

Experiment -1

Network components, utilities, byte-order conversion functions

1.1 Aim: To identify, understand and demonstrate

- a Basic network elements and network utilities (commands/programs)
- b Network byte-order functions

1.2. Description:

Computer Network is collection of interconnection of autonomous computers. Ex. LANs. Computer networks are used to share hardware, software resources and services, to save money and increase the productivity.

a. Network components and utilities

Network components: There are several network components. Some of these are: *hosts, servers, clients, transmission media, shared data, shared printers and other peripherals, network interface card, local operating system, network operating system, hub, switch, router, gateways, firewalls* etc.

Network utilities: are basic utilities or tools are the programs/commands used for network troubleshooting / diagnosis. These tools include *ping, traceroute/tracert, lookup, whois, finger, netstat, ipconfig/ifconfig, nmap (port scan), dig* etc. most of the operating systems provide these tools.

Network operating systems: The operating systems like Windows, GNU/Linux, or Mac OS X etc. provide network support.

Host: A host may be computer or any other device that is attached to a network. These devices hold shared files, programs and network operating systems. It allows processes (applications) to run. These applications actually generate the information. These processes may be servers or clients.

Servers: Servers are the applications that provide network resource access to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are *file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers*, to name a few.

Clients: Clients are *applications that access and use the network and shared network resources*. Clients are basically the customers (users) of the network, as they request and receive services from the servers.

Transmission Media: Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable or wireless media. Transmission media are sometimes called channels, links or lines.

Shared data: Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.

Shared printers and other peripherals: Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, drives or any other items used by clients on the network.

Network Interface Card: Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents. Example: Ethernet Card, WiFi adapter etc.

Local Operating System: A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are *MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP* etc.

Network Operating System: The network operating system is a program that runs on computers and servers, and allows the computers to *communicate over the network*.

Hub: Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Switch: Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.

Like a hub, switch doesn't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

ping: Is a network diagnostic tool used to check the liveness of a connection or host. It sends ICMP echo request packets to a destination. These packets ask the remote destination to reply. If the remote host is configured to reply, it will respond with reply packet. It will also give the statistics like round trip time, packet loss etc.

Syntax:

`$ ping <IP Address or domain name>`

tracert (Windows)/tracert (Linux like Oss): These are similar to ping command but, it additionally gives the path the packet takes from the source to destination. It sends packets to remote destination

asking each internet router along the way to reply. This command will give the information like hops, delays(min, max, average) between the routers and their IPs or domains.

Syntax:

```
# traceroute <domain name or IP Address>
```

Ipconfig (Windows)/ifconfig (Linux like OSs): Allows us to configure or view information about the network interfaces. It can be used to view all the configured network interfaces, IP addresses, DNS servers, subnet mask, gateways and other information. We can also enable, disable network interfaces, and flush the DNS cache, forcing the Operating System to get new IP addresses from the DHCP server. It helps to troubleshoot network problems. *Ex: # nslookup cbir.ac.in*

```
$nslookup <Domain name>
```

nslookup: Used to look up the IP Addresses associated with a domain name. it also allows us to perform a reverse lookup to find the domain name associated with an IP address. *Ex: # nslookup 210.212.217.73* will show the associate domain name

whois: This command is not associated with Windows. It looks up the registration associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information.

```
$whois <Domain name>
```

netstat: netstat stands for network statistics. This command displays incoming and outgoing network connections as well as other network information. It's available on Windows, Mac, and Linux — each version has its own command-line options you can tweak to see different types of information.

```
$netstat
```

finger: It is similar to who command but gives more information than who. The finger command is old and is no longer widely used

```
$finger
```

Port Scan / nmap: This utility is a common tool used for port scans, but there are many utilities that can run this sort of scan. A port scan is the process of attempting to connect to every port on a computer — ports 1 through 65535 — and seeing if they're open. An attacker might port-scan a system to find vulnerable services or you may port scan our own computer to ensure that there are no vulnerable services listening to the network.

b.Network-byte order functions: Computers may not store the data (comprising more than one byte) in the same order. For example, a data item with 16-bit (2bytes) can be stored in two ways:

- **Little Endian:** In this scheme, low-order byte is stored on the address starting address (**A**) and the high-order byte is stored on the next address (**A+1**).
- **Big Endian:** In this scheme, high-order byte is stored on the address starting address (**A**) and the low-order byte is stored on the next address (**A+1**).

