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)



Traceroute from UM to SLAC





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

😫 🗇 💿 saqibali@saqibali-desktop: ~
saqibaligsaqibali-desktop:-\$ traceroute www6.slac.stanford.edu
traceroute to www.6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte pack
ets
1 161.139.68.258 (161.139.68.258) 8.992 MS 1.308 MS 1.536 MS
2 10.110.1.07 (10.110.1.07) 1.902 MS 1.730 MS 1.034 MS
3 161.139.248.234 (161.139.248.254) 10.031 MS 16.316 MS 10.068 MS
4 101-139.475.234 (101.139.243.234) 10.142 HS 4.801 HS 4.800 HS
6 * * *
7 203.80.23.153 (203.80.23.153) 16.585 ns 16.711 ns 16.463 ns
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 * * *
13 t t t
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
saqibaligsaqibali-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.

00	traceroute from 127.0.1	.1 (pinger.fsksm.utm.my) to 134.79.11	96.165 (www6.slac.stanford.edu) for 10.60.80.109 - M	tozilla Firefox	
🗶 tra	ceroute from 127.0.1.1 (🗴	🗍 traceroute from 202.185.10 🗵	🗟 View my IP information: 19 🔀 🌵		1
(–)	pinger.fsksm.utm.my/cgi-	bin/traceroute.pl?target-www6.slac.st	anford.edu&function=traceroute&options=-f6	☆ 🛩 😋 🚷 🕶 Google	🔍 🏫 🕋 Asr: 4:17 pm
An	friod 🐑 🥃 Google 🐑 🚘 Off	ice 👻 🦕 Personal 👻 🍟 PingER 🐑 🍟	Research 🐑 🍙 Search Engines 🐑 🍙 UTM Malaysia 🔻	🛿 Google 🔣 Google Scholar 🛛 W Wiki - Wikipedia, the	
0		tracerout	e from 127.0.1.1 (pinger.ts)	ksm.utm.my) to 134.79.196.165	Related web
			(wwwb.slac.stanford.ed)	u) for 10.60.80.109	Traceroute
ž		CG	3] script maintainer: <u>Les Cottrell</u> , <u>SLAC</u> . Scrip	pt version 6.3334/26/2013, Les Cottrell.	servers.
-	G-M	To another a large state to be a set	Download peri so	urce code.	tutorial,
	Color C	10 perform a traceroute/ping/tracepa 137.	.138.28.228) in the box below. Note the function is perfo	for the desired target instruction (e.g. www.yanob.com) or internet address (e	Internet
200	71	Enter	target name or address:	then push 'Enter' key.	What is my IP
		Lookup: <u>domain name</u>	Locating a Host visual traceroute Find A	S's between hosts Find AS of a host contacting someone	address?
	Please note that trac	eroutes can appear similar to	o port scans. If you see a suspected port	scan alert, for example from your firewall, with a series o	of ports in the range
	33434 - 33465, com	ing from pinger.fsksm.utm.m	ay it is probably a reverse traceroute from It almost certainly be a waste of both of	n our web based reverse traceroute server. Please do NOT	report this to us, it
			Traceroute security	rissues.	
	Executing exec(traceroute - a 30 - q 3 - f6 134.79.196.105 140)				
	tracervute to 134.79.106.165 (134.79.106.65), 30 hops max, 140 byte packets				
	7 203:80.23.153 (200:80.23.153) 16:27 ms 1 26:05 ms 15:067 ms 8 203:80.22.137 (200:80.22.137) 10:699 ms 16:44 am 17:727 ms				
	9 203.80, 23.45 (203.80, 25.42) 12.820 ms 12.754 ms 12.503 ms 1 10 ms-no-0-0-44.b. tenin 1-net [202.179.290; 05] 19.744 ms 1 20.154 (201.10) 10.154 (201.179.200; 05) 19.744 ms 1				
	11 jp-pap-5q-v4 hb tean3.met (202.179.204.78) 91.557 mi 88.044 ms 87.069 ms 12 tpr5-men-10-0005, man.met (202.192.204.78) 91.067 ms 90.2070 ms 88.078 ms				
	13 losa-tokyo-tp2.transpac. 4 esnet-1-is-imb-780.snvac	arg (192.203.116.145) 214.843 ms 21- a.pacificwave.net (207.231.246.2) 213	4.575 ms 217.252 ms 7.509 ms 217.203 ms 216.528 ms		
	15 slacmr2-ip-a-sunner5.es. 16 rtr-border1-p2p-slac-mr2	net (134.55.36.22) 221.211 ms 221.90 slac.stanford.edu (192.68.191.246)	83 ms 223.108 ms 228.594 ms 226.896 ms *		
	17 * * *				
	19 * * *				
	21 ***				
	23 * * *				
	25 * * *				
	27 • • •				
	29 • • •				
	traceroute -# 30 -q 3 -16 13	4.79.196.165 140 took 110 secs.			

