Homework 2

Name – Sati, Ankit Date – 9/30/2021

Section – 001

SID – as14128

Total in points (Maximum 100 points)–

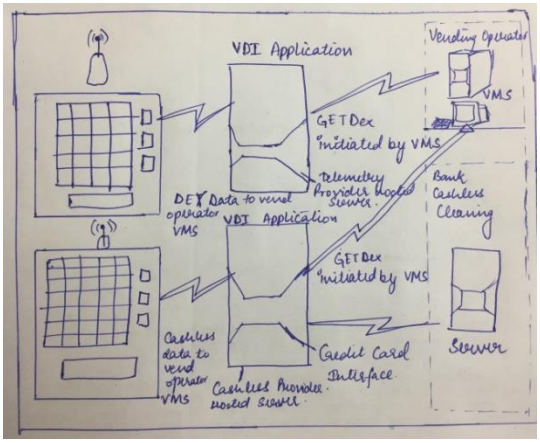
Professors Comments –

Affirmation of Independent Effort – Ankit Sati

Answers

1. There are namely 2 protocols that are used in the vending machines.
   a. Multi Drop bus protocol

   Multi drop bus Protocol - The multidrop bus used by vending machine controllers to communicate with the vending machine's components, such as a currency detector, is also called MDB (for Multi-Drop Bus). The physical connection is realized as a serial bus with a fixed data rate of 9600 baud. There are just 2 communications signals plus the essential common-ground reference signal.



2. a. Explanations of the following
   i. **Network Edge :** The network edge refers to the area where a device or local network interfaces with the internet. The edge is close to the devices it is communicating with and is the entry point to the network. The network edge is a crucial security boundary that network administrators must provide solutions for. The network edge refers to endpoints. It is the first step between endpoints and the core of the network. These include personal computers (PCs), adapters, modems, and the devices that connect to them.

   ii. **Network Core :** Core networks consist of local area networks (LAN), virtual private networks (VPN), voice over internet protocol (VoIP), and geographic information systems (GIS). It is a telecommunication network's core part, which offers numerous services to the customers who are interconnected by the access network. Its key function is to direct telephone calls over the public-switched telephone network.

   iii. **Store and forward Packet Switching :** In telecommunications, store − and − forward packet switching is a technique where the data packets are stored in each intermediate node, before they are forwarded to the next node. The intermediate node checks whether the packet is error−free before transmitting, thus ensuring integrity of the data packets. In general, the network layer operates in an environment that uses store and forward packet switching

   iv. **Bandwidth** : Bandwidth is a term used to express the total capacity of network transmission in a single second. It provides the maximum rate of the data transfer for a given path or connection in the computer network. Bandwidth also called Network Bandwidth, Data Bandwidth, or Digital Bandwidth where generally all of them refer to the same term bandwidth.

   v. **Throughput** : Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a processor, memory and/or network communications.

b.

i. Advantages of circuit switching

- Decreases the delay the user experiences before and during a call
- The call will be done with a steady bandwidth, dedicated channel, and consistent data rate
- Packets are always delivered in the correct order

ii. Advantages of Packet switching

- More efficient than circuit switching
- Data packets are able to find the destination without the use of a dedicated channel
- Reduces lost data packets because packet switching allows for resending of packets
- More cost-effective since there is no need for a dedicated channel for voice or data traffic

3. Packet Transmission Delays.

i.

a. When Circuit switching is used

Total Bandwidth available = 3Mpbs = 3000Kbps
One user requirement = 15Kbps
3000/15 = 200
So total users that can be supported = 200 Users
This means at a single point in time 200 users can access this link.

b. Circuit switching is used

Total Bandwidth available = 3Mpbs
One user requirement = 1.5Mbps
3/1.5 = 2 Users
So total users that can be supported = 2 Users
This means at a single point in time 2 users can access this link.

c. Calculating the probability in Packet switching.

Total users = 4
Transmission per user = 10/100 = 0.1
P^4= (0.1)^4 = 0.0001. Probability that all four users are transmitting simultaneously. Since the queue grows when all the users are transmitting, the fraction of time during which the queue grows (which is equal to the probability that all four users are transmitting simultaneously) is 0.0001.

d. 2 out of 4 users are using at the same time.