But the network protocols are designed for big-endian notation. To allow the machines to communicate with different byte-orders, we need conversion functions. the byte-order conversion functions are:

Table 1: Network byte-order conversion functions

| Function | Description |
|----------|---------------------------------------------------------------------------------|
| htons() | Converts a Host-byte(Little-Endian) order short integer into Network byte-order |
| htonl() | Converts a Host-byte(Little-Endian) order long integer into Network byte-order |
| ntohl() | Converts a Network-byte(Big-Endian) order short integer into Host-byte-order |
| ntohs() | Converts a Network-byte(Big-Endian) order short integer into Host-byte-order |

Source: https://www.tutorialspoint.com/unix_sockets/network_byte_orders.htm

Note: All functions take unsigned short/long integers and returns unsigned short/long integers according to the respective order.

For example, we store the two-byte value 0x0102 in the short integer and then look at the two consecutive bytes c[0] (the address A) and c[1] (the address A+1) to determine the byte-order, the code will be:

```
#include <stdio.h>

int main(int argc, char **argv) {

    union {
        short s;
        char c[sizeof(short)];
    }un;

    un.s = 0x0102;

    if (sizeof(short) == 2) {
        if (un.c[0] == 1 && un.c[1] == 2)
            printf("big-endian\n");

        else if (un.c[0] == 2 && un.c[1] == 1)
            printf("little-endian\n");

        else
            printf("unknown\n");
    }
    else {
        printf("sizeof(short) = %d\n", sizeof(short));
    }

    exit(0);
}
```

An output generated by this program on a Pentium machine is as follows –

```
$> gcc byteorder.c
$> ./a.out
little-endian
$>
```

Task: Write a program to display the hexadecimal number 0x56AB in big-endian and little-endian formats (both in decimal and hexadecimal systems)

1.3 Experimentation results and discussion:

Network components identified in our lab-3:

i. Hardware information

Configuration of my system :
 Network card Type and make :
 Transmission media and connectors :
 Topology and LAN type : Star/Bus/Ring/FDDI/Wireless
 Wireless adapters :

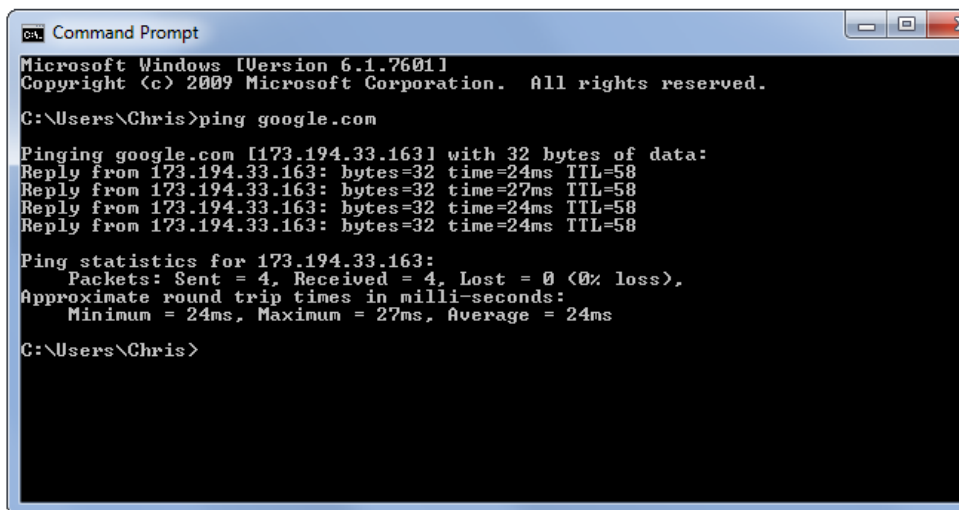
ii. Network information

Communication protocol suites :
 Hardware/physical address :
 IP address :
 Subnet mask :
 Gateway :
 DNS :

