Mawlana Bhashani Science and Technology University
Lab-Report

Report No:02
Course code: ICT-3207
Course title: Computer Network Lab
Date of Performance :25-11-20:
Date of Submission: 25-11-20

Submitted by

Name: MD. Abdullah Al Mamun
ID:IT-18040
3th year 2ndsemester
Session: 2017-2018
Dept. of ICT
MBSTU.

Submitted To

Nazrul Islam
Assistant Professor
Dept. of ICT
MBSTU.

1. PING :The **ping command** is one of the most used tools for troubleshooting, testing, and diagnosing network connectivity issues. **Ping** works by sending one or more ICMP (Internet Control Message Protocol) Echo Request packages to a specified destination IP on the network and waits for a reply.

```
abdullah@abdullah-VirtualBox: ~

File  Edit  View  Search  Terminal  Help
abdullah@abdullah-VirtualBox:~$ ping www.google.com
PING www.google.com (216.58.196.4) 56(84) bytes of data.
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=1 ttl=107 time=1
69 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=2 ttl=107 time=1
51 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=3 ttl=107 time=1
53 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=4 ttl=107 time=9
36 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=5 ttl=107 time=1
98 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=6 ttl=107 time=1
35 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=7 ttl=107 time=1
48 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=8 ttl=107 time=1
44 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=9 ttl=107 time=1
42 ms
64 bytes from kul01s11-in-f4.1e100.net (216.58.196.4): icmp_seq=10 ttl=107 time=
```
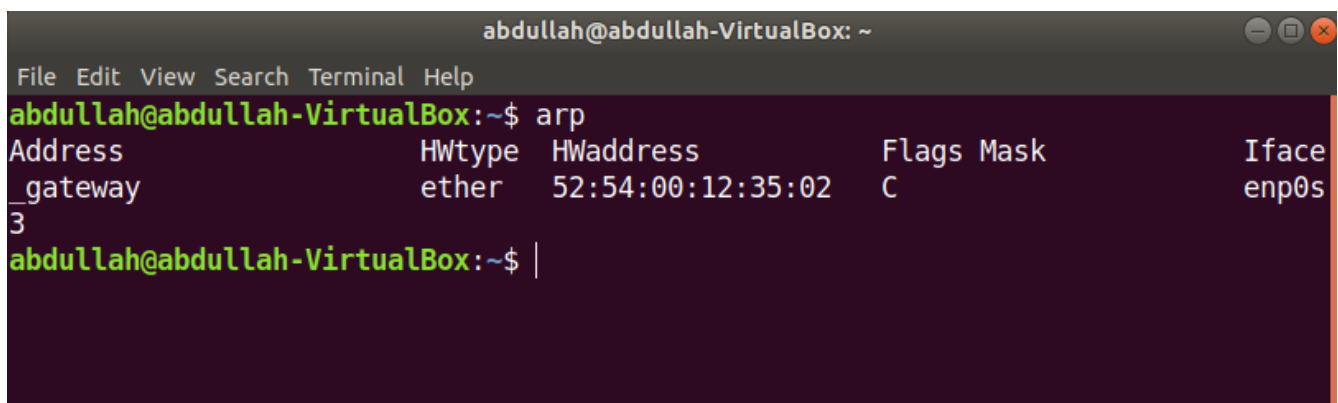
2. CURL : **Linux curl command** is used to download or upload data to a server via supported protocols such as HTTP, FTP, IMAP, SFTP, TFTP, IMAP, POP3, SCP, etc. It is a remote utility, so it works without user interaction. The data transfer from one place to another is one of the vital and most used tasks of a computer system.

```
abdullah@abdullah-VirtualBox: ~

File  Edit  View  Search  Terminal  Help
abdullah@abdullah-VirtualBox:~$ curl -o web.html https://www.youtube.com/watch?v=7bFVuk17Dls
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  684k    0  684k    0     0   156k      0 --:--:--  0:00:04 --:--:--   156k
abdullah@abdullah-VirtualBox:~$ 
```

3. ARP :
The ARP commands to view, display, or modify the details/information in an ARP table/ cache.

The ARP cache or table has the dynamic list of IP and MAC addresses of those devices to which your computer has communicated recently in a local network. The purpose of maintaining an ARP table is that when you want to communicate with another device, your device does not need to send the ARP request for the MAC address of that device.

