Traceroute Over TCP vs UDP

For what purpose would one wish to send traceroute over TCP rather than UDP? What advantages/disadvantages are there in doing so? I know that traceroute normally uses UDP ICMP "echo" packets while traceroute with TCP uses "SYN" packets from its 3-way handshake, but I'm curious as to why one might be better than the other. If it depends on the situation, then what are those situations?

`tcp` `icmp` `traceroute` `udp`

edited Jan 3 '14 at 21:39
Mike Pennington
21.2k 8 52 115

asked Jan 3 '14 at 20:58
THE DOCTOR
413 2 9 23

I assume you're asking about `tcptraceroute` , correct? – Mike Pennington Jan 3 '14 at 21:17

1 Either that implementation or traceroute -T -p 80 which will, for example, execute traceroute over TCP port 80. – THE DOCTOR Jan 3 '14 at 21:21

2 Sometimes udp is blocked, and the only way to do a trace route is to use tcp with a port that is allowed. e.g. port 80 (web) or port 25 (smtp) – Pieter Jan 6 '14 at 6:56

3 Answers

There's no such thing as "*UDP ICMP "echo"*". traceroute sends a UDP *probe* with an increasing TTL. That probe is a single datagram destined for a high port which is unlikely to be a listening service. As the datagram flows out across the network, the TTL decrements until it hits zero at which point an ICMP ERROR ("time exceeded") is generated. That ICMP message identifies a "hop". When the TTL is enough to reach the target, as there's no listener on that port, an ICMP "port unreachable" error is generated, thus ending the trace.

The purpose of `tcptraceroute` is to do the same sort of path check with a TCP connection. It is most useful in diagnosing connection issues to a specific service. (eg. a web server) As the probes look like a normal TCP connection attempt, they'll go through NAT, firewalls, ACLs, rate-limits, etc. exactly as a connection from the intended application.

answered Jan 3 '14 at 22:01
Ricky Beam
16.2k 1 19 49

I was under the impression that traceroute sends UDP ICMP echo request packets to the specified destination, does it not? Also, you specify a good reason to use tcptraceroute. However, why not just use tcptraceroute by default? Does the (UDP) traceroute have any specific advantages? – THE DOCTOR Jan 3 '14 at 22:16

5 There's no such f'ing thing as a "UDP ICMP echo". UDP and ICMP are *totally* different things. By default traceroute uses UDP; many versions support "-I" to use ICMP echo -- useful if your firewall or NAT cannot handle the UDP probes. – Ricky Beam Jan 3 '14 at 22:27

2 I think part of the confusion is that MS Windows DOES send ICMP echo requests (with an increasing TTL) when using tracert.exe. Cisco routers (and most *nix devices) use UDP probes as described by Ricky. – Ron Trunk Jan 3 '14 at 23:14

@Ron so it does. I never paid any attention to how M$ cared to do anything. The main point stands... UDP and ICMP are different things. – Ricky Beam Jan 3 '14 at 23:53

@Ricky Beam - Whoops, yes you are correct. – THE DOCTOR Jan 6 '14 at 16:50

Tcp traceroutes could be used to test for access lists blocking a given protocol on routers, firewalls or intrusion prevention systems. Both good guys and bad guys have an interest in such knowledge. Tools such as tcptraceroute are common in a penetration testers toolbox and

might be found on a savvy network administrators system.

answered Jan 5 '14 at 12:43
packetloss
121 3

Traceroute relies on sending out probes with controlled TTL and monitoring the ICMP time exceeded errors that come back.

The probes can be any protocol. Windows uses ICMP echo packets by default. Most unix-like systems uses UDP packets by default.

If our networks were as simple as the designers of the internet envisaged there would be no need to have options for changing the protocol used in traceroute but in reality we have firewalls, NATs, traffic prioritisation systems etc. Using the same protocol (and possibly the same port number) for your trace as the protocol the application will actually use increases the chance that the results of your traceroute will be representative of the network your application will see.

answered Nov 13 '16 at 10:51
Peter Green
3,461 1 6 19