Total users = 4
Users at a given time =2
Transmission per user = .1
4C2 =6 (Choosing 2 out of 4)
Probability = 6*(0.1)^2*(.9)^2 = 0.486

ii. Calculating delays.

a. Propagation delay = 300000ms
b. Transmission Delay = 1250ms

iii. a. No

c. Yes

iv. Number of packets 10

Length of each packet = 100Kbits

Transmission rate = 10 kbs

Traffic intensity = LA/r = 100

AVG delay = (n*(n-1)*L/R)/2

= 10 *9*10/2 = 450 ms

4. Traceroutes

a. X protocol = ICMP

Traceroute most commonly uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop.

b. The traceroute command uses the **TTL field** in the IP header to cause routers and servers to generate specific return messages.

iii. Screenshots of 3 hostnames

1.Youtube

```
C:\Users\ankit>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.250.65.238]
over a maximum of 30 hops:

  1   107 ms     3 ms     2 ms  10.16.0.2
  2    38 ms    42 ms    23 ms  coregwb-te5-8-vl901-wlangwa-wwh.net.nyu.edu [10.254.4.32]
  3     4 ms     2 ms     1 ms  nyugwa-vl902.net.nyu.edu [128.122.1.36]
  4     6 ms     4 ms     2 ms  ngfw-palo-vl1500.net.nyu.edu [192.168.184.228]
  5     8 ms     4 ms     2 ms  nyugwa-outside-ngfw-vl3080.net.nyu.edu [128.122.254.114]
  6     5 ms     3 ms     5 ms  nyunata-vl1000.net.nyu.edu [192.168.184.221]
  7     4 ms     5 ms     6 ms  nyugwa-vl1001.net.nyu.edu [192.76.177.202]
  8    12 ms     7 ms     4 ms  dmzgwb-ptp-nyugwa-vl3082.net.nyu.edu [128.122.254.111]
  9     4 ms     8 ms     8 ms  extgwa-vrf-cdn-ptp-dmzgwb.net.nyu.edu [128.122.254.62]
 10     6 ms     5 ms     3 ms  nyc-9208-nyu-cdn.nysernet.net [199.109.105.5]
 11     8 ms     3 ms     4 ms  nyc111-9204-nyc-9208.cdn.nysernet.net [199.109.107.166]
 12     6 ms     4 ms     5 ms  72.14.202.166
 13     6 ms     4 ms     4 ms  108.170.248.65
 14     *        7 ms     8 ms  142.251.60.227
^C
C:\Users\ankit>^Z
```

2. CloudProxy

```
C:\Users\ankit>tracert 192.124.249.107

Tracing route to cloudproxy10107.sucuri.net [192.124.249.107]
over a maximum of 30 hops:

  1     8 ms     4 ms    41 ms  10.16.0.2
  2     2 ms     1 ms     1 ms  coregwa-te5-8-vl901-wlangwa-wwh.net.nyu.edu [10.254.2.32]
  3     9 ms    77 ms     6 ms  nyugwa-vl902.net.nyu.edu [128.122.1.36]
  4     4 ms     3 ms     4 ms  ngfw-palo-vl1500.net.nyu.edu [192.168.184.228]
  5     3 ms     3 ms     3 ms  nyugwa-outside-ngfw-vl3080.net.nyu.edu [128.122.254.114]
  6     *        2 ms     2 ms  nyunata-vl1000.net.nyu.edu [192.168.184.221]
  7     9 ms     3 ms     3 ms  nyugwa-vl1001.net.nyu.edu [192.76.177.202]
  8     6 ms     3 ms     3 ms  dmzgwa-ptp-nyugwa-vl3081.net.nyu.edu [128.122.254.109]
  9     9 ms     7 ms     5 ms  extgwd-dmzgwa.net.nyu.edu [10.254.255.3]
 10    25 ms    36 ms     7 ms  ae0-3958.cr2-nyc2.ip4.gtt.net [209.120.137.217]
 11    14 ms     8 ms     9 ms  ae12.cr2-was1.ip4.gtt.net [89.149.130.157]
 12    17 ms    15 ms    10 ms  ip4.gtt.net [173.205.46.86]
 13    10 ms    20 ms     9 ms  cloudproxy10107.sucuri.net [192.124.249.107]

Trace complete.
```

