

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 \(reached at its destination\)](#)
 - [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)

tracert from 127.0.1.1 (pinger.fsksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 10.60.80.109 - Mozilla Firefox

tracert from 127.0.1.1 (pinger.fsksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 10.60.80.109

CGI script maintainer: [Les Cottrell](#), SLAC. Script version 6.3334/26/2013, Les Cottrell.
[Download perl source code.](#)

To perform a tracert/ping/tracert function from pinger.fsksm.utm.my to the target, enter the desired target [host domain](#) (e.g. www.yahoo.com) or [Internet address](#) (e.g. 137.138.28.228) in the box below. Note the function is performed for the target's resolved Internet address.
 Enter target name or address: then push 'Enter' key.

Lookup: [domain name](#) | [Locating a Host](#) | [visual traceroute](#) | [Find AS's between hosts](#) | [Find AS of a host](#) | [contacting someone](#)

Please note that traceroutes can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range 33434 - 33463, coming from pinger.fsksm.utm.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a waste of both of our times. For more on this see [Traceroute security issues](#).

```

Executing exec(tracert -m 30 -q 3 134.79.196.165 140)
tracert to 134.79.196.165 (134.79.196.165), 30 hops max, 140 byte packets
 1 161.139.08.250 (161.139.08.250) 0.975 ms 1.263 ms 1.494 ms
 2 10.110.1.67 (10.110.1.67) 1.936 ms 1.972 ms 1.912 ms
 3 161.139.248.254 (161.139.248.254) 3.701 ms 3.690 ms 3.701 ms
 4 161.139.245.254 (161.139.245.254) 4.316 ms 4.189 ms 7.020 ms
 5 161.139.251.100 (161.139.251.100) 8.406 ms 11.899 ms 7.415 ms
 6 * * *
 7 203.80.23.153 (203.80.23.153) 15.068 ms 15.254 ms 14.432 ms
 8 203.80.22.137 (203.80.22.137) 20.401 ms 13.924 ms 13.508 ms
 9 203.80.23.62 (203.80.23.62) 11.414 ms 11.533 ms 12.303 ms
10 sg-so-05-v4-bb.tein3.net (202.179.240.69) 21.534 ms * *
11 jp-pop-sg-v4-bb.tein3.net (202.179.249.78) 90.056 ms 90.349 ms *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
tracert -m 30 -q 3 134.79.196.165 140 took 135 secs.
  
```

UTM Johor, Malaysia: 32°C Sun: 31°C 23°C Mon: 33°C 24°C

Traceroute from UM to SLAC

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

tracert from 202.185.107.238 (pinger.fsktm.um.edu.my) to 134.79.196.165 (www6.slac.stanford.edu) for 161.139.220.152 - Mozilla Firefox

tracert from 202.185.107.238 (pinger.fsktm.um.edu.my) to 134.79.196.165 (www6.slac.stanford.edu) for 161.139.220.152

CGI script maintainer: [Les Cottrell](#), SLAC. Script version 6.3334/26/2013, Les Cottrell.
[Download perl source code.](#)

To perform a tracert/ping/tracert function from pinger.fsktm.um.edu.my to the target, enter the desired target [host domain](#) (e.g. www.yahoo.com) or [Internet address](#) (e.g. 137.138.28.228) in the box below. Note the function is performed for the target's resolved Internet address.
 Enter target name or address: then push 'Enter' key.

Lookup: [domain name](#) | [Locating a Host](#) | [visual traceroute](#) | [Find AS's between hosts](#) | [Find AS of a host](#) | [contacting someone](#)

