address Resolution Protocol (ARP)

ARP is a protocol for determining the physical address (or MAC address) of a node on a local area network when only the IP address (or logical address) is known. An ARP request is sent to the network, and the node that has the IP address responds with its physical address. Although ARP technically refers only to finding the hardware address, and Reverse ARP (RARP) refers to the reverse procedure, the acronym ARP is commonly used to describe both. ARP is limited to physical network systems that support broadcast packets.

This exercise introduces the use of the "**windump"** and "**arp**" utilities. **Windump** is the porting to the Windows platform of **tcpdump**, the most used network sniffer/analyzer for UNIX. Details for windump can be found at http://windump.polito.it/docs/manual.htm. A printout of this manual is available for use in the lab.

Ping some hosts on your network, the network picture will be showed on the whiteboard, to populate your ARP table. Then use the **arp** utility to observe the current table. Find out the hosts corresponding to the entries. On a command window type:

We use windump to examine headers of packets that are observed on the local physical network. Thus when an ARP packet is recognized, windump looks in the header and reports

- whether it is an ARP request or reply
- the IP addresses of the machines involved.

Delete current entries in the ARP table and start the windump utility by typing

```
>arp –d
>windump -n
```

Ping some hosts on your network and watch for the ARP Request and ARP Reply messages in the windump output and give explanation.

>arp –a

local interface IP address ______________________________

MAC Address	IP address	Type

Table 4: Using the arp utility

Exercise 5: Netstat

Use **netstat** to observe and list the routing table of the host.

>netstat –r

Determine the default route for IP traffic on this machine. Note that the information we obtain is purely local, and has the "next-hop-only" information characteristic of the IP routing table philosophy.

Route Table :

Interface list ____

____

Activate Routes

Network Destination	Net Mask	Gateway	Interface	Metric

Persistent Routes: ____

Table 5: Using the Netstat utility

Exercise 6: Tracert

Use **tracert** utility to examine routes to hosts in the same subnet, hosts on a different subnet and remote hosts (You can get the IP address of hosts in the same subnet, host on different subnet and remote hosts from the whiteboard). Compare and explain the outputs.

1) tracert *ip address or hostname(in same subnet)*
Results:
1
2
3
…

table 6 tracert results in same subnet

2) tracert *ip address or hostname(in different subnet)*
Results:
1
2
3
…

table 7 tracert results in different subnet

3) tracert *ip address or hostname(remote hosts)*
Results:
1
2
3
…

table 8 tracert results in remote host

Exercise 7: Route

Try to configure your host's routing table and add/modify/delete routes to the routing table by playing with the route command. Test the changes by using the tracert and ping command.

PART II: Transmission Control Protocol (TCP)

Objective:

The objective of this lab is to have you explore the characteristics of the transport layer protocol TCP and its mechanism to deal with congestion. You should see the 3-way handshake (Synchronization) when a connection is set up. Also observe the behavior pattern of slow start/congestion avoidance and get to know the difference between TCP and UDP. You may refer the following website to get some detail information on how to decode TCP handshaking packet: http://support.microsoft.com/default.aspx?scid=kb;EN-US;172983.

Descriptive Overview:

The Transmission Control Protocol (TCP) implements guaranteed and reliable delivery over the best-effort Internet Protocol (IP) services. In this lab session, we will concentrate on details of the TCP data transfer mechanism. First, we observe the TCP three-way handshake in detail. Second, we attempt to see the slow-start and congestion avoidance behavior of TCP under nominal conditions. Finally, we will evaluate a UDP application and observe the difference between UDP and TCP.

Note: This experiment involves extensive use of the **windump** utility.

TCP Format

1			16
Source Port		Destination Port	
Sequence Number			
Acknowledgement Number			
Data offset	Reserved	Flags	Window
Checksum		Urgent Pointer	
Option + Padding			
Data			

Exercise 1: TCP Synchronization (handshake)

In this exercise, we will use a simple program (TELNET) to establish a TCP connection to a specified host. Essentially, the following steps should be completed

1. Initialize.
2. Create socket
3. Connect socket
4. Send full packets of data
5. Close connection

Use **windump** to capture the network traffic for observation and analysis. Student should be able to understand the outputs and explain how the data is related to TCP three-way handshakes. Especially, it is important to look closely for the initial sequence number, acknowledgment, and the SYN / FIN packets. Also pay attention to the MSS (Maximum Segment Size) advertised by the connection.

Start Windump by typing:

```
>windump -n
```

To connect to a host using TELNET, type:

>telnet *ip address or hostname*

Table 9
Attach your windump data here:

Table 10

Filter out the TCP three way handshaking packets out from your windump data and explain it as the same style as in the webpage http://support.microsoft.com/default.aspx?scid=kb;EN-US;172983

Table 11
Draw the time sequence diagram for the TCP three way handshaking process here:

Exercise 2: Slow-Start and file transfer using TCP

Slow start is the TCP mechanism to initiate data flow across a connection. It operates by observing that the rate at which new packets should be injected into the network is the rate at which the acknowledgments are returned by the other end.

Here we should observe the slow-start mechanism of TCP, in which the data transfer rate begins at a small value, grows exponentially, and finally levels off to avoid congestion. Notice that FTP uses two TCP connections: the control connection and the data connection. Run windump service on both the FTP client and FTP server.

The basic procedure is as follows:

1. On client, start windump service

```
>windump -n
```

2. From another session on client, initiate an FTP connection and retrieve a data file from the server

```
>ftp ip address of server
>binary
>get file.exe
```

3. After the file transfer is complete, terminate the FTP application and windump service
4. Analyze the windump log and explain how it represents the slow start mechanism.

Table 12 TCP slow start mechanism

Exercise 3: File Transfer using UDP

In this exercise you will use TFTP: Trivial File Transfer Protocol to transfer a file and observe how UDP works. Unlike FTP, TFTP uses UDP as the transport layer protocol and hence the TCP-like advanced functionality is not there. Run Windump on TFTP client:

```
>windump –n
```

Retrieve a file from the TFTP server:

```
>tftp ip address GET filename
```

Once the file transfer is complete, terminate windump and analyze the log file. List the differences you observe between TCP and UDP operation.

Table 13 UDP mechanism