Traceroute at UMT

Table of Contents

- Table of Contents
- Summary:
 - Traceroute from UTM to SLAC
 - Traceroute from UM to SLAC
- · Details with screenshots:
 - Traceroute from UTM to SLAC
 - Traceroute from UM to SLAC
 - Traceroute from UTM Pinger command line to SLAC (Stop at 11th hop)
 - Traceroute from UTM to SLAC Option -f6 (reached at its destination)

 - Traceroute from UM to SLAC Option -f6
 Traceroute from UTM Pinger command line to SLAC Option -f6 (reached at its destination)
 - Traceroute from UTM to SLAC Option -f6 -n (reached at its destination)
 - Traceroute from UM to SLAC Option -f6 -n (reached at its destination)
 - o Traceroute from UTM Pinger command line to SLAC Option -f6 -n (reached at its destination)
- Traceroute from UTM Cisco border router to CERN
- Traceroute from UTM to CERN on a Mac
- Possible Explanation

Summary:

Traceroute from UTM to SLAC

 traceroute -m 30 -q 3 134.79.196.165 140 took 135 secs. (Stop at 11th hop) traceroute -m 30 -q 3 -f6 134.79.196.165 140 took 110 secs. (reached at its destination) traceroute -m 30 -q 3 -n -f6 134.79.196.165 140 took 15 secs. (reached at its destination)

From Command Line:

- traceroute from UTM Pinger command line to SLAC (Stop at 11th hop)
- traceroute from UTM Pinger command line to SLAC Option -f6 (reached at its destination)
- traceroute from UTM Pinger command line to SLAC Option -f6 -n (reached at its destination)
- sudo traceroute -I www6.slac.stanford.edu (reached at its destination successfully without using -f6)

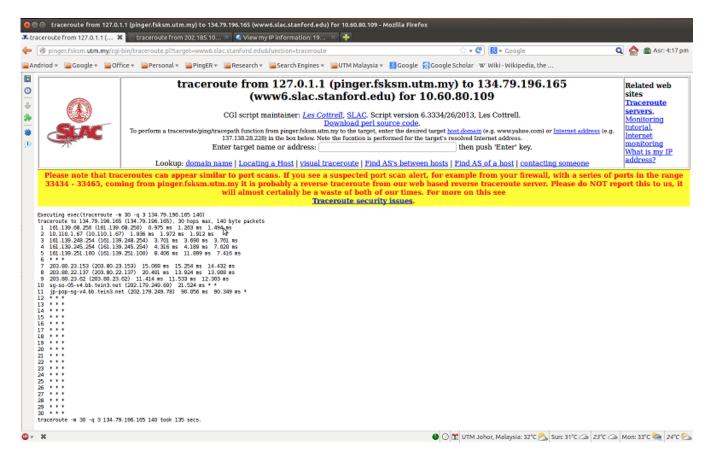
Traceroute from UM to SLAC

• traceroute -m 30 -q 3 134.79.196.165 140 took 19 secs. • traceroute -m 30 -q 3 -f6 134.79.196.165 140 took 21 secs. traceroute -m 30 -q 3 -n -f6 134.79.196.165 140 took 20 secs.

Details with screenshots:

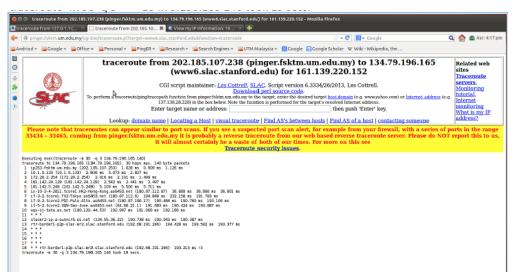
Traceroute from UTM to SLAC

traceroute -m 30 -q 3 134.79.196.165 140 took 135 secs. (Stop at 11th hop)



Traceroute from UM to SLAC

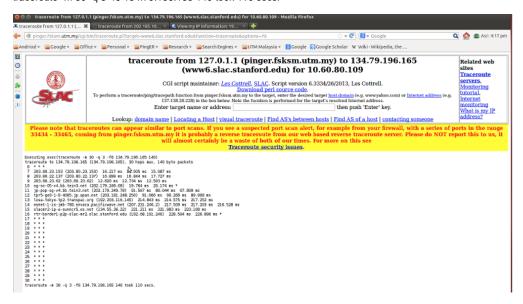
traceroute -m 30 -q 3 134.79.196.165 140 took 19 secs.



