

## PRE LAB SOLUTIONS

1. On Linux, the **groups** command will show which groups you are part of
2. The \$ sign holds the result of the last executed command
3. Ctrl + Z
4. You can find the kernel version by typing in: `uname -v` . You can find the nodename by typing in: `uname -n`. You can find both together by typing in: `uname -vn`.
5. The ~ symbol is the home directory. The . symbol is the current directory. The .. symbol is the previous directory, you go up a directory. The / symbol is the root directory.
6. Pid is the process id. It shows the processes that are running. You should use the **ps** command to find the pid for a process that is currently running.
7. Type in: `getent passwd | cut -d: -f1,7`
8. Both commands are used to gain administrative privileges. However, the 'sudo' command temporarily gives you administrative privileges for the single command ran with it and does not require credentials. The 'su root' switches you to the root account and required root credentials. It allows you to do all administrative tasks until you log out.
9. You use the cron software to schedule tasks. Use the cron tab command to manage all of the cron jobs.
10. Solution in Christy Jose-script.sh

## LAB SOLUTIONS

1. Refer to Christy-topo.py
2. dump

```
mininet@mininet-vm:~/workspace$ sudo su
root@mininet-vm:/home/mininet/workspace# python test.py
mininet> dump
<Host h1: h1-eth0:10.0.0.1 pid=3702>
<Host h2: h2-eth0:10.0.0.2 pid=3706>
<Host h3: h3-eth0:10.0.0.3 pid=3708>
<Host h4: h4-eth0:10.0.0.4 pid=3710>
<OVSSwitch s1: lo:127.0.0.1,s1-eth1:None,s1-eth2:None,s1-eth3:None,s1-eth4:None pid=3715>
<Controller c0: 127.0.0.1:6633 pid=3695>
mininet>
```

This screenshot shows the topology of the given network. In the beginning, I saved my code in the file test.py. Later, I renamed the file to Christy-topo.py.

pingall

```
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 h4
h2 -> h1 h3 h4
h3 -> h1 h2 h4
h4 -> h1 h2 h3
*** Results: 0% dropped (12/12 received)
mininet>
```

The pingall command checks the connectivity of all of the hosts in the network by checking if any packets were dropped

## 3. iperf

```

mininet>
mininet> iperf
*** Iperf: testing TCP bandwidth between h1 and h4
*** Results: ['62.0 Gbits/sec', '62.1 Gbits/sec']
mininet>

```

The connect was 62.0 Gbits/sec

## 4. .

Wireshark 1.10.6 (v1.10.6 from master-1.10)

Filter: of

No.	Time	Source	Destination	Protocol	Length	Info
97	92.062334000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
98	92.063485000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
102	97.067256000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
103	97.068026000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
106	97.952900000	10.0.0.2	10.0.0.3	OF 1.0	184	of_packet_in
107	97.953238000	127.0.0.1	127.0.0.1	OF 1.0	92	of_packet_out
114	97.953444000	10.0.0.3	10.0.0.2	OF 1.0	184	of_packet_in
115	97.953641000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
119	98.955530000	10.0.0.2	10.0.0.3	OF 1.0	184	of_packet_in
120	98.957530000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
138	102.963780000	1e:fc:ed:9e:73:a5	fa:83:fd:57:05:7f	OF 1.0	128	of_packet_in
139	102.964253000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
143	102.964891000	fa:83:fd:57:05:7f	1e:fc:ed:9e:73:a5	OF 1.0	128	of_packet_in
144	102.965446000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
147	107.061146000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request

a.