3. Google

```
C:\Users\ankit>tracert www.google.com

Tracing route to www.google.com [142.251.35.164]
over a maximum of 30 hops:

  1    17 ms     2 ms     2 ms  10.16.0.2
  2     3 ms     2 ms     6 ms  coregwa-te5-8-vl901-wlangwa-wwh.net.nyu.edu [10.254.2.32]
  3     6 ms     3 ms     2 ms  nyugwa-vl902.net.nyu.edu [128.122.1.36]
  4     6 ms     5 ms     2 ms  ngfw-palo-vl1500.net.nyu.edu [192.168.184.228]
  5     9 ms     8 ms     6 ms  nyugwa-outside-ngfw-vl3080.net.nyu.edu [128.122.254.114]
  6     4 ms     2 ms     6 ms  nyunata-vl1000.net.nyu.edu [192.168.184.221]
  7     6 ms     7 ms     5 ms  nyugwa-vl1001.net.nyu.edu [192.76.177.202]
  8     5 ms     7 ms     7 ms  dmzgwb-ptp-nyugwa-vl3082.net.nyu.edu [128.122.254.111]
  9     6 ms     3 ms     3 ms  extgwa-vrf-cdn-ptp-dmzgwb.net.nyu.edu [128.122.254.62]
 10     9 ms     9 ms     8 ms  nyc-9208-nyu-cdn.nysernet.net [199.109.105.5]
 11     5 ms     3 ms     3 ms  nyc111-9204-nyc-9208.cdn.nysernet.net [199.109.107.166]
 12     *        6 ms     7 ms  72.14.202.166
 13     8 ms     5 ms     8 ms  108.170.248.1
 14    10 ms     4 ms     7 ms  142.251.64.5
 15    12 ms     9 ms     5 ms  lga25s78-in-f4.1e100.net [142.251.35.164]

Trace complete.
```

B

- Generally we cannot see the ISP details from the just looking at the host names. However there are multiple applications available that can trave the IP and the hops and by that they can resolve to the ISP.

- There ate at least 3 packets that are sent at a time to a single router. It is true that the first packet will not feel any delays, however as soon as the second packet comes we can see some delays. This happens due to the Queuing delays. These delays are exponential delays as soon as the packets start queuing up, the delay goes up substantially. This is what happens in the example shared in the question above.

5. Web Application Architecture

The application architecture is designed by the application developer and dictates how the application is structured over the various end systems. A developer will likely draw on one of the two architectural paradigms used in modern network applications:

a. Client/Server

In a client-server architecture, there is an always-on host, called the server, which services requests from many other hosts, called clients. A classic example is the Web application for which an always-on Web server services requests from browsers running on client hosts. When a Web server receives a request for an object from a client host, it responds by sending the requested object to the client host. Note that with the client-server architecture, clients do not directly communicate with each other; for example, in the Web application, two browsers do not directly communicate. Because the server has a fixed, well-known address, and because the server is always on, a client can always contact the server by sending a packet to the server's IP address. Some of the better-known applications with a client-server architecture include the Web, FTP, Telnet, and e-mail.

b. Peer to Peer

Instead the application exploits direct communication between pairs of intermittently connected

hosts, called peers. The peers are not owned by the service provider, but are instead desktops and laptops controlled by users, with most of the peers residing in homes, universities, and offices. Because the peers communicate without passing through a dedicated server, the architecture is called peer-to-peer. For example, for many instant messaging applications, servers are used to track the IP addresses of users, but user-to-user messages are sent directly between user hosts (without passing through intermediate servers).

Features of P2P architectures is their self-scalability. For example, in a P2P file-sharing application, although each peer generates workload by requesting files, each peer also adds service capacity to the system by distributing files to other peers.