Please note that traceroutes can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range 33434 - 33463, coming from pinger.fsktm.um.edu.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a waste of both of our times. For more on this see [Traceroute security issues](#).

```

Executing exec(tracert -m 30 -q 3 134.79.196.165 140)
tracert to 134.79.196.165 (134.79.196.165), 30 hops max, 140 byte packets
 1 ip253.fsktm.um.edu.my (202.185.107.238) 1.028 ms 0.909 ms 1.126 ms
 2 10.1.0.138 (10.1.0.138) 2.808 ms 3.073 ms 2.807 ms
 3 172.20.2.254 (172.20.2.254) 2.015 ms 2.101 ms 1.499 ms
 4 161.142.24.129 (161.142.24.129) 2.542 ms 2.440 ms 2.407 ms
 5 161.142.5.249 (161.142.5.249) 5.103 ms 5.500 ms 5.711 ms
 6 ix-10-3-4-2011.tcore1.m2-rmg-hong.as463.net (180.87.112.07) 36.689 ms 36.566 ms 36.501 ms
 7 ix-2-tcore1.t2-tokyo.as463.net (180.87.112.0) 186.868 ms 232.158 ms 181.783 ms
 8 ix-0-2-tcore2.PDX-Palo-Alto.as463.net (180.87.180.17) 190.484 ms 190.760 ms 193.106 ms
 9 ix-0-2-tcore2.SFO-San-Jose.as463.net (64.86.21.1) 191.089 ms 190.424 ms 193.087 ms
10 eqx-sj-tata.as.net (198.120.44.53) 192.997 ms 191.069 ms 192.186 ms
11 * * *
12 slac2-ip-a-suncr5.as.net (134.55.36.22) 190.738 ms 190.943 ms 190.387 ms
13 rtr-border1-pdp-slab-er2.slac.stanford.edu (152.68.191.246) 194.428 ms 193.582 ms 193.377 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * rtr-border1-pdp-slab-er2.slac.stanford.edu (152.68.191.246) 193.213 ms 193.213 ms 193.213 ms
tracert -m 30 -q 3 134.79.196.165 140 took 19 secs.
  
```

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


```

saqibali@saqibali-desktop: ~
saqibali@saqibali-desktop:~$ traceroute www6.slac.stanford.edu
traceroute to www6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte packets
 1  161.139.60.250 (161.139.60.250)  0.992 ms  1.308 ms  1.536 ms
 2  10.110.1.67 (10.110.1.67)  1.902 ms  1.736 ms  1.834 ms
 3  161.139.248.254 (161.139.248.254)  10.031 ms  10.316 ms  10.068 ms
 4  161.139.245.254 (161.139.245.254)  10.142 ms  4.861 ms  4.800 ms
 5  161.139.251.100 (161.139.251.100)  5.302 ms  10.583 ms  11.420 ms
 6  * * *
 7  203.80.23.153 (203.80.23.153)  16.505 ms  16.711 ms  16.463 ms
 8  203.80.22.137 (203.80.22.137)  15.111 ms  15.381 ms  16.749 ms
 9  203.80.23.62 (203.80.23.62)  14.736 ms  14.976 ms  14.600 ms
10  sg-so-05-v4.bb.tein3.net (202.179.249.69)  19.659 ms  * *
11  jp-pop-sg-v4.bb.tein3.net (202.179.249.78)  91.551 ms  91.653 ms  *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
saqibali@saqibali-desktop:~$

```

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 127.0.1.1 (pinger.fksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 10.60.80.109

CGI script maintainer: [Les Cottrell](#), SLAC. Script version 6.3334/26/2013, Les Cottrell.

To perform a traceroute using the path function from pinger.fksm.utm.my to the target, enter the desired target [host domain](#) (e.g. www.yahoo.com) or [Internet address](#) (e.g. 137.138.28.228) in the box below. Note the function is performed for the target's resolved Internet address.

Enter target name or address: then push 'Enter' key.

Lookup: [domain name](#) | [Locating a Host](#) | [visual traceroute](#) | [Find AS's between hosts](#) | [Find AS of a host](#) | [contacting someone](#)

