Greg Miller

SAT3711

Lab 1

What we can draw from the data presented from pinging teamliquid.net with 60 packets at 1 hour intervals over a 24 hour period is not particularly interesting, test began at 12:15AM Jan 26 (T-0). The data indicates that both the recipient and the sender (teamliquid.net and MTU resp.) have apparently stable connections. The two outlying pings, after some research, were likely cause by two events that occurred on the website at that time causing increased traffic. With a total packet loss of 0% over the entire period and an extremely consistent ping we can conclude that over this interval both systems were up and communicating with no issues that can be detected, at least not from this data alone.

Part 1:
audit.chk

```
#!/bin/bash
# Search a file (audit.log) in the current directory for the string
# 1 521 1 and output all lines containing it to the file audit.chk
#
# If the file is greater than 2K cut the first 2K to a new file
# (denoted as audit.<daymonthyear>).

#get all lines with the string
grep "1 521 1" audit.log >> audit.chk

#get the line count
linecount=`grep "1 521 1" audit.log | wc -l | awk -F ' ' '{ print $1 }'`
echo $linecount >> audit.chk

#get file size
filesize=`wc -c audit.log | awk -F ' ' '{ print $1 }'`

#trim off the first 2048...
if [ $filesize -gt 2048 ]; then
  head -c 2048 audit.log >> audit.`date '+%m%d%y'` #write out the first 2048 (APPENDED)
  tail -c +2049 audit.log > audit.log #delete the first 2048 from the file
fi
```

Part 2:
trace.sh

```
#!/bin/bash
if [ $# -ne 1 ]; then
  echo "Usage:"
  echo "    trace.sh <host>"
  exit 1
fi

echo "Route to "$1
traceroute $1 | grep -e 'ms\|\*' | awk -F ' ' '{ print $1" "$2 }'
```