Traceroute from UTM Pinger command line to SLAC (Stop at 11th hop)

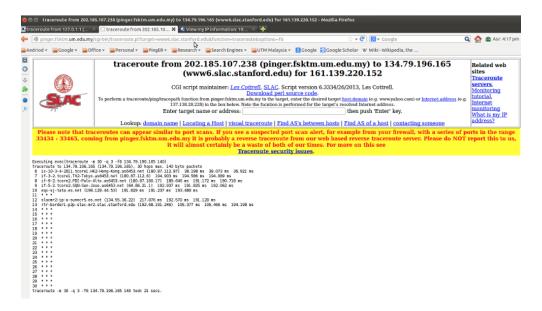
Traceroute from UTM to SLAC Option -f6 (reached at its destination)

traceroute -m 30 -q 3 -f6 134.79.196.165 140 took 110 secs.



Traceroute from UM to SLAC Option -f6

traceroute -m 30 -q 3 -f6 134.79.196.165 140 took 21 secs.



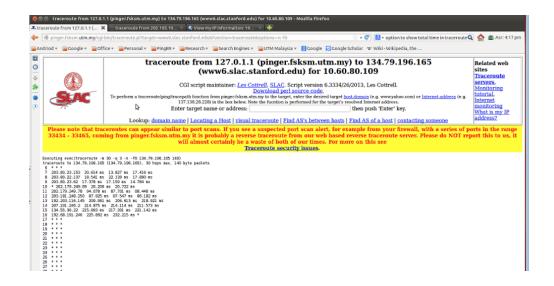
Traceroute from UTM Pinger command line to SLAC Option -f6 (reached at its destination)

```
Saqibali@saqibali-desktop:~

saqibali@saqibali-desktop:-5 traceroute -f6 wmw6.slac.stanFord.edu
traceroute to wmw6.slac.stanFord.edu (134.79.196.165), 36 hops max, 60 byte packets
6 ***
7 203.80.23.153 (203.00.23.153) 20.485 ms 17.611 ms 18.342 ms
8 203.80.22.137 (203.00.22.137) 29.717 ms 29.567 ms 40.934 ms
9 203.80.23.62 (203.80.23.62) 17.881 ms 17.690 ms 19.765 ms
10 sg.so-05-v4.bb.tetn3.net (202.179.249.69) 22.035 ms 21.238 ms 19.101 ms
11 jp-pop-sg-v4.bb.teln3.net (202.179.249.78) 91.058 ms 107.815 ms 92.397 ms
12 tpr5-ge0-1-0-4005.jp.apan.net (203.181.240.250) 93.894 ms 93.583 ms 90.567 ms
13 xe-0-0.259-trt.losa.transpac.org (192.203.116.145) 209.151 ms 210.522 ms 211.691 ms
14 esnet-1-is-jmb-780.snvaca.pacificwave.net (207.231.246.2) 235.567 ms 212.310 ms 211.691 ms
15 slacmr2-ip-a-sunncr5.es.net (134.55.36.22) 220.430 ms 225.509 ms 227.197 ms
16 rtr-border1-p2p-slac-mr2.slac.stanford.edu (192.68.191.246) 226.601 ms 228.616 ms *
17 ***
18 ***
20 ***
21 ***
22 ***
23 ***
24 ***
25 ***
26 ***
27 ***
28 ***
29 ***
29 ***
saqibali@saqibali-desktop:-5 □
```

Traceroute from UTM to SLAC Option -f6 -n (reached at its destination)

traceroute -m 30 -g 3 -n -f6 134.79.196.165 140 took 15 secs.



Traceroute from UM to SLAC Option -f6 -n (reached at its destination)

traceroute -m 30 -q 3 -n -f6 134.79.196.165 140 took 20 secs.



Traceroute from UTM Pinger command line to SLAC Option -f6 -n (reached at its destination)

```
Saqibali@saqibali-desktop:-

saqibali@saqibali-desktop:-

saqibali@saqibali-desktop:-

traceroute to www6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte packets

* * * *

7 203.80.23.153 27.674 ms 25.845 ms 25.630 ms

8 203.80.22.137 24.530 ms 21.168 ms 23.204 ms

9 203.80.23.62 20.793 ms 23.544 ms 26.801 ms

10 202.179.249.69 26.310 ms 30.714 ms 30.000 ms

11 202.179.249.69 26.310 ms 30.714 ms 30.000 ms

11 202.179.249.78 119.901 ms 105.178 ms 104.467 ms

12 203.181.248.250 105.324 ms 108.037 ms 107.179 ms

13 192.203.116.145 222.649 ms 223.193 ms 222.755 ms

14 207.231.246.2 230.793 ms 232.907 ms 229.780 ms

15 134.55.36.22 246.096 ms 214.475 ms 215.571 ms

16 192.68.191.246 212.000 ms 215.501 ms *

17 * * *

18 * *

19 * *

20 * * *

21 * *

22 * *

23 * * *

24 * * *

25 * * *

26 * * *

27 * * *

28 * * *

29 * * *

saqibali@saqibali-desktop:-$
```