Network utilities:

ping:

- Ping tool is tested from my DOS command prompt and a sample snapshot is shown in Figure 1.1.



```

C:\Users\Chris>ping google.com

Pinging google.com [173.194.33.163] with 32 bytes of data:
Reply from 173.194.33.163: bytes=32 time=24ms TTL=58
Reply from 173.194.33.163: bytes=32 time=27ms TTL=58
Reply from 173.194.33.163: bytes=32 time=24ms TTL=58
Reply from 173.194.33.163: bytes=32 time=24ms TTL=58

Ping statistics for 173.194.33.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 27ms, Average = 24ms

C:\Users\Chris>
  
```

Figure 1.1: Sample snapshot of ping command

- Used 'ping' to test the connection and the liveness of the host '**google.com**'.
- The reply tells that the network software in my machine is working and the connection from my host to google is working and the host google is reachable (live).
- Also, it shows that the packet loss is zero, the RTT from my host to google is 24ms (minimum), 27ms (maximum) and 24ms (Average).

tracert:

- Tested from my DOS prompt to by passing the '**google.com**' as an argument and the response is shown in the figure 1.2.

```

CA: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Chris>tracert google.com

Tracing route to google.com [173.194.33.169]
over a maximum of 30 hops:

  0  2 ms    1 ms    1 ms  192.168.1.254
  1  7 ms    7 ms    9 ms  10.31.188.1
  2 11 ms   34 ms   19 ms  STILLWABCI01.bb.telus.com [75.154.217.108]
  3 11 ms   11 ms   10 ms  74.125.49.177
  4 11 ms   11 ms   10 ms  209.85.249.34
  5 11 ms   11 ms   11 ms  209.85.244.65
  6 11 ms   10 ms   11 ms  sea09s18-in-f9.1e100.net [173.194.33.169]

Trace complete.

C:\Users\Chris>

```

Figure 1.2: Sample snapshot of tracert google.com command

- From the results, it can be understood that destination machine i.e. **google** is live and reachable and the number of hops between our router to google router is **7**.
- It also displayed the intermediate router information along with the delays between routers.
- We can also understand that the delay between **10.31.188.1** to **175.154.217.108** is more.

Ipconfig:

- Tested DOS prompt and the response is shown in Fig 1.3.

```

CA: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Chris>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Laptop
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : telus

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : telus
Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Physical Address. . . . . : 68-5D-43-66-0B-0C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::799d:c5a7:c72:b925%11(Preferred)
IPv4 Address. . . . . : 192.168.1.66(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : June-01-14 12:41:11 PM
Lease Expires . . . . . : June-03-14 12:41:11 AM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

```

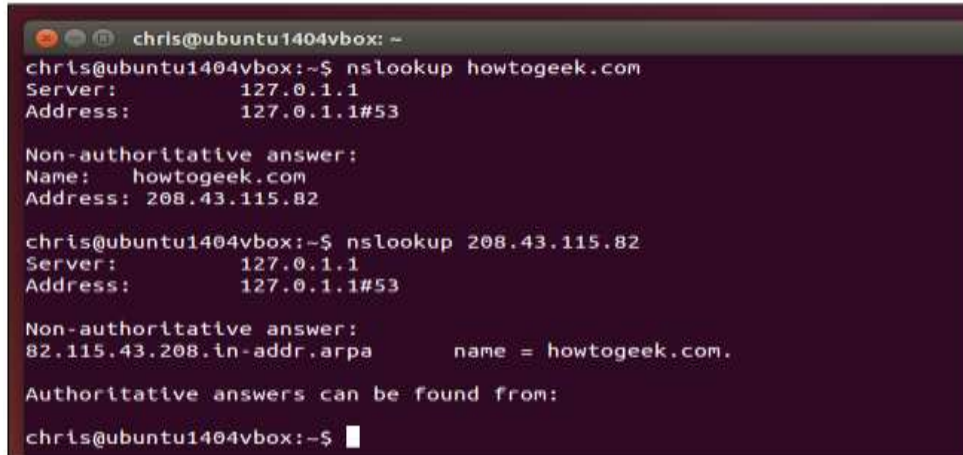
Figure 1.3: Sample snapshot of ipconfig command