6. Real Time messaging application.
   a. **BlackBerry Messenger**: It is a proprietary Internet-based instant messenger and video telephony application. Messages sent via BlackBerry Messenger are sent over the Internet and use the BlackBerry PIN system, it is their proprietary protocol. The communications are not end-to-end encrypted.
   Reference:
   https://en.wikipedia.org/wiki/BlackBerry_Messenger

   b. **WhatsApp:** It uses a customized version of the open standard Extensible Messaging and Presence Protocol (XMPP). Multimedia messages are sent by uploading the image, audio or video to be sent to an HTTP server and then sending a link to the content along with its Base64 encoded thumbnail (if applicable).
   Reference:
   https://en.wikipedia.org/wiki/WhatsApp

   c. **iMessage:** It is an instant messaging service developed by Apple Inc. The iMessage protocol is based on the Apple Push Notification Service (APNs)—a proprietary, binary protocol. It sets up a Keep-Alive connection with the Apple servers. Every connection has its own unique code, which acts as an identifier for the route that should be used to send a message to a specific device. The connection is encrypted with TLS. iMessage provides end-to-end encryption.
   Reference:
   https://en.wikipedia.org/wiki/IMessage

   d. **Yahoo Messenger:** The Yahoo! Messenger Protocol (YMSG) is the underlying network protocol used by the Yahoo! Messenger instant messaging client. Yahoo! Instant Messenger supports many features beyond just messaging, including off-line messaging, file transfer, chat, conferencing, voice chat, webcams and avatars. The YMSG protocol communicates between the client application, and a server, using a TCP/IP connection on port 5050 by default.

   Reference:
   https://en.wikipedia.org/wiki/Yahoo!_Messenger_Protocol

The RFCs for instant messaging are:

- 2000-02 RFC 2778: AModel for Presence and Instant Messaging (Informational)
- 2000-02 RFC 2779: Instant Messaging / Presence Protocol Requirements (Informational)
- 2002-07 RFC 3339: Date and Time on the Internet: Timestamps (Proposed Standard)
- 2004-08 RFC 3859: Common Profile for Presence (CPP) (Proposed Standard)

- 2004-08 RFC 3860: Common Profile for Instant Messaging (CPIM) (Proposed Standard)
- 2004-08 RFC 3861: Address Resolution for Instant Messaging and Presence (Proposed Standard)
- 2004-08 RFC 3862: Common Presence and Instant Messaging (CPIM): Message Format (Proposed Standard)
- 2004-08 RFC 3863: Presence Information Data Format (PIDF) (Proposed Standard)

7. Email applications

Outlook: It supports both IMAP4 and POP3 protocols to receive emails. SSL is required for incoming emails and TLS is required for outgoing emails. POP uses port 995 and IMAP uses port 993. Only TLS can be
used for outgoing connection and both ports 25 and 587 can be used.
References:
https://en.wikipedia.org/wiki/Outlook.com
https://support.office.com/en-us/article/POP-and-IMAP-settings-for-Outlook-Office-365-for-business-7fc677eb-2491-4cbc-8153-8e7113525f6c

Gmail: It supports both IMAP4 and POP3 protocols to receive emails. TLS or SSL are required for security. POP uses port 995 and for IMAP port 993 is used for incoming mail and port 465 or 587 for outgoing mail. For SSL Port 465 is used and for TLS Port 587 used.
References:
coderoman.com/2013/01/pop-imap-and-smtp-settings-for-gmail/
en.wikipedia.org/wiki/Gmail
support.google.com

iCloud: IMAP is supported for receiving email and SMPT for sending emails. SSL or TLS are required. Port 993 is used for IMAP and Port 587 is used for SMTP.
Reference:
https://support.apple.com/en-us/HT202304

Yahoo! Mail: It supports both IMAP and POP3 for incoming emails and SMTP for outgoing emails. IMAP uses port 993 and port 995 for POP. Port 465 or 587 can be used for SMTP. SSL is required for incoming emails and both SSL or TLS can be used for outgoing emails.
References:
https://help.yahoo.com/kb/SLN4724.html
https://help.yahoo.com/kb/SLN4075.html

	Protocol to send (User agent)	Mail Server	Protocol to download emails on client machine
GMail	SMTP	SMTP [RFC2821]	IMAP/POP
Outlook	SMTP	SMTP [RFC2821]	IMAP/POP
iCloud	SMTP	SMTP [RFC2821]	IMAP/POP
Yahoo! Mail	SMTP	SMTP [RFC2821]	IMAP/POP

Differences:

