In this exercise, we will have three sections providing an introduction to the use of IP over a Local Area Network and the Internet. The exercises will help you understand the operation of an Ethernet LAN and an IP network.

Network Commands
Commands you will be using include:

- ping - to send an ICMP echo request and examine the response
- arp - to examine the Ethernet address resolution protocol cache
- ifconfig (or ipconfig on a PC) - to examine the configuration of an IP network interface
- netstat - to retrieve network statistics (including routing information) for your computer
- nslookup - to send Domain Name Server queries to the network
- traceroute - print the route packets take to network host

You may find out more about each of these commands by looking at the manual pages. These are accessed by typing 'man xxx' where xxx is the name of the command about which you wish to know more. For example 'man ping' will provide information about how to use the ping command and what options are available to control the way in which the command is used.

Before starting the exercises, please read the following about ICMP and ARP.

Internet Control Message Protocol (ICMP)
The Internet Control Message Protocol (ICMP) is used to report problems with delivery of IP datagrams within an IP network. It can be used to show when a particular End System (ES) is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, etc. The protocol is also frequently used by Internet managers to verify correct operations of ES and to check that routers are correctly routing packets to the specified destination address.

The "ping" program contains a client interface to ICMP. This may be used by a user to verify an end to end connection is operational. The -c option specifies how many packets to send. So, "ping -c10 yahoo.com" sends ten ICMP-echo requests, and displays the time it takes to receive each reply from the ICMP echo server running on the remote computer (i.e. "yahoo.com" in this example). In windows, you should type "ping -n10 yahoo.com", since the option is "n" in this case. Each time an echo reply packet is received a single line of text is displayed. Each echo request packet contains a sequence number (starting at 0) which is incremented after each transmission, and a timestamp value indicating the transmission time. The text printed by ping shows the received sequence number, and the measured round trip time (in milliseconds).

Address Resolution Protocol (ARP)
The address resolution protocol is a protocol used by the IP network layer to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the OSI link layer, and is used when IP is used over Ethernet. The hardware address is also known as the Medium Access Control (MAC) address, in reference to the standards which define Ethernet. Each computer network interface card is allocated a

globally unique 6 byte address when the factory manufactures the card (stored in a PROM). This is the normal source address used by an interface. A computer sends all packets which it creates with its own hardware source address, and receives all packets which match its hardware address or the broadcast address. When configured to use multicast, a selection of multicast hardware addresses may also be received.

The Ethernet address is a link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the network addresses of individual nodes which are to be used. A protocol known as the Address Resolution Protocol (ARP) is therefore used to translate between the two types of address. The arp client and server processes operate on all computers using IP over Ethernet. The processes are normally implemented as part of the software driver which drives the network interface card.

To reduce the number of address resolution requests, a client normally caches resolved addresses for a (short) period of time. The arp cache is of a finite size, and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The arp cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers which are not currently running.

1. Finding out about your own network connection

The purpose of this exercise is to find out about the connection of your computer (an End System) to the network. Most computers at a University or Company are directly connected to one or another type of Local Area Network. The exercise will consider only the protocol layers at, and below, the network layer.

1) Examine the connection to the local LAN

The computers use the IP network protocol to communicate. The details of the IP configuration for your computer may usually be found by using the ifconfig (interface configuration) program with a '-a' option to show the status all network interfaces. (On a PC use the alternative command 'ipconfig –all'.)

Type: ifconfig -a

The information which is displayed consists of a series of lines, with one entry for each network interface connected to the computer. All computers will have at least two interfaces. One will be an interface to a network interface card (e.g. an Ethernet card). A computer with additional network interface cards will have one entry for each network connection which may be used by IP.

Another interface will be a software driver called the "loop back interface". The loop back interface is used by the computer to route IP packets from a client program on a computer to a server program which is running on the same computer. The information displayed by ifconfig

will include an entry for the loop back interface (normally called lo0:). This output may look something like:

```
lo0: flags=8049<UP,LOOPBACK,RUNNING> mtu 16384 inet 127.0.0.1 netmask 0xff000000
```

This example information shows that some options have been set (8049) that the interface is connected (UP), it is running in loop back (LOOPBACK) and that it is currently operational (RUNNING). The internet (IP) network address is 127.0.0.1 (in dotted decimal notation) and the IP netmask is 0xff000000 (in hexadecimal).
This is not shown by the ipconfig command on a PC, but the loopback interface is still there!

Q:/ What information is displayed about the loop back interface on your computer?

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=3<RXCSUM,TXCSUM>
inet6 ::1 prefixlen 128
inet 127.0.0.1 netmask 0xff000000

2) Verify that the loop back interface is indeed working!