ping.sh

```bash
#!/bin/bash

if [ $# -ne 1 -a $# -ne 2 ]; then
  echo "Usage:"
  echo "    trimmed_ping.sh <host> [num_pings]"
  exit 1
fi

numpings=60
echo "----------------------------------------------------------------------"
echo -n "Ping results for "
echo -n `date +%c`
echo " on "$1

#do the ping
pingresult=`ping -c $numpings $1`

#retrieve the right lines "$var" to preserve spacing
loss=`echo "$pingresult" | grep "packets"`
time=`echo "$pingresult" | grep "rtt"`

#get the avg time
avgtime=`echo $time | awk -F ' = ' '{ print $2 }' | awk -F '/' '{ print $2 }'`

#get the lossrate
lossrate=`echo $loss | awk -F ', ' '{ print $3 }' | awk -F ' ' '{ print $1 }'`

echo "Loss rate: "$lossrate
echo "Average time: "$avgtime
echo "----------------------------------------------------------------------"
```
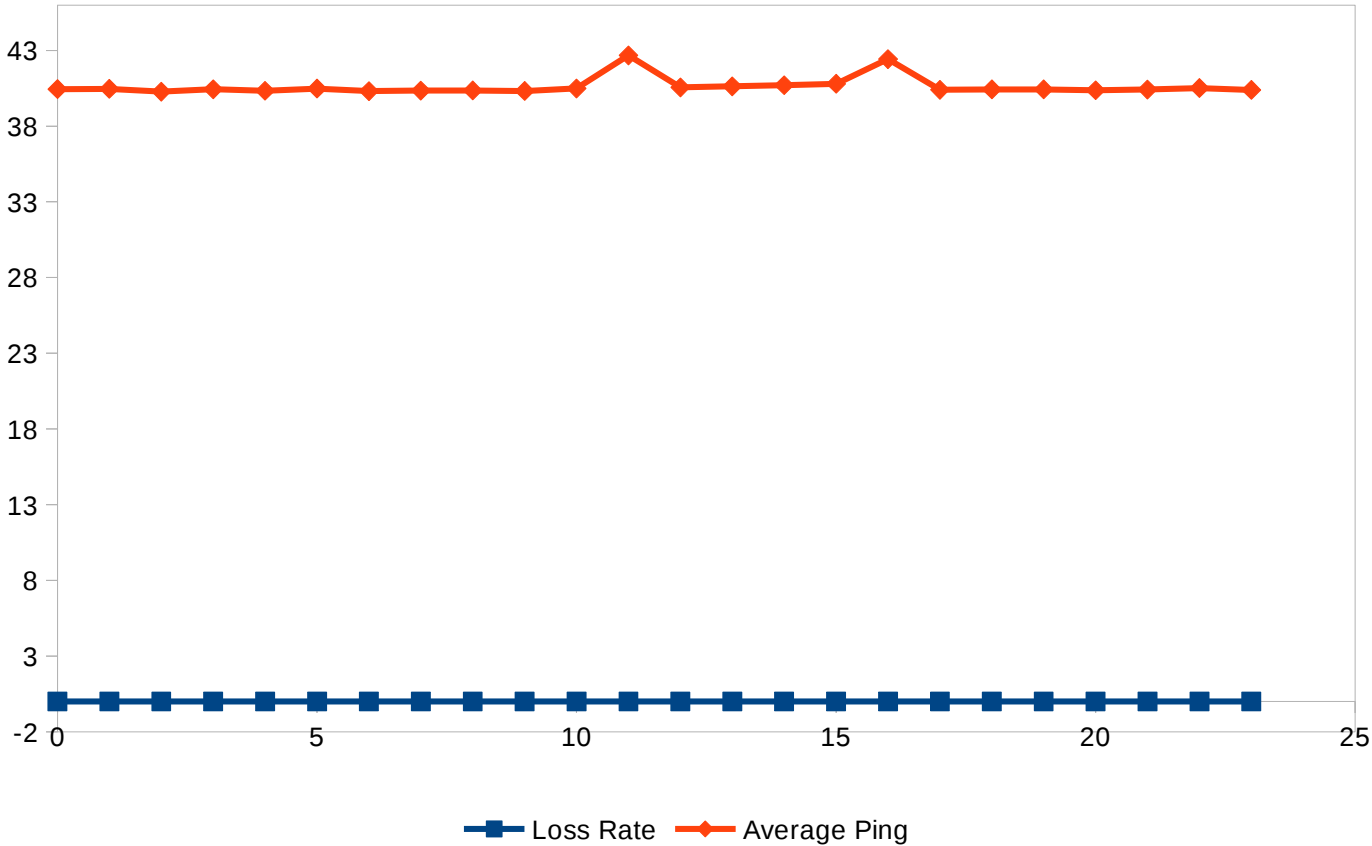
Ping to teamliquid.net

Time	Loss Rate	Average Ping
0	0	40.444
1	0	40.464
2	0	40.281
3	0	40.442
4	0	40.337
5	0	40.479
6	0	40.316
7	0	40.35
8	0	40.362
9	0	40.323
10	0	40.492
11	0	42.679
12	0	40.56
13	0	40.632
14	0	40.703
15	0	40.801
16	0	42.426
17	0	40.403
18	0	40.427
19	0	40.424
20	0	40.37
21	0	40.417
22	0	40.52
23	0	40.397

```
btcraig@localhost:~/classes/sat3711

File   Edit   View   Search   Terminal   Help

[btcraig@localhost sat3711]$ ls -la
total 44
drwxrwxr-x. 2 btcraig btcraig  4096 Jan 28 13:31 .
drwxrwxr-x. 4 btcraig btcraig  4096 Jan 26 10:18 ..
-rw-rw-r--. 1 btcraig btcraig  2048 Jan 28 13:31 audit.012815
-rw-rw-r--. 1 btcraig btcraig 10004 Jan 28 13:31 audit.chk
-rw-rw-r--. 1 btcraig btcraig     0 Jan 28 13:31 audit.log
-rwx------. 1 btcraig btcraig   740 Jan 28 13:31 audit.sh
-rw-rw-r--. 1 btcraig btcraig  4939 Jan 28 13:25 ping.results
-rwx------. 1 btcraig btcraig   907 Jan 25 23:50 ping.sh
-rwx------. 1 btcraig btcraig   178 Jan 25 23:58 trace.sh
[btcraig@localhost sat3711]$ $
```