sign up log in tour help

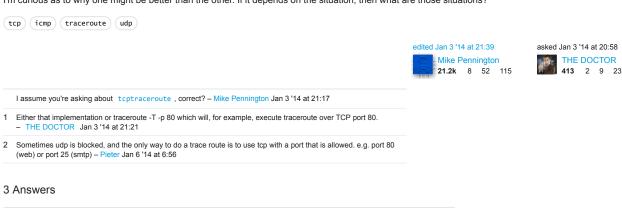
Network Engineering Stack Exchange is a question and answer site for network engineers. Join them; it only takes a minute:

Sign up

Anybody can ask Anybody can The best answers are voted a question answer up and rise to the top

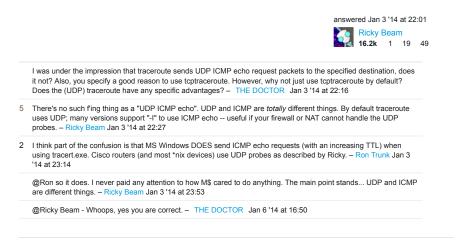
Traceroute Over TCP vs UDP

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?



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.



Top 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 toptraceroute are common in a penetration testers toolbox and

1 of 2 3/18/17, 23:49

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

2 of 2 3/18/17, 23:49