- Displayed the host name and other network related information
- From the results it is understood that the machine is connected using wireless interface and its vendor is **Intel Centrino**, MAC address: **68-5D-43-66-0B-0C**, IP address is: **192.168.1.66** , IP

address life time, subnet mask: **255.255.0.0**, gateway address as **192.168.1.254**, DHCP address as **8.8.8.8**, primary and the secondary DNS address as **8.8.4.4**

nslookup:

- Tested this command from my Linux machine to check the IP address details associated with 'howtogeek' domain. A sample snapshot of this command response is shown in Fig 1.4.



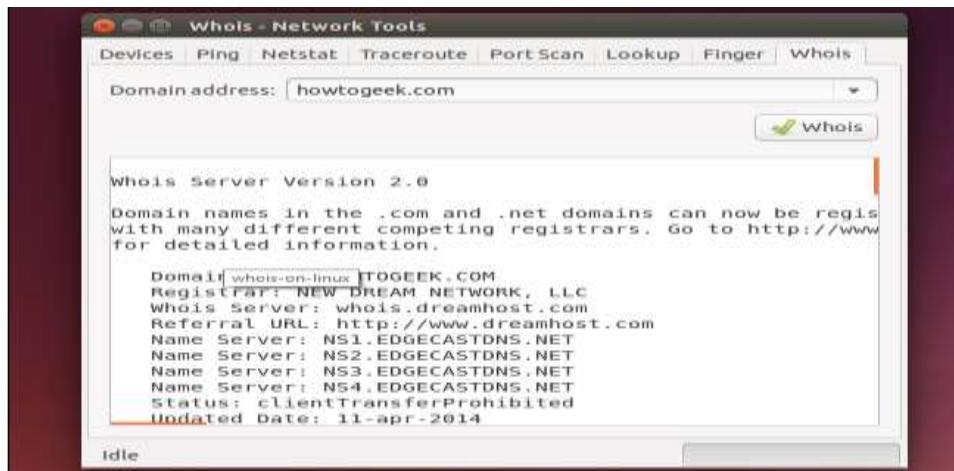
```
chris@ubuntu1404vbox: ~  
chris@ubuntu1404vbox:~$ nslookup howtogeek.com  
Server:      127.0.1.1  
Address:     127.0.1.1#53  
  
Non-authoritative answer:  
Name:   howtogeek.com  
Address: 208.43.115.82  
  
chris@ubuntu1404vbox:~$ nslookup 208.43.115.82  
Server:      127.0.1.1  
Address:     127.0.1.1#53  
  
Non-authoritative answer:  
82.115.43.208.in-addr.arpa      name = howtogeek.com.  
  
Authoritative answers can be found from:  
  
chris@ubuntu1404vbox:~$
```

Figure 1.4: A sample snapshot for ipconfig command

- The DNS server IP address and port number associated with the domain 'howtogeek' is 127.0.1.1 and 127.0.1.1#53 and the IP address of 'howtogeek' host is 208.43.115.82.

whois:

- This command is tested by using the Linux network utilities tool to check the registration details of the domain 'howtogeek'. The corresponding response is shown in Fig 1.5.



```
Whois - Network Tools  
Domain address: howtogeek.com  
Whois  
  
Whois Server Version 2.0  
Domain names in the .com and .net domains can now be regis  
with many different competing registrars. Go to http://www  
for detailed information.  
  
Domain: whois-on-linux | HOWGEEK.COM  
Registrar: NEW DREAM NETWORK, LLC  
Whois Server: whois.dreamhost.com  
Referral URL: http://www.dreamhost.com  
Name Server: NS1.EDGECASTDNS.NET  
Name Server: NS2.EDGECASTDNS.NET  
Name Server: NS3.EDGECASTDNS.NET  
Name Server: NS4.EDGECASTDNS.NET  
Status: clientTransferProhibited  
Updated Date: 11-apr-2014  
idle
```

Figure 1.5: A sample snapshot of whois command

- The whois server version is 2.0
- Domain registrar is New Dream Network , URL is <http://www.dreamhost.com>

- The 'howtogeek' has 4 DNSes named NS1.EDGECASTONS.NET, NS2.EDGECASTONS.NET, NS3.EDGECASTONS.NET and NS4.EDGECASTONS.NET
- Its last update was 11th April 2014

netstat:

- Tested the command from my DOS command prompt. A sample output is shown in Fig 1.6.

```

Administrator: Command Prompt - netstat -b
[googledrivesync.exe]
TCP 127.0.0.1:58778 Laptop:58779 ESTABLISHED
[Battle.net.exe]
TCP 127.0.0.1:58779 Laptop:58778 ESTABLISHED
[Battle.net.exe]
TCP 127.0.0.1:65001 Laptop:49184 ESTABLISHED
[Invstreamsvc.exe]
TCP 192.168.1.66:2869 192.168.1.254:58286 TIME_WAIT
TCP 192.168.1.66:49210 74.125.129.125:https ESTABLISHED
[chrome.exe]
TCP 192.168.1.66:49233 pc-in-f188:5228 ESTABLISHED
[chrome.exe]
TCP 192.168.1.66:49234 74.125.129.125:5222 ESTABLISHED
[chrome.exe]
TCP 192.168.1.66:49290 74.125.129.125:5222 ESTABLISHED
[pidgin.exe]
TCP 192.168.1.66:49295 bos-m010c-new-rdr2:https ESTABLISHED
[pidgin.exe]
TCP 192.168.1.66:49299 chat-d02c-rdr2:https ESTABLISHED
[pidgin.exe]
TCP 192.168.1.66:49316 do-4:https ESTABLISHED
[chrome.exe]
TCP 192.168.1.66:49325 netstat-b-on-windows 25:5222 ESTABLISHED
[googledrivesync.exe]

```

Figure 1.6 : A sample snapshot of 'nstat' command

- Write your observations and analysis

finger:

- Demonstrated the use of this command from the Linux network utilities.

