Trace route command using in linux command line

Installing the package
[crayon-6684c76a23468768438879/]
[crayon-6684c76a23471508336791/]

> Windows tracert in linux ?

[crayon-6684c76a23475428947869-i/] equivalents to [crayon-6684c76a23477894696210-i/]

To run Windows equivalent tracert command,

enter:
[crayon-6684c76a23479818164768/]
[crayon-6684c76a2347b389376858/]
Disable IP address and host name mapping
Traceroute provides an option through which the mapping of IP addresses with host name (that traceroute tries) is disabled. The option for doing this is '-n' . The following example illustrates this :
[crayon-6684c76a2347d550102669/]

Configure Response Wait Time

The time for which traceroute utility waits after issuing a probe can also be configured. This can be done through '-w' option that it provides. The -w option expects a value which the utility will take as the response time to wait for. In this example, the wait time is 0.1 seconds and the traceroute utility was unable to wait for any response and it printed all the *'s.
[crayon-6684c76a23480387379651/]

Configure Number of Queries per Hop
[crayon-6684c76a23482429707065/]

Configure the TTL value to start with

Traceroute utility is flexible enough to accept the TTL value that the user wants to start the utility with. By default its value is 1 which means it starts off with the first router in the path but using the '-f' option (which expects the new value of TTL) a new value of the TTL field can be set. For example, I tried a normal traceroute operation and then tried a traceroute with a different TTL value.
[crayon-6684c76a23484278976575/]

Description of Tracert
[crayon-6684c76a23487716612622/]

Tracert Options

[crayon-6684c76a2348a984010706/]

*** Implementation of tracert**

Traceroute running on OS X Snow Leopard
Traceroute, by default, sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host; ICMP Echo Request or TCP SYN packets can also be used.[1] The time-to-live(TTL) value, also known as *hop limit*, is used in determining the intermediate routers being traversed towards the destination. Routers decrement TTL values of packets by one when routing and discard packets whose TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded.[2] Common default values for TTL are 128 (Windows OS) and 64 (Unix-based OS).

Traceroute works by sending packets with gradually increasing

TTL value, starting with TTL value of one. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of two, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.[2]

The timestamp values returned for each router along the path are the delay (latency) values, typically measured in milliseconds for each packet.
[crayon-6684c76a23491608098236/]
The sender expects a reply within a specified number of seconds. If a packet is not acknowledged within the expected interval, an asterisk is displayed. The Internet Protocol does not require packets to take the same route towards a particular destination, thus hosts listed might be hosts that other packets have traversed. If the host at hop #N does not reply, the hop is skipped in the output.

On Unix-like operating systems, the traceroute utility uses User Datagram Protocol (UDP) datagrams by default, with destination port numbers ranging from 33434 to 33534. The traceroute utility usually has an option to instead use ICMP Echo Request (type 8) packets, like the Windows tracert utility does, or to use TCP SYN packets.[1][2] If a network has a firewall and operates both Windows and Unix-like systems, more than one protocol must be enabled inbound through the firewall for traceroute to work and receive replies.

Some traceroute implementations use TCP packets, such as tcptraceroute or layer four traceroute. PathPing is a utility introduced with Windows NT that combines ping and traceroute

functionality. MTR is an enhanced version of ICMP traceroute available for Unix-like and Windows systems. The various implementations of traceroute all rely on ICMP Time Exceeded (type 11) packets being sent to the source.

The implementations of traceroute shipped with Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, and OS X include an option to use ICMP Echo packets (-I), or any arbitrary protocol (-P) such as UDP, TCP or ICMP. On Linux, tracepath is a utility similar to traceroute, with the primary difference of not requiring superuser privileges.[3]

Cisco's implementation of traceroute also uses a sequence of UDP datagrams, each with incrementing TTL values, to an invalid port number at the remote host; by default, UDP port 33434 is used. Extended version of this command (known as the *extended traceroute* command) can change the destination port number used by the UDP probe messages.[4]

Usage

Most implementations include at least options to specify the number of queries to send per hop, time to wait for a response, the **hop limit** and port to use. Invoking traceroute with no specified options displays the list of available options, while man traceroute presents more details, including the displayed error flags. Simple example on Linux:

[crayon-6684c76a23496017508259/]
In the example above, selected options are to wait for three seconds (instead of five), send out only one query to each hop (instead of three), limit the maximum number of hops to 16 before giving up (instead of 30), with example.com as the final host.

This can help identify incorrect routing table definitions or

firewalls that may be blocking ICMP traffic, or high port UDP in Unix ping, to a site. Note that a firewall may permit ICMP packets but not permit packets of other protocols.

Traceroute is also used by penetration testers to gather information about network infrastructure and IP ranges around a given host.

It can also be used when downloading data, and if there are multiple mirrors available for the same piece of data, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Origins

The traceroute manual page states that the original traceroute program was written by Van Jacobson in 1987 from a suggestion by Steve Deering, with particularly cogent suggestions or fixes from C. Philip Wood, Tim Seaver and Ken Adelman. Also, the inventor of the ping program, Mike Muuss, states on his website that traceroute was written using kernel ICMP support that he had earlier coded to enable raw ICMP sockets when he first wrote the ping program.[5]

References

1. ^ Jump up to:[a] [b] “traceroute(8) – Linux man page”. linux.die.net. Retrieved 2014-02-26.
2. ^ Jump up to:[a] [b] [c] Comer, Douglas (2004). *Computer Network and Internets with Internet Applications*. Pearson Education, Inc. pp. 360–362. ISBN 0131433512.
3. **Jump up^** “tracepath(8) – Linux man page”. *linux.die.net*.

Retrieved 2015-06-21.
4. **Jump up^** “Understanding the Ping and Traceroute Commands”. *Cisco IOS Software Releases 12.1 Mainline*. cisco.com. 2006-11-29. Retrieved 2013-12-08.
5. **Jump up^** The Story of the PING Program
6. kutayzorlu.com