- When using POP, clients typically connect to the e-mail server briefly, only as long as it takes to download new messages. When using IMAP, clients often stay connected as long as the user interface is active and download message content on demand. For users with many or large messages, this IMAP usage pattern can result in faster response times.
- The POP protocol requires the currently connected client to be the only client connected to the mailbox. In contrast, the IMAP protocol specifically allows simultaneous access by multiple clients and provides mechanisms for clients to detect changes made to the mailbox by other, concurrently connected, clients.
- IMAP supports flags on the server to keep track of message state: for example, whether or not the message has been read, replied to, or deleted.
- POP is a much simpler protocol, making implementation easier.
- POP mail moves the message from the email server onto your local computer, although there is usually an option to leave the messages on the email server as well. IMAP defaults to leaving the message on the email server, simply downloading a local copy.

The RFCs related to email are:

- RFC 821 – Simple Mail Transfer Protocol (Obsoleted by RFC 2821)
- RFC 822 – Standard for the Format of ARPA Internet Text Messages (Obsoleted by RFC 2822)
- RFC 1035 – Domain names, Implementation and specification
- RFC 1123 – Requirements for Internet Hosts, Application and Support (Updated by RFC 2821, RFC 5321)
- RFC 2142 – Mailbox Names for Common Services, Roles and Functions
- RFC 2821 – Simple Mail Transfer Protocol (Obsoletes RFC 821, Updates RFC 1123, Obsoleted by RFC 5321)

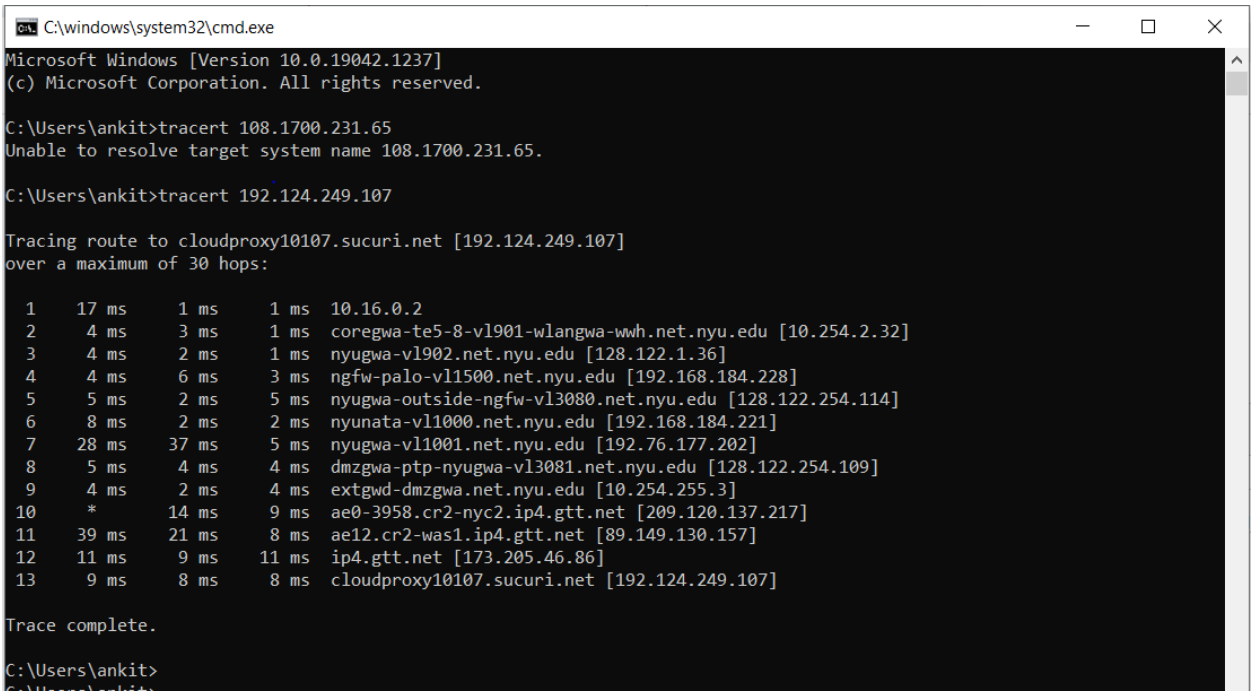
- RFC 2822 – Internet Message Format (Obsoletes RFC 822, Obsoleted by RFC 5322)
- RFC 3696 – Application Techniques for Checking and Transformation of Names
- RFC 4291 – IP Version 6 Addressing Architecture (Updated by RFC5952)
- RFC 5321 – Simple Mail Transfer Protocol (Obsoletes RFC 2821, Updates RFC 1123)
- RFC 5322 – Internet Message Format (Obsoletes RFC 2822)
- RFC 5952 – A Recommendation for IPv6 Address Text Representation (Updates RFC 4291)
- RFC 6530 – Overview and Framework for Internationalized Email (Obsoletes RFC 4952, 5504, 5825)

