The following lab is designed to introduce you to a few basic networking commands. This will give you some powerful tools for trouble shooting future labs. You are encouraged to explore the various switches and options that you find using other resources such as man or the World Wide Web.

Checking the Network Interface

When you are setting up a computer on a network, configuration errors can cause security breaches and other problems. To check the configuration of the interface eth0 on your system type:

$>**cat /etc/sysconfig/network**

What is the output of this command?

_____
_____
_____
_____

The meaning of these entries is obvious.

Checking the Ethernet Interface

You can display the configuration by entering the command **ifconfig** and the interface name. Try typing:

$>**ifconfig eth0**

What does this tell you?

_____
_____
_____
_____

Exchange IP addresses with the person beside you and try the following:

a) One person types:

$>**ifconfig eth0 down**

b) The other types tries to telnet to the first machine:

c) Person one types:

$>**ifconfig eth0 up**

What happens?

_____
_____
_____
_____
_____

Change roles and try it again.

Testing the Connection

The ping tool is used to test the connection between your system and a remote host: Try the following command:

$>ping www.uniserve.com

What is does this command tell you?

_____
_____

Testing Routing

You can examine the routing table using the **route** command. If the table was built dynamically by a routing protocol it might be very large and contain specific routing information. Use the **route** command with the **–n** option to display the table.

$> route -n

We will discuss the routing table in class.

You can use the **traceroute** command to test the route end to end. Try the following command:

$>traceroute terp.umd.edu

What is displayed on your screen?

_____
_____
_____
_____

Analyzing Network Protocols

Checking Socket Status

You can check on a wide variety of of network information using **netstat**. Try the following:

$>netstat –n --inet

What does this tell you?

_____
_____
_____
_____
_____

The **tcpdump** utility reads every packet from the Ethernet and compares it to the filter you define. If the packet matches the filter , the packet header is displayed on your terminal. This allows you to monitor traffic in real time. For example:

$>tcpdump host 192.168.1.100

Exchange IP addresses with the person sitting beside you and try the following:

a) The fist student types the **tcpdump** command with the **host** option and her/his neighbours IP address similar to what is shown above.
b) From the other computer try and telnet into the first computer.
c) Watch the display on both computers.
d) Try it with ftp.

What is **tcpdump** doing?

_____
_____
_____

Testing DNS

A powerful tool that comes with the BIND software is **nslookup** it is an interactive program that allows you to directly query a DNS server for any type of resource and directly view the servers response.

Follow through the following example on your terminal:

$>*nslookup*

Default Server: wren.foobirds.org
Address: 172.16.5.1

>*set type=NS*
>*ucfv.bc.ca*
Server: helium.bc.tac.net
Address: 208.53.4.130

>

The parts that are in italics are what you type in. What is the output of the above session?

_____
_____
_____
_____
_____

The **host** command can be used to return the IP address of another computer on a network. For example sing the –l option you can find all available IPs for any given domain.

$> host –t any www.ucfv.bc.ca

$>host –l ubc.ca

$>host –l bcit.ca

What is the difference between the results you get using the **–t any** and the **–l** optionsn?

_____
_____
_____
_____

Another DNS test command is **dig** one very useful use for **dig** is its ability to make reverse domain queries simple. When IP addresses are mapperd back they are first reversed to make the structure compatible.

Here are two example of **dig**. Try typing the following two examples:

$>**dig –x 172.16.55.105**

$>**dig @ucfv.bc.ca**

The meat of the response is the answer section buried in the middle of the display which says the address **123.123.123.123 is assigned to xxx.yyy.zzz**