CSCD58 A3

Derek Lai

November 2014

1. Short Answers

1.1. i. IPv4: 142.1.96.164
IPv6: fe80::250:56ff:fe84:4547/64

```
        laihoche@mathlab:~$ ifconfig etho0
eth0      Link encap:Ethernet  HWaddr 00:50:56:84:45:47
          inet addr:142.1.96.164  Bcast:142.1.96.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe84:4547/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:580254778 errors:0 dropped:265623 overruns:0 frame:0
          TX packets:415566604 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:276375779821 (276.3 GB)  TX bytes:1052600140617 (1.0 TB)
```

ii. MAC: 00:50:56:84:45:47

```
        laihoche@mathlab:~$ ifconfig etho0
eth0      Link encap:Ethernet  HWaddr 00:50:56:84:45:47
          inet addr:142.1.96.164  Bcast:142.1.96.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe84:4547/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:580254778 errors:0 dropped:265623 overruns:0 frame:0
          TX packets:415566604 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:276375779821 (276.3 GB)  TX bytes:1052600140617 (1.0 TB)
```

iii. IPv4: 142.1.96.1
MAC: 40:55:39:27:da:c1

```
laihoche@mathlab:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         142.1.96.1      0.0.0.0         UG    100    0        0 eth0
10.15.2.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
142.1.96.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0

laihoche@mathlab:~$ arp 142.1.96.1
Address                  HWtype  HWaddress           Flags Mask            Iface
utsc-srv.gw.utsc.utoron  ether   40:55:39:27:da:c1   C                     eth0
```

iv. Ip of Pardus = 128.100.96.17
Ip of Lupus = 128.100.96.16
No MAC for both addresses

```
laihoche@mathlab:~$ traceroute google.com
traceroute to google.com (74.125.226.102), 30 hops max, 60 byte packets
 1  utsc-srv.gw.utsc.utoronto.ca (142.1.96.1)  0.645 ms  0.882 ms  0.915 ms
 2  mcl-utsc-gpb.gw.utoronto.ca (128.100.96.113)  2.596 ms  2.541 ms  2.531 ms
 3  pardus-gpb.gw.utoronto.ca (128.100.96.17)  2.641 ms  2.629 ms  2.603 ms
 4  ut-hub-utoronto2-if-re.gtanet.ca (205.211.94.129)  2.510 ms  2.484 ms  2.450 ms
 5  ORION-GTANET-RNE.DIST1-TORO.IP.orion.on.ca (66.97.23.57)  2.426 ms  2.392 ms  2.332 ms
 6  be201.gw01-toro.orion.on.ca (66.97.16.22)  2.293 ms  2.382 ms  1.746 ms
^C
laihoche@mathlab:~$ traceroute google.com
traceroute to google.com (74.125.226.100), 30 hops max, 60 byte packets
 1  utsc-srv.gw.utsc.utoronto.ca (142.1.96.1)  0.475 ms  0.615 ms  0.746 ms
 2  mcl-utsc-gpb.gw.utoronto.ca (128.100.96.113)  1.031 ms  1.101 ms  1.159 ms
 3  lupus-gpb.gw.utoronto.ca (128.100.96.16)  1.588 ms  1.599 ms  1.595 ms
 4  ut-hub-utoronto1-if-re.gtanet.ca (205.211.94.233)  1.848 ms  2.122 ms  2.092 ms
 5  ORION-GTANET-RNE.DIST1-TORO.IP.orion.on.ca (66.97.23.57)  2.179 ms  2.440 ms  2.448 ms
 6  be201.gw01-toro.orion.on.ca (66.97.16.22)  1.816 ms  2.060 ms  2.040 ms
 7  74.125.48.230 (74.125.48.230)  1.295 ms  1.325 ms  1.238 ms
 8  216.239.47.114 (216.239.47.114)  1.318 ms  1.237 ms  1.251 ms
 9  209.85.250.207 (209.85.250.207)  1.710 ms  1.842 ms  1.562 ms
10  yyz08s13-in-f4.1e100.net (74.125.226.100)  1.243 ms  1.250 ms  1.209 ms

laihoche@mathlab:~$ arp 128.100.96.16
128.100.96.16 (128.100.96.16) -- no entry
laihoche@mathlab:~$ arp 128.100.96.17
128.100.96.17 (128.100.96.17) -- no entry
```

v. There are 2^{96} host addresses allocated to Uoft AS (AS 239), 128-bits - 32 static bits. The AS is allocated in the range 2606:fa00::/32. This was found at http://www.tcpiputils.com/browse/as/239.