Please note that traceroutes can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range 33434 - 33465, coming from pinger.fksm.utm.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a waste of both of our times. For more on this see [Traceroute security issues](#).

```

Executing exec(traceroute -m 30 -q 3 -f6 134.79.196.165)
traceroute to 134.79.196.165 (134.79.196.165), 30 hops max, 140 byte packets
 0  * * *
 1  161.139.60.250 (161.139.60.250)  0.992 ms  1.308 ms  1.536 ms
 2  10.110.1.67 (10.110.1.67)  1.902 ms  1.736 ms  1.834 ms
 3  161.139.248.254 (161.139.248.254)  10.031 ms  10.316 ms  10.068 ms
 4  161.139.245.254 (161.139.245.254)  10.142 ms  4.861 ms  4.800 ms
 5  161.139.251.100 (161.139.251.100)  5.302 ms  10.583 ms  11.420 ms
 6  * * *
 7  203.80.23.153 (203.80.23.153)  16.505 ms  16.711 ms  16.463 ms
 8  203.80.22.137 (203.80.22.137)  15.111 ms  15.381 ms  16.749 ms
 9  203.80.23.62 (203.80.23.62)  14.736 ms  14.976 ms  14.600 ms
10  sg-so-05-v4.bb.tein3.net (202.179.249.69)  19.659 ms  20.174 ms  20.174 ms
11  jp-pop-sg-v4.bb.tein3.net (202.179.249.78)  91.551 ms  91.653 ms  91.653 ms
12  tpr5-gb-1-0-4000.jp.apn.net (203.192.248.250)  91.005 ms  90.205 ms  89.908 ms
13  losa-tokyo-102.transpac.org (202.203.115.145)  214.843 ms  214.375 ms  217.252 ms
14  asnet1-1-is-jab-780.svcsa.pacificcable.net (207.231.246.2)  217.509 ms  217.203 ms  216.528 ms
15  slac2-18-a-superfz.es.net (134.55.36.22)  221.211 ms  221.983 ms  223.108 ms
16  rtr-border1-p2p-slac-mr2.slac.stanford.edu (192.68.191.240)  228.594 ms  228.896 ms  *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *

```

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

Related web sites

- [Traceroute](#)
- [ASes](#)
- [Monitoring](#)
- [tutorial](#)
- [Internet](#)
- [monitoring](#)
- [What is my IP address?](#)


Traceroute from UM to SLAC Option -f6

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

tracroute from 127.0.1.1 (pinger.fsksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 10.60.80.109 - Mozilla Firefox

tracroute from 127.0.1.1 ... | tracroute from 202.185.10... | View my IP information: 19...

Android | Google | Office | Personal | PingER | Research | Search Engines | UTM Malaysia | Google | Google Scholar | Wiki - Wikipedia, the ...



tracroute from 127.0.1.1 (pinger.fsksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 10.60.80.109

CGI script maintainer: [Les Cottrell](#), SLAC. Script version 6.3334/26/2013, Les Cottrell.

To perform a tracroute/ping/tracpath function from pinger.fsksm.utm.my to the target, enter the desired target host domain (e.g. www.yahoo.com) or Internet address (e.g. 137.138.28.228) in the box below. Note the function is performed for the target's resolved Internet address.

Enter target name or address: then push 'Enter' key.

Lookup: [domain name](#) | [Locating a Host](#) | [visual traceroute](#) | [Find AS's between hosts](#) | [Find AS of a host](#) | [contacting someone](#)

Related web sites

- [Traceroute servers.](#)
- [Monitoring tutorial.](#)
- [Internet monitoring](#)
- [What is my IP address?](#)