There are 5 packet\_in messages

- b. The source IP addresses are 10.0.0.2, and 10.0.0.3. The destination IP addresses are the same ones. For the packet\_out, the source IP address is 127.0.0.1, and the destination IP address is 127.0.0.1

Wireshark 1.10.6 (v1.10.6 from master-1.10)

Filter: of

No.	Time	Source	Destination	Protocol	Length	Info
97	92.062334000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
98	92.063485000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
102	97.067256000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
103	97.068026000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
106	97.952900000	10.0.0.2	10.0.0.3	OF 1.0	184	of_packet_in
107	97.953238000	127.0.0.1	127.0.0.1	OF 1.0	92	of_packet_out
114	97.953444000	10.0.0.3	10.0.0.2	OF 1.0	184	of_packet_in
115	97.953641000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
119	98.955530000	10.0.0.2	10.0.0.3	OF 1.0	184	of_packet_in
120	98.957530000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
138	102.963780000	1e:fc:ed:9e:73:a5	fa:83:fd:57:05:7f	OF 1.0	128	of_packet_in
139	102.964253000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
143	102.964891000	fa:83:fd:57:05:7f	1e:fc:ed:9e:73:a5	OF 1.0	128	of_packet_in
144	102.965446000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
147	107.061146000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request

- c. 48 entries were generated on wireshark. The types of icmp entries that showed up were Echo request and Echo reply.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help									
Filter: icmp && not of				Expression... Clear Apply Save					
No.	Time	Source	Destination	Protocol	Length	Info			
38	33.29244900	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) request	id=0x1296, seq=1/256, ttl=64		
41	33.29321400	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) request	id=0x1296, seq=1/256, ttl=64 (reply in 42)		
42	33.29322800	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1296, seq=1/256, ttl=64 (request in 41)		
45	33.29408000	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1296, seq=1/256, ttl=64		
57	33.29901100	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) request	id=0x1298, seq=1/256, ttl=64		
60	33.29935200	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) request	id=0x1298, seq=1/256, ttl=64 (reply in 61)		
61	33.29936000	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1298, seq=1/256, ttl=64 (request in 60)		
64	33.29965300	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1298, seq=1/256, ttl=64		
76	33.30192000	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) request	id=0x1299, seq=1/256, ttl=64		
79	33.30214800	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) request	id=0x1299, seq=1/256, ttl=64 (reply in 80)		
80	33.30215400	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1299, seq=1/256, ttl=64 (request in 79)		
83	33.30237100	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) reply	id=0x1299, seq=1/256, ttl=64		
84	33.30369200	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129a, seq=1/256, ttl=64		
87	33.30420200	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129a, seq=1/256, ttl=64 (reply in 88)		
88	33.30423400	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129a, seq=1/256, ttl=64 (request in 87)		
91	33.30472800	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129a, seq=1/256, ttl=64		
92	33.30563700	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) request	id=0x129b, seq=1/256, ttl=64		
95	33.30597700	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) request	id=0x129b, seq=1/256, ttl=64 (reply in 96)		
96	33.30609900	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129b, seq=1/256, ttl=64 (request in 95)		
99	33.30633700	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129b, seq=1/256, ttl=64		
111	33.30828000	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129c, seq=1/256, ttl=64		
114	33.30875400	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129c, seq=1/256, ttl=64 (reply in 115)		
115	33.30878800	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129c, seq=1/256, ttl=64 (request in 114)		
118	33.30907400	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129c, seq=1/256, ttl=64		
119	33.31136700	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129d, seq=1/256, ttl=64		
122	33.31178900	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129d, seq=1/256, ttl=64 (reply in 123)		
123	33.31179400	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129d, seq=1/256, ttl=64 (request in 122)		
126	33.31249200	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129d, seq=1/256, ttl=64		
127	33.31760900	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request	id=0x129e, seq=1/256, ttl=64		
130	33.31807100	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request	id=0x129e, seq=1/256, ttl=64 (reply in 131)		
131	33.31818900	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129e, seq=1/256, ttl=64 (request in 130)		
134	33.31847100	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129e, seq=1/256, ttl=64		
146	33.32278800	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129f, seq=1/256, ttl=64		
149	33.32274400	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129f, seq=1/256, ttl=64 (reply in 150)		
150	33.32278800	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129f, seq=1/256, ttl=64 (request in 149)		
153	33.32330700	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129f, seq=1/256, ttl=64		
154	33.33880400	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) request	id=0x12a0, seq=1/256, ttl=64		
157	33.33876700	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) request	id=0x12a0, seq=1/256, ttl=64 (reply in 158)		
158	33.33880600	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a0, seq=1/256, ttl=64 (request in 157)		
161	33.33920100	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a0, seq=1/256, ttl=64		
162	33.34343600	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) request	id=0x12a1, seq=1/256, ttl=64		
165	33.34381200	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) request	id=0x12a1, seq=1/256, ttl=64 (reply in 166)		
166	33.34384400	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a1, seq=1/256, ttl=64 (request in 165)		
169	33.34414200	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a1, seq=1/256, ttl=64		
170	33.34578600	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) request	id=0x12a2, seq=1/256, ttl=64		
173	33.34612900	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) request	id=0x12a2, seq=1/256, ttl=64 (reply in 174)		
174	33.34616200	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a2, seq=1/256, ttl=64 (request in 173)		
177	33.34648700	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a2, seq=1/256, ttl=64		