1.2. Gratuitous ARP:
Gratuitous ARP can be used as an announcement protocol to update mapping of hardware addresses on other hosts when senders IP or MAC address changes. It can also be used to update ARP Cache of other systems before an ARP request. This is done by sending an ARP request packet where both the source and destination IP are set to the host system and the destination MAC address is the broadcast MAC address (ff:ff:ff:ff:ff:ff)

ARP Cache Poisoning:
Also called ARP Spoofing, an attacker sends a fake ARP message on a local network to associate the attacker's MAC address with an IP of another host. This will cause all traffic meant for that IP to be sent to the attacker instead. The attacker may choose to modify and redirect the traffic (MITM) or just leave it alone to stop traffic (DOS). The attacker would need to send an ARP reply to a victim associating its MAC address, A, with its intended target's IP, B. They can choose A to be a fake MAC address causing the victim to to send packets to a fake location, cutting internet for the victim.

IPv6 tunnelling:
IPv6 tunnelling is allowing for IPv6 hosts and router to connection with other IPv6 devices over the current IPv4 internet. This is done by encapsulating the IPv6 datagram within IPv4 packets where they travel across IPv4 internet until they reach their destination. The IPv6 host will then decapsulate the IPv6 datagram.

Token Ring:
Token Ring is a LAN where all computers are connected in a ring/star like configuration and a bit or token passing scheme is used to prevent data collision between two computers communicating at the same time. A special token is passed around the ring, an empty data frame. When a computer wishes to pass data, it must catch the free token and insert its data into the frame along with its destination. The token is then passed around the ring, if the destination is not the next computers it would pass the token to the next one in the circle until the recipient receives the data.

1.3. i. Polling:
If you wish to talk to someone then you must:
- Tap on that persons shoulder, if that person ignores you then they are preoccupied
- If someone is preoccupied, continue to tap them until they are free (polling)
- If a person is free to talk then you may talk, they will give you their full attention and ignore others

ii. Token Passing:
Token passing is similar to passing notes around in school:
- All the patrons must gather around in a circle
- They can only communicate through a note pad
- The note pad is continuously passed around the circle while no one wishes to talk
- If a person wishes to talk they must wait until the note pad is passed to them
- Once the notepad is in hand, they may write their message and fold that piece of paper in half and write their recipient's name on the back
- The notepad is passed to the next person
- If the notepad has something written on it, the next person looks at the name. If the name does not belong to them the note pad is passed on
- When the notepad is finally given to the recipient, they may open the paper and read the message. They then rip that page off to a new and empty page and either pass the notepad on or write their own message

iii. ALOHA:
Pure ALOHA is similar to people trying to talk:
- If a person wishes to talk, they talk at any time
- If two people talk over each other their message is not heard due to the speech collision at which point they must repeat their message after waiting random length of time so they don't talk over each other again
- If the message is heard without anyone talking over them, the recipient will reply saying they heard the message

iv. slotted-ALOHA:
Slotted-ALOHA has the same principle as ALOHA in which people speak and a reply is expected if their message is heard:
- If a person wishes to talk, they talk at any time
- Messages are limited to a max of 15 seconds
- Messages must be spoken at the beginning of an interval, they must wait if they have to
- Each 15 second interval is measured by a clock
- If two people talk over each other their message is not heard due to the speech collision at which point they must repeat their message after waiting random length of time so they don't talk over each other again
- If the message is heard without anyone talking over them, the recipient will reply saying they heard the message

v. CSMA/CD:
Carrier Sense Multiple Access/Collision Detection. This is like people trying to enter a narrow doorway:
- Everyone in the room is allowed to enter through that doorway
- Before a person enters, they check to see if the doorway is clear
- If the doorway is clear then they can walk through
- If someone is already in it then they must wait until it is clear
- If two people check and see the doorway is clear and they both try to walk through, they will get stuck in the doorway
- When this occurs, both people step back and wait a random amount of time before attempting to walk through