**CS3377.0W1 Week 10 Lab 1**

**Drew Pulliam - DTP180003**

**(Documentation with Terminal Log)**

┌────────────────────────────────────────────────────────────────────┐

│ • MobaXterm 20.2 • │

│ (SSH client, X-server and networking tools) │

│ │

│ → SSH session to dtp180003@cslinux1.utdallas.edu │

│ • SSH compression : v │

│ • SSH-browser : v │

│ • X11-forwarding : v (remote display is forwarded through SSH) │

│ • DISPLAY : v (automatically set on remote server) │

│ │

│ → For more info, ctrl+click on help or visit our website │

└────────────────────────────────────────────────────────────────────┘

1. **Ping** [**www.utdallas.edu**](http://www.utdallas.edu) **(use a count of 4 so it stops after 4 pings)**

{cslinux1:~} ping www.utdallas.edu -c 4

PING www.utdallas.edu (10.182.71.70) 56(84) bytes of data.

64 bytes from lb-int-ti-1a.utdallas.edu (10.182.71.70): icmp\_seq=1 ttl=248 time=0.790 ms

64 bytes from lb-int-ti-1a.utdallas.edu (10.182.71.70): icmp\_seq=2 ttl=248 time=0.829 ms

64 bytes from lb-int-ti-1a.utdallas.edu (10.182.71.70): icmp\_seq=3 ttl=248 time=0.824 ms

64 bytes from lb-int-ti-1a.utdallas.edu (10.182.71.70): icmp\_seq=4 ttl=248 time=0.839 ms

--- www.utdallas.edu ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3002ms

rtt min/avg/max/mdev = 0.790/0.820/0.839/0.034 ms

1. **Traceroute to** [**www.utdallas.edu**](http://www.utdallas.edu)

{cslinux1:~} traceroute www.utdallas.edu

traceroute to www.utdallas.edu (10.182.71.70), 30 hops max, 60 byte packets

1 utdig1-92.utdallas.edu (129.110.92.1) 13.986 ms 13.970 ms 13.937 ms

2 129.110.90.110 (129.110.90.110) 0.416 ms 0.410 ms 13.932 ms

3 corephy-xe-2-0-7.utdallas.edu (10.222.4.187) 0.961 ms 0.960 ms 1.160 ms

4 \* \* \*

5 pa-eth-2-14-unit-600.utdallas.edu (10.222.1.2) 1.023 ms 1.001 ms 0.929 ms

6 \* \* \*

7 vwn9kcore1-eth2-52.utdallas.edu (10.222.0.33) 1.272 ms 1.244 ms 1.271 ms

8 lb-int-ti-1a.utdallas.edu (10.182.71.70) 0.920 ms 0.866 ms 0.868 ms

**3. Netstat (first do netstat -aopt)**

{cslinux1:~} netstat -aopt

(No info could be read for "-p": geteuid()=633083 but you should be root.)

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name Timer

tcp 0 0 0.0.0.0:33780 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:43605 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:ssh 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:ipp 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 9 0 0.0.0.0:hbci 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:smtp 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhos:x11-ssh-offset 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6011 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6012 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6013 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6014 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:42238 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:33822 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6015 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:6016 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 localhost:smux 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:52622 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 0.0.0.0:sunrpc 0.0.0.0:\* LISTEN - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:60925 ESTABLISHED - keepalive (2772.30/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:64163 ESTABLISHED - keepalive (6999.37/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63747 ESTABLISHED - keepalive (1363.28/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:58984 ESTABLISHED - keepalive (6606.16/0/0)

tcp 7 0 localhost:hbci localhost:50254 CLOSE\_WAIT - off (0.00/0/0)

tcp 7 0 localhost:hbci localhost:50140 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:59460 ESTABLISHED - keepalive (3591.50/0/0)

tcp 1 0 localhost:hbci localhost:50566 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-125-:16269 ESTABLISHED - keepalive (6704.43/0/0)

tcp 1 0 localhost:hbci localhost:50466 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utd:cycleserv2 10.182.21.35:nfs ESTABLISHED - keepalive (15.41/0/0)

tcp 0 0 cslinux1.utdallas.e:850 csbinlet7.utdallas.:nfs ESTABLISHED - keepalive (3.57/0/0)

tcp 0 1792 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:64160 ESTABLISHED - on (0.09/0/0)

tcp 7 0 cslinux1.utdallas.:hbci cslinux1.utdallas:33896 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-12:omnisky ESTABLISHED - keepalive (6442.29/0/0)

tcp 0 0 cslinux1.utdallas:53800 oitpipa02.ipa.utda:ldap ESTABLISHED - keepalive (6540.59/0/0)

tcp 0 0 cslinux1.utdallas.e:976 10.182.21.22:nfs ESTABLISHED - keepalive (21.17/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63898 ESTABLISHED - keepalive (4738.35/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63748 ESTABLISHED - keepalive (1396.02/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63897 ESTABLISHED - keepalive (4721.97/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-12:rich-cp ESTABLISHED - keepalive (6458.67/0/0)

tcp 0 0 cslinux1.utd:netviewdm3 10.182.21.24:nfs ESTABLISHED - keepalive (3.63/0/0)