4.DIG : **Linux dig command** stands for Domain Information Groper.
This **command** is used for tasks related to DNS lookup to **query** DNS name servers. It mainly deals with troubleshooting DNS related problems. It is a flexible utility for examining the DNS (Domain Name Servers).

abdullah@abdullah-VirtualBox: ~

File Edit View Search Terminal Help

abdullah@abdullah-VirtualBox:~$ dig yahoo.com

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48337
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITION
AL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;yahoo.com.   IN   A

;; ANSWER SECTION:
yahoo.com.   1159   IN   A   98.137.11.164
yahoo.com.   1159   IN   A   74.6.143.25
yahoo.com.   1159   IN   A   98.137.11.163
yahoo.com.   1159   IN   A   74.6.143.26
yahoo.com.   1159   IN   A   74.6.231.21
yahoo.com.   1159   IN   A   74.6.231.20

5.httpie:

HTTPie – A Modern HTTP Client Similar to Curl and Wget Commands. HTTPie (pronounced aitch-tee-tee-pie) is a cURL-like, modern, user-friendly, and cross-platform command line HTTP client written in Python. It is designed to make CLI interaction with web services easy and as user-friendly as possible

```
abdullah@abdullah-VirtualBox:~$ http -p Hh https://google.com
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Host: google.com
User-Agent: HTTPie/0.9.8

HTTP/1.1 301 Moved Permanently
Alt-Svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=259
2000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;
 v="46,43"
Cache-Control: public, max-age=2592000
Content-Length: 220
Content-Type: text/html; charset=UTF-8
Date: Wed, 25 Nov 2020 02:04:18 GMT
Expires: Fri, 25 Dec 2020 02:04:18 GMT
Location: https://www.google.com/
Server: gws
X-Frame-Options: SAMEORIGIN
```

6. IFCONFIG:

ifconfig is used to configure the system's kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging, or when system tuning is needed. If no arguments are given, ifconfig displays the status of the system's active interfaces

```
abdullah@abdullah-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::70ef:c804:58a4:1afb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:dc:b9:7c  txqueuelen 1000  (Ethernet)
        RX packets 318136  bytes 439962444 (439.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 145221  bytes 13238172 (13.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 11432  bytes 650837 (650.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

7.NC :

ncat or nc is networking utility with functionality similar to cat command but for network. It is a general purpose CLI tool for reading, writing, redirecting data across a network. It is designed to be a reliable back-end tool that can be used with scripts or other programs.

```
abdullah@abdullah-VirtualBox:~$ nc -h
OpenBSD netcat (Debian patchlevel 1.187-1ubuntu0.1)
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M tt
l]
          [-m minttl] [-O length] [-P proxy_username] [-p source_
port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W r
ecvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]
  [destination] [port]
        Command Summary:
                -4              Use IPv4
                -6              Use IPv6
                -b              Allow broadcast
                -C              Send CRLF as line-ending
                -D              Enable the debug socket option
```

8.NGREP :

ngrep – A Network Packet Analyzer for **Linux**
1. **Ngrep** (network grep) is a simple yet powerful network packet analyzer. ...
2. The following **command** will help you match all ping requests on the default working interface. ...
3. To match only traffic going to a particular destination site, for instance 'google.com', run the following **command**, then try to access it from a browser.

```
abdullah@abdullah-VirtualBox:~$ ngrep -h
usage: ngrep <-hNXViwqpevxlDtTRM> <-IO pcap_dump> <-n num> <-d dev> <-A num>
             <-s snaplen> <-S limitlen> <-W normal|byline|single|none> <-c cols>
             <-P char> <-F file>              <-K count>
             <match expression> <bpf filter>
   -h  is help/usage
   -V  is version information
   -q  is be quiet (don't print packet reception hash marks)
   -e  is show empty packets
   -i  is ignore case
   -v  is invert match
   -R  is don't do privilege revocation logic
   -x  is print in alternate hexdump format
   -X  is interpret match expression as hexadecimal
   -w  is word-regex (expression must match as a word)
   -p  is don't go into promiscuous mode
   -l  is make stdout line buffered
   -D  is replay pcap dumps with their recorded time intervals
```

9.Route:

route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static **routes** to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.

```
abdullah@abdullah-VirtualBox:~$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
abdullah@abdullah-VirtualBox:~$  sudo route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
abdullah@abdullah-VirtualBox:~$
```

10 : ss :

The **ss command** is a tool used to dump socket statistics and displays information in similar fashion (although simpler and faster) to netstat. The **ss command** can also display even more TCP and state information than most other tools.

