Unix lab

Experiment no. 3: To study and execute Unix networking commands.

Content:

Online linux link: https://bellard.org/jslinux/vm.html?url=buildroot-x86.cfg
Or simply https://bellard.org/jslinux and then selecting x86 Linux 4.12.0 Buildroot
Or use cygwin

Command	Use
ifconfig	To configure the kernel-resident network interfaces
ping	To test the connection between the local server/computer and a remote UNIX server
traceroute	To show how a data transmission travelled from a local machine to a remote one
netstat	To display network connections (both incoming and outgoing), routing tables, and a number of network interface statistics
nslookup	To get information from DNS server
hostname	To obtain DNS name
tcpdump	Command line packet sniffer

Complete run of above commands:

```
erKashif-Pc+erKashifK@erKashif-Pc ~
$ ping google.com

Pinging google.com [172.217.174.238] with 32 bytes of data:
Reply from 172.217.174.238: bytes=32 time=2ms TTL=248
Reply from 172.217.174.238: bytes=32 time=2ms TTL=248
Reply from 172.217.174.238: bytes=32 time=2ms TTL=248
Reply from 172.217.174.238: bytes=32 time=2ms TTL=248

Ping statistics for 172.217.174.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms


erKashif-Pc+erKashifK@erKashif-Pc ~
$ netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49716        erKashif-Pc:49717      ESTABLISHED
  TCP    127.0.0.1:49717        erKashif-Pc:49716      ESTABLISHED
  TCP    172.16.64.55:56577     sa-in-f188:5228        ESTABLISHED
  TCP    172.16.64.55:56638     104.17.64.4:https      TIME_WAIT
  TCP    172.16.64.55:56657     103.231.98.196:https   ESTABLISHED
  TCP    172.16.64.55:56683     unknown:https          ESTABLISHED
  TCP    172.16.64.55:56776     a104-120-71-193:https  ESTABLISHED
  TCP    172.16.64.55:56840     bom07s15-in-f14:https  ESTABLISHED
  TCP    172.16.64.55:56843     bom05s12-in-f14:https  ESTABLISHED
  TCP    172.16.64.55:56844     server-13-227-234-57:https  TIME_WAIT
  TCP    172.16.64.55:56845     104.20.187.5:https     TIME_WAIT
  TCP    172.16.64.55:56848     server-13-227-185-225:https  TIME_WAIT
  TCP    172.16.64.55:56850     server-99-86-162-2:https  TIME_WAIT
  TCP    172.16.64.55:56852     104.17.64.4:https      ESTABLISHED
  TCP    172.16.64.55:56853     a23-52-73-61:https     CLOSE_WAIT
  TCP    172.16.64.55:56854     server-99-86-162-14:https  ESTABLISHED
  TCP    172.16.64.55:56855     amidt:https            CLOSE_WAIT
```

Try netstat –a (to list all sockets) netstat –at (to list all TCP ports) netstat –au (to list all UDP ports) netstat –l (to list all listening ports)

```
erKashif-Pc+erKashifK@erKashif-Pc ~
$ nslookup google.com
Non-authoritative answer:
Server:  UnKnown
```

Unix lab

Experiment no. 3: To study and execute Unix networking commands.

```
Address:  172.16.1.1

Name:    google.com
Addresses:  2404:6800:4009:80f::200e
          172.217.174.238


erKashif-Pc+erKashifK@erKashif-Pc ~
$ hostname
erKashif-Pc

erKashif-Pc+erKashifK@erKashif-Pc ~
$ hostname -A
erKashif-Pc.it.com erKashif-Pc.it.com

erKashif-Pc+erKashifK@erKashif-Pc ~
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:7E:C0:E3:22:BC
          inet addr:10.5.182.201  Bcast:10.5.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8568 (8.3 KiB)  TX bytes:1282 (1.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

erKashif-Pc+erKashifK@erKashif-Pc ~
$ traceroute google.com

traceroute to google.com (172.217.6.78), 30 hops max, 38 byte packets
 1  10.5.0.1 (10.5.0.1)  270.305 ms  261.935 ms  255.064 ms
 2  172.17.0.1 (172.17.0.1)  267.495 ms  259.044 ms  257.800 ms
 3  107.170.233.253 (107.170.233.253)  259.491 ms  265.875 ms  255.440 ms
 4  138.197.248.206 (138.197.248.206)  254.900 ms  138.197.248.222 (138.197.248.
222)  261.266 ms  138.197.248.206 (138.197.248.206)  260.300 ms
 5  138.197.244.233 (138.197.244.233)  262.620 ms  260.175 ms  138.197.244.237 (
138.197.244.237)  259.045 ms
 6  138.68.33.9 (138.68.33.9)  264.150 ms  263.341 ms  266.219 ms
 7  *  *  *
 8  72.14.239.42 (72.14.239.42)  264.985 ms  108.170.243.1 (108.170.243.1)  269.
239 ms  269.460 ms
 9  209.85.247.55 (209.85.247.55)  262.760 ms  108.170.243.13 (108.170.243.13)
256.871 ms  267.090 ms
10  74.125.253.151 (74.125.253.151)  263.465 ms  259.774 ms  sfo07s17-in-f14.1e1
00.net (172.217.6.78)  257.060 ms


erKashif-Pc+erKashifK@erKashif-Pc ~
$ nslookup google.com
Server:         10.5.0.1
Address:        10.5.0.1:53

Non-authoritative answer:
Name:   google.com
Address: 172.217.6.78

Non-authoritative answer:
Name:   google.com
Address: 2607:f8b0:4005:807::200e

erKashif-Pc+erKashifK@erKashif-Pc ~
$ tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:22:59.639897 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:00.646098 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:01.688188 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:02.729833 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:03.765827 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:04.806127 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:05.845182 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
```

Unix lab

Experiment no. 3: To study and execute Unix networking commands.

```
13:23:06.887307 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:07.921222 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:08.969135 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:10.006674 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:11.042444 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:12.090189 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:13.127687 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:14.164463 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:15.203168 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:16.247628 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:17.290480 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:18.329690 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:19.365515 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:20.410094 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:21.448474 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:22.490865 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
13:23:23.528807 ARP, Request who-has 10.5.0.1 tell 10.5.182.201, length 28
^Z[2]+  Stopped                    tcpdump
```