USING TRACEROUTE

Using a traceroute can be explained in terms of diagnosing or troubleshooting network problems by using the same tool, as below
Finding the problem:

1. Timeouts
2. Long routes
3. High round-trip times
4. Routing weirdness

Timeouts
Once a probe packet is injected on the network the traceroute cannot wait forever for the reply packet, as the probe packet may be lost on transit due to various reasons or even if the probe packet ever reached the destination machine the reply packet may have been lost because of various reasons. And thus it is needed to set up a timeout for each probe-reply cycles. If there is a reply back within that timeout parsing the reply packet can be continued, else a traditional '*' can be printed and continue with the next probe-reply cycle.

Long routes
If route to a server is very long, performance is going to suffer. A long route can be due to less-than-optimal configuration within some network along the way.

High latency
The three numbers given on each line of output show the round trip times (latency) in milliseconds. Smaller numbers generally mean better connections. As the latency of a connection increases, interactive response suffers. Download speed can also suffer as a result of high latency (due to TCP windowing), or as a result of whatever is actually causing that high latency.

Typically, a modem connection's inherent latency will be around 120-130ms. The latency on an ISDN line is usually around 40-45ms.

In a trace output, a large "jump" in latency from one hop to the next, that could indicate a problem. It could be a saturated (overused) network link; a slow network link; an overloaded router; or some other problem at that hop. Of course, it could also be a problem anywhere on the return route from the high-latency hops as well. Ping program (described below) to get a better idea of the latency as well as the packet loss to a given site or router; traceroute only does three probes per router (by default), which isn't a very good sample on its own.

A jump in latency can also indicate a long hop, such as a cross-country link or one that crosses an ocean. A long line is naturally going to have higher latency than a short one.

Routing weirdness
One example of "weirdness" that might be seen in traceroute output is exposure of private address space. Certain ranges of IP addresses are reserved for private, non-Internet use. These address ranges are not assigned to anyone, and are open for use by any system. They cannot be routed over the Internet, and thus are for internal

use only. Sending traffic between private address space and outside networks must be done via internal routing or address translation.
The reserved private address ranges are:

- 10.*
- 172. [16-31].*
- 192.168.*

Private addresses should never be visible over the Internet. But, sometimes it can be seen in the traceroute output. If they appear within local network, this is okay; private addresses inside own network can be visible. If, however, they appear within someone else's network, it can be problematic.

Visibility of private IP addresses doesn't necessarily (or even usually) mean that the route does not work. It is often simply the way the administrators of the target network have set up their system. In fact, the output above, despite the private IP address and the timeouts, shows a route that works perfectly well for web access.

However, a route which includes private addresses is difficult to troubleshoot. As it is not possible to ping the private routers to see if there is any packet loss, it can’t trace directly from other sites. And in general, they show a certain level of cluelessness in how the network is set up.

The network companies for security purpose do it, by not exposing their network for traceroute request. Obviously, this makes any kind of troubleshooting of this connection next to impossible. If such encounter problems in this situation, the best to do is contact the network provider.

Sometimes it might be seen that a router start “looping” back and forth between two routers, until the 30-hop limit is reached. This is a routing loop. This usually means that one router has lost communication (BGP) with another, and thus has dropped that route. Since the router has lost the route it needs, it sends the packet back where it came from, thinking maybe that is the best route. That router knows better and sends it back to the other one, over and over.

Input
As mentioned before entire user interface will be on the command line. The usage of the tool will be as below
USAGE: program_name [options] hostname
Program_name is the name of the executable

- Hostname will be a valid hostname which has IPv4 address associated to it.
- There are two options: port and max_hop. By default, port is 33434 and max_hop is 30. However, user may explicitly specify these values.

Output
Output will be in the format as given below
<TTL> <Host Name> < (Host IP address) >
The output format is similar to the output obtained when UNIX traceroute command is run. In case the host name field cannot be retrieved the IP address itself is printed in its place. This occurs when host name is not visible. In cases of private IP addresses only * is displayed since IP address cannot be retrieved.