```
abdullah@abdullah-VirtualBox:~$ ss | more
Netid State    Recv-Q    Send-Q                            Local Addr
ess:Port                                            Peer Address:Port

u_seq ESTAB    0         0                                          @00
012 38312                                                     * 3831
3
u_str ESTAB    0         0                            @/tmp/dbus-c5X06bb
8yo 27214                                                    * 2721
3
u_str ESTAB    0         0                         /run/systemd/journal/std
out 25016                                                    * 2501
4
```

11 .wget:

Wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.
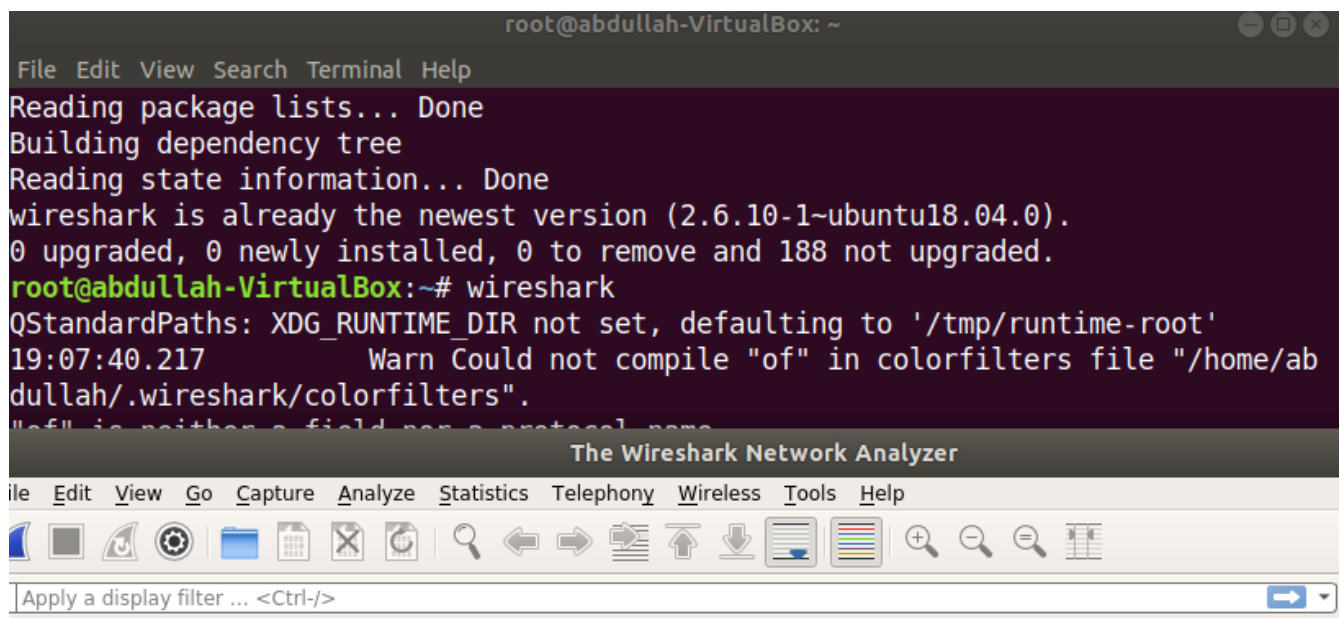
```
                    abdullah@abdullah-VirtualBox: ~                    ⊖ ⊡ ⊗
File  Edit  View  Search  Terminal  Help
abdullah@abdullah-VirtualBox:~$ wget https://www.google.com/doodles/gerardus-mer
cators-503rd-birthday
--2020-11-25 14:12:37--  https://www.google.com/doodles/gerardus-mercators-503rd
-birthday
Resolving www.google.com (www.google.com)... 172.217.31.196, 2404:6800:4007:809:
:2004
Connecting to www.google.com (www.google.com)|172.217.31.196|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2515330 (2.4M) [text/html]
Saving to: 'gerardus-mercators-503rd-birthday'

gerardus-mercators- 100%[===================>]   2.40M   189KB/s    in 17s

2020-11-25 14:12:58 (144 KB/s) - 'gerardus-mercators-503rd-birthday' saved [2515
330/2515330]
```

12. wireshark:

Wireshark is a popular open source graphical user interface (GUI) tool for analyzing packets. However, it also provides a powerful **command**-line utility called TShark for people who prefer to work on the **Linux command** line.

File   Edit   View   Search   Terminal   Help

Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (2.6.10-1~ubuntu18.04.0).
0 upgraded, 0 newly installed, 0 to remove and 188 not upgraded.
root@abdullah-VirtualBox:~# wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
19:07:40.217   Warn Could not compile "of" in colorfilters file "/home/ab
dullah/.wireshark/colorfilters".

The Wireshark Network Analyzer

ile   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...   All interfaces shown

| enp0s3 |
| any |
| Loopback: lo |
| nflog |
| nfqueue |
| usbmon1 |
| Cisco remote capture: ciscodump |
| Random packet generator: randpkt |