tcp 1 0 localhost:hbci localhost:50476 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas:59894 csf2b.utdallas.ed:shell ESTABLISHED - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:60167 ESTABLISHED - keepalive (5557.55/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63574 ESTABLISHED - keepalive (347.44/0/0)

tcp 0 0 cslinux1.utdallas.e:858 10.182.21.19:nfs ESTABLISHED - keepalive (22.96/0/0)

tcp 1 0 localhost:hbci localhost:50166 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-121-:63580 ESTABLISHED - keepalive (347.44/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:58947 ESTABLISHED - keepalive (740.65/0/0)

tcp 1 0 localhost:hbci localhost:50414 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:56634 ESTABLISHED - keepalive (7064.88/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-125-:16276 ESTABLISHED - keepalive (6704.43/0/0)

tcp 2 0 localhost:hbci localhost:50068 CLOSE\_WAIT - off (0.00/0/0)

tcp 0 0 cslinux1.utdallas.e:ssh utdvpn-10-50-120-:56515 ESTABLISHED - keepalive (7032.11/0/0)

tcp6 0 0 [::]:54356 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 [::]:ssh [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:ipp [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:smtp [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhos:x11-ssh-offset [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6011 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6012 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6013 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6014 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6015 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 [::]:rxmon [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 localhost:6016 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 [::]:40768 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 [::]:35917 [::]:\* LISTEN - off (0.00/0/0)

tcp6 0 0 [::]:sunrpc [::]:\* LISTEN - off (0.00/0/0)

**Case 1: check which ports are being used from 10-99**

{cslinux1:~} netstat -aont | grep "`hostname -i`:[1-9][0-9] "

tcp 0 0 129.110.92.15:22 10.50.120.49:60925 ESTABLISHED keepalive (2721.84/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.26:64163 ESTABLISHED keepalive (6948.91/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63747 ESTABLISHED keepalive (1312.82/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.24:58984 ESTABLISHED keepalive (6555.70/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.16:59460 ESTABLISHED keepalive (3541.04/0/0)

tcp 0 0 129.110.92.15:22 10.50.125.194:16269 ESTABLISHED keepalive (6654.00/0/0)

tcp 0 48 129.110.92.15:22 10.50.120.26:64160 ESTABLISHED on (0.23/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.143:2056 ESTABLISHED keepalive (6391.86/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63898 ESTABLISHED keepalive (4687.92/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63748 ESTABLISHED keepalive (1345.58/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63897 ESTABLISHED keepalive (4671.54/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.143:2057 ESTABLISHED keepalive (6408.24/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.49:60167 ESTABLISHED keepalive (5507.12/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63574 ESTABLISHED keepalive (297.01/0/0)

tcp 0 0 129.110.92.15:22 10.50.121.19:63580 ESTABLISHED keepalive (297.01/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.16:58947 ESTABLISHED keepalive (690.22/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.115:56634 ESTABLISHED keepalive (7014.45/0/0)

tcp 0 0 129.110.92.15:22 10.50.125.194:16276 ESTABLISHED keepalive (6654.00/0/0)

tcp 0 0 129.110.92.15:22 10.50.120.115:56515 ESTABLISHED keepalive (6981.68/0/0)

**Case 2: check which ports are being used from 30000-30099 (none are in use)**

{cslinux1:~} netstat -aont | grep "`hostname -i`:300[0-9][0-9] "

**Case 3: find the TCP connection with my computer (my IP address hidden)**

{cslinux1:~} netstat -aont | grep "MY IP ADDRESS"

tcp 0 0 129.110.92.15:22 MY IP ADDRESS:64163 ESTABLISHED keepalive (6770.54/0/0)

tcp 0 48 129.110.92.15:22 MY IP ADDRESS:64160 ESTABLISHED on (0.24/0/0)

**4. nslookup www.utdallas.edu**

{cslinux1:~} nslookup www.utdallas.edu

Server: 10.176.92.9

Address: 10.176.92.9#53

Non-authoritative answer:

Name: www.utdallas.edu

Address: 10.182.71.70

**5. ifconfig -a**

{cslinux1:~} ifconfig -a

em1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 129.110.92.15 netmask 255.255.255.0 broadcast 129.110.92.255

inet6 fe80::92b1:1cff:fe4b:8b8d prefixlen 64 scopeid 0x20<link>

ether 90:b1:1c:4b:8b:8d txqueuelen 1000 (Ethernet)

RX packets 13857162 bytes 6502594473 (6.0 GiB)

RX errors 0 dropped 99 overruns 0 frame 0

TX packets 15047433 bytes 6552630798 (6.1 GiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 40

eno2: flags=4098<BROADCAST,MULTICAST> mtu 1500

ether 90:b1:1c:4b:8b:8e txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 54

eno3: flags=4098<BROADCAST,MULTICAST> mtu 1500

ether 90:b1:1c:4b:8b:8f txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 56

eno4: flags=4098<BROADCAST,MULTICAST> mtu 1500

ether 90:b1:1c:4b:8b:90 txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 57

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 82323 bytes 185627863 (177.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 82323 bytes 185627863 (177.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0