Traceroute from UM to SLAC Option -f6

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

00	traceroute from 202.18	5.107.238 (pinger.fsktm.um.edu.my) to 1	34.79.196.165 (www6.slac.stanford.edu) for 1	61.139.220.152 - Mozilla FireFox	
X tra	sceroute from 127.0.1.1 (🔅	🗌 🗌 traceroute from 202.185.10 🕷 🚺	View my IP information: 19 🗵 💠		
4	pinger.fsktm.um.edu.my/	ogi-bin/traceroute.pl?target-www6.slac.st	anford.edu&function=traceroute&options=-f6	☆ ♥ 😋 🔣 ♥ Google	🔍 🏫 🕋 Asr: 4:17 pm
An	driod 👻 🥁 Google 👻 🚞 Off	ice 👻 🚞 Personal 👻 🚞 PingER 👻 🚞 Res	earch 👻 🍙 Search Engines 👻 🚘 UTM Malaysi	a 🔻 🚦 Google 🛜 Google Scholar 🛛 Wiki - Wikipedia, the	
2 O -> 🚓 🖨 💬		traceroute from CGI a To perform a traceroute/sing/tracegoth fi 137.13 Enter ta Lookup: domain name 1 Lookup: domain name 1 Lookup	202.185.107.238 (pinge www6.slac.stanford.edu cript maintainer: <u>Les Controll</u> , SLAC, S <u>Download perl</u> actos from pingerfatm.um eduany to the targu 2228) in the bot helw. Note the fruction is jr gret name or address: <u>controlledual tracerouter</u>	er.fsktm.um.edu.my) to 134.79.196.165 u) for 161.139.220.152 cript version 6.334/26(2013, Las Cottrell. <u>source code</u> et. eater the desired target <u>tackdomain</u> (e.g. www.sho.com) or <u>internet add</u> artformed for the target's resolved targetened address. then push "Enter' key. <u>dAS's between hosts [Find AS of a host] contacting someone</u> of com alort for avanuel for the my wave forward in with a conf	Related web sites Traceroute servers. Monitoring times (e.g. 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 rang 33434 - 33465, coming from pinger.fsktm.m.edu.my it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to u it will almost certainly be a waste of both of our times. For more on this see Traceroute security issues.				
	Executing exec(firserrate - traceruste 10:147, 20:54,00 6 ir-10-3-4-20:11.core:14,0 7 if-3_1ire(1-7,0-16,0),0 9 if-5_3_tire(1-7,0-16,0),0 9 if-5_3_tire(1-7,0-16,0),0 10 regreg if tarks.reft [18,8] 11 shear-in-sumer5.es. 12 shear-in-sumer5.es. 13 rft-Bardwir1-20-shear-0 14 shear-in-sumer5.es. 15 shear-in-sumer5.es. 16 shear-in-sumer5.es. 17 shear-in-sumer5.es. 18 shear-in-s	20 - 0 - 7 - 134, 79, 195, 105, 100) [114]7, 203, 204, 205, 20 hops nav. 140 byte 2-4ener-Angu as/053, net [106, 07, 112, 97] 2-4ener-Angu as/053, net [106, 07, 112, 97] 2-4ener-Angu as/053, net [106, 112, 20] 2-4e, 204, 201, 201, 202, 204, 204, 204, 204, 204, 204, 204	puckets 19.196 #1 38.073 mt 36.921 mt 3 4.66 mt 154.060 mt 19.195 mt 154.060 mt 19.125 mt 154.062 mt 19.125 mt 152.062 mt 19.126 mt 19.128 mt 19.128 mt 377 mt 105.466 mt 104.100 mt		