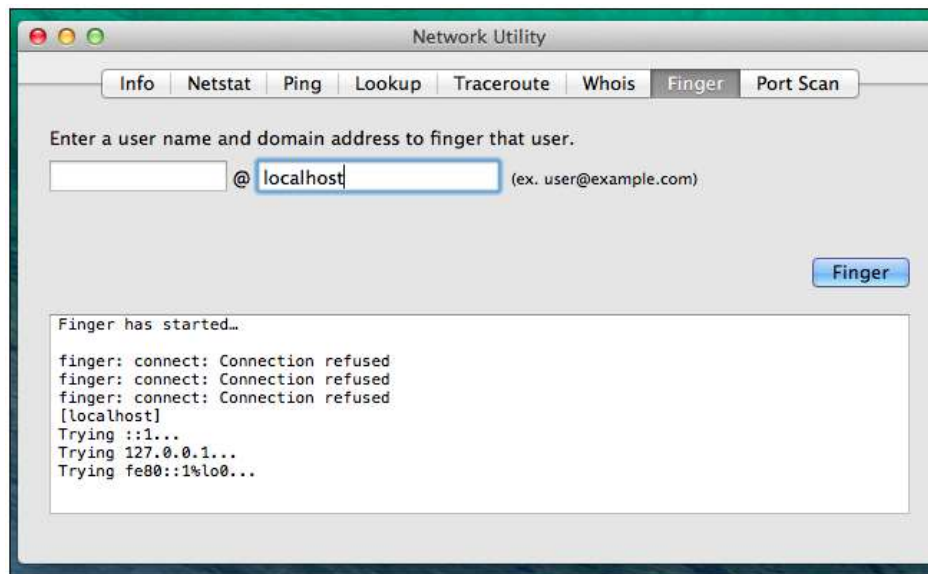


Figure 1.7: A sample snapshot of 'finger' command

- Test with the host 'cbit.ac.in' and write your observations and analysis

Nmap:

- Tested the open ports on the local machine and the results are shown in Fig. 1.8.

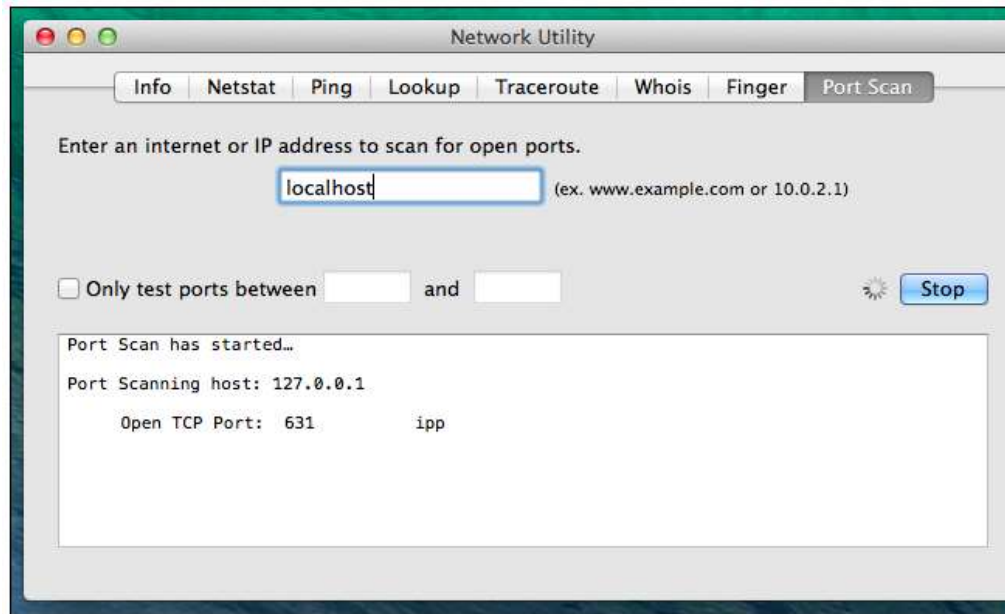


Figure 1.8: Sample response to the 'nmap' command

- Test the services on the host 'cbit.ac.in' and write your observations

1.4 Conclusions:

- We have identified various network components and utilities from the literature survey
- Identified various network components, transmission media, topology in our lab and determined the network information like IP addresses, DNS, Gateway etc.
- Demonstrated the basic network utilities like *ping*, *ipconfig/ifconfig*, *tracert/traceroute*, *whois*, *finger*, *netstat*, *nslookup*, *nmap*.
- Demonstrated the use of byte-order conversion functions
- However, still there are several other network tools which are available.

References:

- https://en.wikiversity.org/wiki/Basic_computer_network_components
- <https://centralops.net/co/> //tools for online usage
- <http://network-tools.com/>
- <http://pingtool.org/>
- <http://ping.eu/bandwidth/>
- <http://www.nmonitoring.com/>
- <http://www.howtogeek.com/190148/8-common-network-utilities-explained/>
- <https://centralops.net/co/>
- http://www.tutorialspoint.com/unix_system_calls/socket.htm socket tutorials