sudo traceroute -l www6.slac.stanford.edu (reached at its destination)

```
New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 6 15:23:39 2014 from 10.60.80.109
saqibaligsaqibali-desktop: $ sudo traceroute -1 www6.slac.stanford.edu
[sudo] password for saqibali:
traceroute to www6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte packets

1 161.139.68.250 (161.139.68.250) 0.868 ms 1.167 ms *

2 * * *

3 * * *

4 * * *

5 * * *

6 * * *

7 203.80.23.153 (203.80.23.153) 15.702 ms 15.872 ms 15.793 ms

8 203.80.22.137 (203.80.23.153) 19.577 ms 19.792 ms 19.480 ms

9 203.80.23.62 (203.80.23.62) 14.079 ms 13.978 ms 14.127 ms

10 sg-so-05-v4.bb.tein3.net (202.179.249.69) 20.369 ms 19.723 ms 19.664 ms

11 jp-pop-sg-v4.bb.tein3.net (202.179.249.78) 89.333 ms 89.419 ms 86.207 ms

12 tpr5-ge0-1-0-4005.jp.apan.net (203.181.248.250) 86.165 ms 86.249 ms 86.641 ms

13 losa-tokyo-tp2.transpac.org (192.203.116.145) 203.668 ms 203.571 ms 202.658 ms

14 esnet-1-ts-jmb-780.snvaca.pactficwave.net (207.231.246.2) 249.285 ms 248.450 ms 249.666 ms

15 slacnr2-tp-a-sunncr5.es.net (134.55.36.22) 210.297 ms 209.982 ms 210.062 ms

16 rtr-border1-p2p-slac-mr2.slac.stanford.edu (192.68.191.246) 210.339 ms 212.898 ms 212.397 ms

17 * * *

18 * * *

19 drupal-prod.slac.stanford.edu (134.79.196.165) 211.724 ms 215.760 ms 215.046 ms

saqtbaligsaqtbali-desktop: $
```

Traceroute from UTM Cisco border router to CERN

```
Translating "www.cern.ch"...domain server (202,188.0,133) [OK]
Type escape sequence to abort.
Tracing the route to webrlb02.cern.ch (188,184,9,235)
VRF info: (vrf in name/id, vrf out name/id)
   1 161,139,244,6 1 msec 1 msec 0 msec
  2 203,80,23,153 [AS 24514] [MPLS: Label 1048533 Exp 0] 743 msec 757 msec 770 msec
  3 203,80,22,137 [AS 24514] [MPLS: Label 16047 Exp 0] 751 msec 791 msec 740 msec 4 203,80,23,242 [AS 24514] 757 msec 749 msec 737 msec 5 202,179,249,85 [AS 24490] 724 msec 717 msec 712 msec
  6 mb-so-01-v4.bb.tein3.net (202.179.249.54) [AS 24490] 776 msec 781 msec 843 msec
     eu-mad-pr-v4.bb.tein3.net (202.179.249.118) [AS 24490] 971 msec 958 msec 929 msec
     se3.mxi.par.fr.geant.net (62.40.98.65) [AS 20965] 939 msec 954 msec 937 msec
     switch-bckp-gw.mx1.par.fr.geant.net (62.40.124.82) [AS 20965] 216 msec 216 msec 217 msec
 10 e513-e-rbrxl-2-te20.cern.ch (192.65.184.70) [AS 513] 924 msec 958 msec 981 msec
 11
 12
 13
      *
             *
          *
 14
15
      *
             *
          *
      *
             *
 16
      *
             *
 17
 18
 19
20
      *
      *
 21
22
23
24
25
26
      *
             *
      *
             *
      *
          *
             *
             *
      *
 27
 28
 29
      *
             *
          *
 30
```

Since this router can see cern in 10 hops there are no blocks for the first 10 UDP ports starting at 33434. There may be blocks in higher number UDP ports that is unknown from this result.

Typically when one blocks a set of ports in an ACL one blocks them both for TCP and UDP. If this is the case you may be able to use the telnet <cern-host> <tcp port command and see if you get a response as you increase the <tcp-port> starting at 33433 where <cern-host> = e513-e-rbx1-2-te20.cern.ch

You might also play around with the -p option in the traceroute command

Traceroute from UTM to CERN on a Mac

This gives the same result as on Linux. This is not unexpected since the Mac OS is Unix based and so uses UDP probes unlike Windows that uses ICMP probes and hence does not see the effect.

Possible Explanation

Traceroute uses UDP to send the requests (see http://en.wikipedia.org/wiki/Traceroute). The first request is sent to a particular port (33434), with a ttl to tell it how many hops to go to. The ttl starts at 1 is incremented as it tries the next hop, also the port is incremented (up to 33465). It looks like the first few UDP ports are enabled and then they are blocked. The blocking could be at the border or in the ISP. Can you try a traceroute from just outside the border (e.g. in the border router itself), or if you can get access to the routers try traceroute from them to the destination. Note Windows tracert uses ICMP and not UDP to send the probes and so should not suffer this problem.