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

saqibali@saqibali-desktop:—\$ traceroute -f6 www6.slac.stanford.edu traceroute to www6.slac.stanford.edu (134.79.196.165), 30 hops max, 60 byte packets 6 * * *
7 203.80.23.153 (203.80.23.153) 20.485 ns 17.611 ns 18.342 ns 8 203.80.22.137 (203.80.22.137) 29.717 ns 29.567 ns 40.934 ns
9 203.00-23.02 (203.00-23.02) 17.001 NS 17.090 NS 19.05 NS 10 sg-so-05-v4.bb.tein3.net (202.179.249.69) 22.035 NS 21.238 NS 19.101 NS 11 jp-pop-sg-v4.bb.tein3.net (202.179.249.78) 91.058 NS 107.015 NS 92.397 NS
12 tpr5-ge0-1-0-4005.jp.apan.net (203.181.248.250) 93.894 ms 93.583 ms 90.367 ms 13 xe-0-0-0.259.ttr.losa.transpac.org (192.203.116.145) 209.151 ms 210.522 ms 211.691 ms
14 esnet-1-\s-jmb-/80.snvaca.pactT\cwave.net (207.231.246.2) 235.567 MS 212.310 MS 211.691 MS 15 slacmr2-\p-a-sunncr5.es.net (134.55.36.22) 220.430 MS 225.589 MS 227.197 MS 211.691 MS 16 rtr.border1-02n-slac-mr2.slac.stanford.edu (192.68.191.246.) 226.661 MS 228.616 MS *
17 * * * 18 * * *
19 * * * 28 * * *
22 * * *
24 * * * 25 * * *
26 * * * 27 * * *
29 * * * 39 * * *
saqtbali@saqtbali-desktop:-\$

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

traceroute -m 30 -q 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 127.0.1.1 (🔅	🛛 🖂 traceroute from 202.185.10 🛪 🔍 View my IP Information: 19 🗶 🌸			
🔶 🛞 pinger.fsktm. um.edu.my	r/cgi-bin/traceroute.pl?target=www6.slac.stanford.edu&function=traceroute&options=n=f6 💠 😴 🔃 • option to show total time in tracerouteQ	🕋 Asr: 4:17 pm		
Andriod = Google = Go	ffice 🔻 冲 Personal 👻 🎬 PingER 🐐 🏣 Research 🐐 🎬 Search Engines 👻 🚆 UTM Malaysia 🗴 🚼 Google 🔣 Google Scholar 🛛 W. Wiki - Wiki Pedia, the			
	traceroute from 202.185.107.238 (pinger.fsktm.um.edu.my) to 134.79.196.165 (www6.slac.stanford.edu) for 161.139.220.152	ated web s ceroute		
	CGI script maintainer: <u>Les Cottrell</u> , <u>SLAC</u> . Script version 6.334/26/2013. Les Cottrell. Mon <u>Download per l'ource code</u> .	vers. hitoring rial,		
	To perform a uncertainty and plan function in page 1 standing on the mapy curve the other angle programming with equivalence on an angle of the largest of t	rnet utoring at is my IP		
	Lookup: domain name Locating a Host visual traceroute Find AS's between hosts Find AS of a host contacting someone additional additionadditional additional additionad	ress?		
April 1, 2014 at 8:22 PM 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.				
Beculting esec(Tractrute -) terestrute (1147 y):152 1 (000000000000000000000000000000000000	a 20 - a 2 - a - (5 13 - 25 190 - 100 -			

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 6 * * *
7 203.80.23.153 27.674 ms 25.645 ms 25.630 ms 8 203.80.22.137 24.530 ms 21.168 ms 23.264 ms
9 203.80.23.62 20.793 MS 23.344 MS 20.681 MS N 10 202.179.249.69 26.310 MS 30.714 MS 30.680 MS 11 202.179.249.78 119.981 MS 105.178 MS 104.467 MS
12 203.101.248.250 105.324 ms 108.837 ms 107.179 ms 13 192.203.116.145 222.649 ms 223.193 ms 222.755 ms
14 207.231.246.2 236.793 MS 232.987 MS 229.788 MS 15 134.55.36.22 246.096 MS 214.475 MS 215.571 MS 16 192.68.191.246 212.880 MS 215.581 MS *
17 * * * 18 * * *
20 * * *
23 * * * 24 * * *
25 * * * 26 * * * 27 * * *
28 * * * 29 * * *
sogibali@saqibali-desktop:-\$

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



Traceroute from UTM Cisco border router to CERN

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 nsec 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 7 8 ae3.mx1.par.fr.geant.net (62.40.98.65) [AS 20965] 939 meec 954 meec 937 meec 9 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 × × ×

Translating "www.cern.ch"...domain server (202,188,0,133) [OK]

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

30 *

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.