File Machine View Input Devices Help									
Capturing from any [Wireshark 1.10.6 (v1.10.6 from master-1.10)]									
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help									
Filter: icmp && not of				Expression... Clear Apply Save					
No.	Time	Source	Destination	Protocol	Length	Info			
111	33.30828800	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129c, seq=1/256, ttl=64		
114	33.30875400	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129c, seq=1/256, ttl=64 (reply in 115)		
115	33.30878800	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129c, seq=1/256, ttl=64 (request in 114)		
118	33.30907400	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply	id=0x129c, seq=1/256, ttl=64		
119	33.31136700	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129d, seq=1/256, ttl=64		
122	33.31178900	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request	id=0x129d, seq=1/256, ttl=64 (reply in 123)		
123	33.31179400	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129d, seq=1/256, ttl=64 (request in 122)		
126	33.31249200	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129d, seq=1/256, ttl=64		
127	33.31760900	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request	id=0x129e, seq=1/256, ttl=64		
130	33.31807100	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request	id=0x129e, seq=1/256, ttl=64 (reply in 131)		
131	33.31818900	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129e, seq=1/256, ttl=64 (request in 130)		
134	33.31847100	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129e, seq=1/256, ttl=64		
146	33.32278800	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129f, seq=1/256, ttl=64		
149	33.32274400	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) request	id=0x129f, seq=1/256, ttl=64 (reply in 150)		
150	33.32278800	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129f, seq=1/256, ttl=64 (request in 149)		
153	33.32330700	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) reply	id=0x129f, seq=1/256, ttl=64		
154	33.33880400	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) request	id=0x12a0, seq=1/256, ttl=64		
157	33.33876700	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) request	id=0x12a0, seq=1/256, ttl=64 (reply in 158)		
158	33.33880600	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a0, seq=1/256, ttl=64 (request in 157)		
161	33.33920100	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a0, seq=1/256, ttl=64		
162	33.34343600	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) request	id=0x12a1, seq=1/256, ttl=64		
165	33.34381200	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) request	id=0x12a1, seq=1/256, ttl=64 (reply in 166)		
166	33.34384400	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a1, seq=1/256, ttl=64 (request in 165)		
169	33.34414200	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a1, seq=1/256, ttl=64		
170	33.34578600	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) request	id=0x12a2, seq=1/256, ttl=64		
173	33.34612900	10.0.0.4	10.0.0.3	ICMP	100	Echo (ping) request	id=0x12a2, seq=1/256, ttl=64 (reply in 174)		
174	33.34616200	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a2, seq=1/256, ttl=64 (request in 173)		
177	33.34648700	10.0.0.3	10.0.0.4	ICMP	100	Echo (ping) reply	id=0x12a2, seq=1/256, ttl=64		