Type: ping -c10 127.0.0.1

The ping command sends an ICMP echo request packet from the client (your computer) to another IP network node. The ICMP server program at the specified destination (which in this case is also your computer, but is more normally another system) receives the echo request message and generates an echo reply message. This is transported by the IP network (in an IP packet) back to the client program. When the message is received, the client displays a line of text telling you that the remote computer is "alive". If the message is not received within a set period of time (i.e., the IP packet was discarded or corrupted within the network), the client program assumes that the remote computer did not reply.

In the information displayed when you typed 'ifconfig -a' or 'ipconfig -all', there should be information about the main or primary IP address of your computer. This is the network interface which connects your computer to the LAN. This will probably be labelled le0:, ie0:, eth0:, en0:, en20:. ed0:, or something similar. An example for a computer with a primary IP addresses of 172.17.203.45 (in dotted decimal notation) is shown below:

```
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 172.17.203.45 netmask 0xffffff8 broadcast 172.17.203.47
        ether 00:23:12:00:85:e4
```

Some computers have more than one network interface, in this case the first entry in the table is usually identified as the primary interface. the MTU (maximum transmission unit) usually specifies the upper limit on packet sizes.

Q:/ From the information returned when you typed 'ifconfig -a' **can you find out the primary IP address of your computer?**

192.168.1.103
HEX:C0A80167

Now use the ping program to check that this interface is working.

Type: ping followed by the IP number.

Q:/ Did you receive a reply? (i.e. a line of text showing that the interface is "alive").

yes have

Q:/ Is any packet sent on the Ethernet during your ping?

No

Q:/ Does your host use an all 1's or all 0's host part for its IP network broadcast address?

yes,
The IP network broadcast address is the same as the IP network address with all the bits of the host number part of the address set to 1's or 0's.

Q:/ Can you use the subnet mask to find out the network address of the local IP network?

YES
For the address 192.168.1.103, the network address is 192.168.1.100, and the broadcast address is 192.168.1.255.

2. Learning about computers on remote networks

This exercise examines how an IP network sends IP packets to a remote network using the local router. It will start by using the default router for the computer's IP network.

Examine the computers attached to your local IP network using arp

Type: arp -a

If the IP addresses are shown as names (e.g. macintosh.ashland.edu), rather than numeric IP addresses (in dotted decimal notation) you should use the Domain Name Service (DNS) to find (resolve) the numeric address of a few of the names. The dns service may be accessed via a client program called nslookup by typing:

nslookup name

Q:/Do you notice something in common about the network part of all the listed IP addresses on your primary Ethernet interface?

All the IP addresses that were listed

To proceed further, we will need to use your default router. This is the router for your computer's IP network (sometimes books refer to this confusingly as the gateway router). It is the router to which all non-local IP packets will be sent - and the path by which your computer communicates with all computers that are not directly connected to your local LAN.

We will also use a remote end system, that you know is not local to your site (e.g. choose your favourite web site, the Micro soft web site, or something that you know is in another country). In this exercise, you will send packets directly to the ICMP echo server running on your chosen end system.

- Verify that your computer is connected to the campus network.

Try to contact the ICMP server on the computer at your chosen web site (e.g. yahoo.com).

Type: ping –c10 www.yahoo.com

Q:/ Did you get a reply?

Yes

Now
Type: arp -a

One of the computers listed in the arp cache must be the default IP router. But how does your computer know which IP address corresponds to the default router for your IP network?

The answer is the person who set-up your computer has already configured this (or your computer discovered this, e.g. using DHCP).

You can find the address of the default router by typing netstat -rn (the options "r" indicates that the routing table should be printed and the option "n" indicates ip addresses should be printed in numeric (i.e., dotted decimal notation)).

Type: netstat -rn

This lists the routing table in your computer. (Other information such as the MTU size of each interface may also be shown). Among other addresses there should be an entry here for the loop back interface that was used in exercise 1. There should also be an entry marked as "default", "default gateway", or sometimes just labelled "0.0.0.0", this is the default router IP address. Note the address down (you will need it in a moment).

Q:/ Which router is specified as the local (default) router?

192.168.1.1

3. Learning about the Internet

You now know your computer's IP address, and how your computer uses arp to find out local hardware addresses for computers connected to your local LAN. You should also know how your computer determines that an IP address is remote and how it uses a default router to start to forward packets to other networks via a network of links (serial communications links leased

from national telecommunication providers, e.g. VERIZON, SPRINT) and routers forming a WAN.

In this exercise, you will contact some remote end systems located far away on the Internet (you could use the same one that you "pinged" in exercise 2). The way in which computers communicate with local systems and remote systems is different. To communicate with a remote system your computer will first send to the default router.