Please note that traceroutes can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range 33434 - 33465, coming from pinger.fsksm.utm.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a waste of both of our times. For more on this see [Traceroute security issues](#).

```

Executing exec(tracroute -s 30 -q 3 -n -f6 134.79.196.165 140)
tracroute to 134.79.196.165 (134.79.196.165), 30 hops max, 140 byte packets
 0 * * *
 1 203.80.23.153 20.434 ms 13.427 ms 17.436 ms
 2 203.80.22.137 18.541 ms 22.139 ms 17.890 ms
 3 203.80.23.62 17.378 ms 17.150 ms 14.794 ms
 4 202.179.249.09 20.306 ms 20.722 ms
 5 202.179.249.78 04.078 ms 87.701 ms 88.448 ms
 6 203.181.248.250 87.925 ms 87.547 ms 90.182 ms
 7 192.203.116.145 209.051 ms 206.613 ms 218.921 ms
 8 207.231.245.2 214.875 ms 214.114 ms 211.573 ms
 9 134.55.36.22 265.892 ms 217.380 ms 221.140 ms
10 192.08.191.246 225.892 ms 232.225 ms *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```


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

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

tracroute from 127.0.1.1 (pinger.fsksm.utm.my) to 134.79.196.165 (www6.slac.stanford.edu) for 161.139.220.152 - Mozilla Firefox

tracroute from 202.185.10... | View my IP information: 19...

Android | Google | Office | Personal | PingER | Research | Search Engines | UTM Malaysia | Google | Google Scholar | Wiki - Wikipedia, the ...



tracroute from 202.185.107.238 (pinger.fsktm.um.edu.my) to 134.79.196.165 (www6.slac.stanford.edu) for 161.139.220.152

CGI script maintainer: [Les Cottrell](#), SLAC. Script version 6.3334/26/2013, Les Cottrell.

To perform a tracroute/ping/tracpath function from pinger.fsktm.um.edu.my to the target, enter the desired target host domain (e.g. www.yahoo.com) or Internet address (e.g. 137.138.28.228) in the box below. Note the function is performed for the target's resolved Internet address.

Enter target name or address: then push 'Enter' key.

Lookup: [domain name](#) | [Locating a Host](#) | [visual traceroute](#) | [Find AS's between hosts](#) | [Find AS of a host](#) | [contacting someone](#)

Related web sites

- [Traceroute servers.](#)
- [Monitoring tutorial.](#)
- [Internet monitoring](#)
- [What is my IP address?](#)

Traceroute server at UTM April 1, 2014 at 8:22 PM

can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range pinger.fsktm.um.edu.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a waste of both of our times. For more on this see [Traceroute security issues](#).

```

Executing exec(tracroute -s 30 -q 3 -n -f6 134.79.196.165 140)
tracroute to 134.79.196.165 (134.79.196.165), 30 hops max, 140 byte packets
 0 180.87.112.87 37.152 ms 37.507 ms 36.493 ms
 1 180.87.112.8 226.355 ms 201.180 ms 226.392 ms
 2 180.87.180.17 190.533 ms 191.071 ms 190.308 ms
 3 64.86.21.1 160.753 ms 183.081 ms 191.270 ms
 4 190.129.44.53 151.506 ms 192.759 ms 194.632 ms
 5 * * *
 6 134.55.36.22 190.507 ms 190.718 ms 190.103 ms
 7 192.08.191.246 192.491 ms 194.045 ms 193.575 ms
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

tracroute -s 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:~$ traceroute -n -f6 www6.slac.stanford.edu  
traceroute to www6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte packets  
 0 * * *  
 1 * * *  
 2 * * *  
 3 * * *  
 4 * * *  
 5 * * *  
 6 * * *  
 7 203.80.23.153 27.674 ms 25.045 ms 25.630 ms  
 8 203.80.22.137 24.530 ms 21.160 ms 23.204 ms  
 9 203.80.23.62 20.793 ms 23.544 ms 26.001 ms  
10 202.179.249.69 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 100.837 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 232.987 ms 229.788 ms  
15 134.55.36.22 246.096 ms 214.475 ms 215.571 ms  
16 192.68.191.246 212.800 ms 215.501 ms *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 * * *  
23 * * *  
24 * * *  
25 * * *  
26 * * *  
27 * * *  
28 * * *  
29 * * *  
30 * * *  
saqibali@saqibali-desktop:~$
```

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

```
saqibali@saqibali-desktop: ~  
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  
saqibali@saqibali-desktop:~$ sudo traceroute -I 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 (203.80.22.137) 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) 20.309 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-is-jnb-780.snvaca.pacificwave.net (207.231.246.2) 249.285 ms 248.450 ms 249.666 ms  
15 slacnr2-ip-a-sunnrcs.es.net (134.55.36.22) 210.297 ms 209.982 ms 210.062 ms  
16 rtr-border1-p2p-slac-nr2.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  
saqibali@saqibali-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
 7 eu-mad-pr-v4.bb.tein3.net (202.179.249.118) [AS 24490] 971 msec 958 msec 929 msec
 8 ae3.mxl.par.fr.geant.net (62.40.98.55) [AS 20965] 939 msec 954 msec 937 msec
 9 switch-bckp-gw.mxl.par.fr.geant.net (62.40.124.82) [AS 20965] 216 msec 216 msec 217 msec
10 e513-e-rbx1-2-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.