Reference:
https://en.wikipedia.org/wiki/Email_address

8. Network management Utilities

a. traceroute:

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route, one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. traceroute utilizes the IP protocol `time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.



b. ping:

The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings") have an IP and ICMP header, followed by a ``struct timeval" and then an arbitrary number of ``pad" bytes used to fill out the packet.

```
operable program or batch file.

C:\Users\ankit>ping 192.124.249.107

Pinging 192.124.249.107 with 32 bytes of data:
Reply from 192.124.249.107: bytes=32 time=12ms TTL=52
Reply from 192.124.249.107: bytes=32 time=13ms TTL=52
Reply from 192.124.249.107: bytes=32 time=8ms TTL=52
Reply from 192.124.249.107: bytes=32 time=10ms TTL=52

Ping statistics for 192.124.249.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 13ms, Average = 10ms

C:\Users\ankit>
```

c. nslookup is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non- interactive mode is used to print just the name and requested information for a host or domain.

```
C:\Users\ankit>nslookup 192.124.249.107
Server:  dns1-ha.noc.nyu.edu
Address:  128.122.0.11

Name:    cloudproxy10107.sucuri.net
Address:  192.124.249.107


C:\Users\ankit>
```

d. ipconfig

ipconfig is a utility that communicates with the IPConfiguration agent to retrieve and set IP configuration parameters. It should only be used in a test and debug context. Using it for any other purpose is strongly discouraged. Public API's in the SystemConfiguration framework are currently the only supported way to access and control the state of IPConfiguration.

```
Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6dc4:727f:ebd8:aec4%54
   IPv4 Address. . . . . . . . . . . : 172.23.96.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f1d7:41d1:8d32:8e31%15
   Autoconfiguration IPv4 Address. . : 169.254.142.49
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : nyu.edu
   Link-local IPv6 Address . . . . . : fe80::852b:4afa:3ded:dd67%17
   IPv4 Address. . . . . . . . . . . : 10.16.185.38
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.16.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\ankit>
```

e. dig

dig is useful for network troubleshooting and for educational purposes. It can operate based on command line option and flag arguments, or in batch mode by reading requests from an operating system file. When a specific name server is not specified in the command invocation, it uses the operating system's default resolver, usually configured in the file resolv.conf. Without any arguments it queries the DNS root zone.

```
; <<>> DiG 9.7.3 <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55976
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         353657  IN      CNAME   www.l.google.com.
www.l.google.com.       146     IN      A       74.125.236.19
www.l.google.com.       146     IN      A       74.125.236.20
www.l.google.com.       146     IN      A       74.125.236.16
www.l.google.com.       146     IN      A       74.125.236.17
www.l.google.com.       146     IN      A       74.125.236.18

;; AUTHORITY SECTION:
com.                    168931  IN      NS      e.gtld-servers.net.
com.                    168931  IN      NS      d.gtld-servers.net.
com.                    168931  IN      NS      b.gtld-servers.net.
com.                    168931  IN      NS      g.gtld-servers.net.
com.                    168931  IN      NS      f.gtld-servers.net.
com.                    168931  IN      NS      m.gtld-servers.net.
com.                    168931  IN      NS      c.gtld-servers.net.
com.                    168931  IN      NS      l.gtld-servers.net.
com.                    168931  IN      NS      j.gtld-servers.net.
com.                    168931  IN      NS      k.gtld-servers.net.
com.                    168931  IN      NS      a.gtld-servers.net.
com.                    168931  IN      NS      h.gtld-servers.net.
com.                    168931  IN      NS      i.gtld-servers.net.

;; Query time: 2 msec
;; SERVER: 192.168.0.254#53(192.168.0.254)
;; WHEN: Mon Jul 16 11:21:00 2012
;; MSG SIZE  rcvd: 356
```

ii. A few more utilities.