Contacting remote sites from your computer
Use the ping program to examine whether some remote sites are reachable from your computer. Here are some addresses to try. Be sure to specify that you would like statistics (-c) and that you are to send only ten (10) messages .

Type:

```
ping -c10 space.mit.edu
```

```
ping -c10 www.nasa.gov
```

```
ping -c10 www.ashland.edu
```

Q:/Do you always get a reply when you send an ICMP echo-request?

no

Q:/Is it acceptable for packets to be lost?

Yes
1. don't want you know the ip
2. need processing time, may overloaded

Q:/ Do all the measurements of the delay to the same computer take the same time? - Why not?

No,
the network load, the transmission speed, and the loading of the destination host.

Q:/ Does the distance to the host determine the measured time?

The time taken to receive a reply measures the distance in "cyber space" to the destination
this need not have a relationship to the actual distance to the destination

You can also use traceroute command to trace the path your packet may use to go from your computer to a remote host. The syntax of the command is

```
traceroute servername
```

A sample output of a traceroute command is given as the following

```
traceroute: Warning: www.google.com has multiple addresses; using 72.14.204.104
traceroute to www.l.google.com (72.14.204.104), 64 hops max, 40 byte packets
1  172.16.112.252 (172.16.112.252)  0.844 ms  0.316 ms  0.444 ms
```

```
2  172.16.0.32 (172.16.0.32)  0.651 ms  0.767 ms  0.730 ms
3  198.30.217.1 (198.30.217.1)  3.599 ms  7.111 ms  6.180 ms
4  akrnq-r1-t3-0-2-1.bb.oar.net (199.18.101.53)  45.661 ms  32.978 ms  25.387 ms
5  akrnq-r0-ge-4-0-1s100.core.oar.net (199.218.38.213)  22.522 ms  28.770 ms  29.776 ms
6  clevs-r0-xe-0-0-0s100.core.oar.net (199.218.38.182)  29.624 ms  33.289 ms  29.727 ms
7  toldb-r0-xe-4-0-0s100.core.oar.net (199.218.39.14)  47.851 ms  56.168 ms  67.407 ms
8  199.18.168.130 (199.18.168.130)  94.337 ms  87.156 ms  91.202 ms
9  209.85.254.130 (209.85.254.130)  75.285 ms  63.077 ms  77.127 ms
10  209.85.248.222 (209.85.248.222)  126.981 ms  115.384 ms  63.634 ms
11  66.249.94.46 (66.249.94.46)  60.961 ms  40.061 ms  65.852 ms
12  iad04s01-in-f104.1e100.net (72.14.204.104)  47.534 ms  57.802 ms  53.511 ms
```

The first line basically displays what I did and for each numbered item, it represents a hop. So it took 12 hops to reach one of the google web servers. You can also use a –m option for traceroute to limit the max number of hops.

Try to traceroute to www.ashland.edu and www.ucla.edu and answer the following questipons

Q:/ Do you already obtain a route that can reach the destination host?

Yes

Q:/ Is it a problem if there is no route available from the output of traceroute command?

Yes

Timeout or jump to next hops

4. Basic Cisco Switch Commands

- The most important command in IOS is '?'. Pressing ? at any point will give you all of the possibilities of what you can use. Tab can also be used for auto complete purposes.
- When making configuration, use 'no' keyword to get rid of the command.

save configuration Hand in late

- copy run start (copy running-config startup-config)

configuration modes from priviledged EXEC mode

- config t (configure terminal)
- interface <interface>
- vlan <vlan id>

user commands

- ping <ip address>
- traceroute <ip address>

show commands

- show run (show running-config)
- show start (show startup-config)
- show ip route

- show ip int br (show ip interface brief)
- show ip arp
- show mac address
- show ip ospf
- show interface [<interface>]
- show version

interface commands

- no shutdown
- shutdown
- switchport mode access
- switchport mode trunkswitchport access vlan <vlan id>
- switchport trunk encap dot1q
- switchport trunk allowed vlan <vlan ids>

Answer the following questions on the cisco network in Patterson 204

- **What is the ip address of each switch? What is the command that setup their ip address?**

- **If you plug in your computer into AjwaField's port 5, what's is your IP address? Why is that IP address assigned to your computer? Justify your answer from the configuration of the switch.**

- **When you plug in your computer into a port at CaoLand, do you get an IP address? Why?**

- **Find you find the route to go from a computer at CaoCity to a computer on AjwaField? What command do you use? You might want to work with a partner so you can have two computers connected to the switches**

- **If you unplug the connections between KerkezLand and CaoLand (i.e. the fiber link), how do you go from CaoCity to AjwaField now?**