a. Netstat.
Netstat (Network Statistic) command display connection information, routing table information etc.

```
C:\Users\ankit>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.16.185.38:49464     40.83.240.146:https    ESTABLISHED
  TCP    10.16.185.38:49674     199.232.37.253:https   ESTABLISHED
  TCP    10.16.185.38:49675     60:https               ESTABLISHED
  TCP    10.16.185.38:49683     140:https              ESTABLISHED
  TCP    10.16.185.38:49941     173:https              ESTABLISHED
  TCP    10.16.185.38:51376     text-lb:https          ESTABLISHED
  TCP    10.16.185.38:51778     104.36.115.109:https   ESTABLISHED
  TCP    10.16.185.38:52274     63.251.28.234:https    ESTABLISHED
  TCP    10.16.185.38:52325     46:https               ESTABLISHED
  TCP    10.16.185.38:52342     104.17.120.107:https   ESTABLISHED
  TCP    10.16.185.38:52539     30:https               ESTABLISHED
  TCP    10.16.185.38:52799     30:http                TIME_WAIT
  TCP    10.16.185.38:53020     30:http                ESTABLISHED
^C
C:\Users\ankit>^Z
```

b. Arp: The arp utility displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol (arp(4)). With no flags, the program displays the current ARP entry for hostname. The host may be specified by name or by number, using Internet dot notation.

```
C:\Users\ankit>arp -a

Interface: 169.254.142.49 --- 0xf
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.16.185.38 --- 0x11
  Internet Address      Physical Address      Type
  10.16.0.1             00-00-5e-00-01-53     dynamic
  10.16.184.163         f0-18-98-a3-cf-01     dynamic
  10.16.255.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.23.96.1 --- 0x36
  Internet Address      Physical Address      Type
  172.23.111.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ankit>
```

9. Overlay Networks.
   a. In P2P systems, a peer can come or go without warning. To handle peer churn, we require each peer to track (that is, know the IP address of) its first and second successors. We also require each peer to periodically verify that its two successors are alive, by periodically sending ping messages to them and asking for responses.

   b. The Gnutella and Kad overlays provide a keyword-search function that allows users to locate files that have the keyword in the filename. Gnutella performs these lookups using an

unstructured topology, while Kad uses a DHT. BitTorrent, on the other hand, forms an overlay to facilitate the rapid transfer of large files to a large number of peers.

Kad: Kad is a Kademlia-based P2P search network used by the eMule P2P file-sharing software. To our knowledge, Kad is the largest deployed DHT, with more than 1 million simultaneous users. Similar to other DHTs, each peer has a persistent, globally-unique identifier of length b bits (in Kad's case b = 128 bits). Keywords are hashed to b bits and stored on the peer with the closest matching identifier. Each peer stores a structured routing table pointing to other nodes in the network such that the expected number of overlay hops to perform any lookup is O(log n), where n is the population size.

BitTorrent: BitTorrent is a popular P2P application for distributing very large files (100+ MB) to a large group of users. Unlike most P2P systems, which form one large overlay, BitTorrent has a distinct overlay for each file. To download a file, peers exchange different blocks of the content until each peer has the entire file. The peers locate one another using a rendezvous point, called a tracker, whose address is provided to new members out of band. Each new peer contacts the tracker via HTTP, periodically sends an update of its progress to the tracker, and informs the tracker when it departs. Each peer may receive the entire file across multiple sessions, i.e., it may obtain only a subset of blocks in one session and resume the download later.

Gnutella: Gnutella is currently one of the most popular P2P systems, with more than 1 million simultaneous users. It uses a two-tier overlay structure, similar to FastTrack and eDonkey. Most peers are leaf peers, while a small fraction of peers act as ultrapeers. The leaf peers connect to a handful of ultrapeers, which index the content of the leaves. Searches spread out from ultrapeers using a modified expanding-ring search.

Source:
http://conferences.sigcomm.org/imc/2006/papers/p19-stutzbach2.pdf