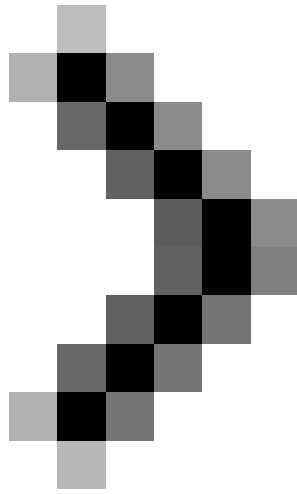


# Troubleshoot connectivity problems in the network - Part 5

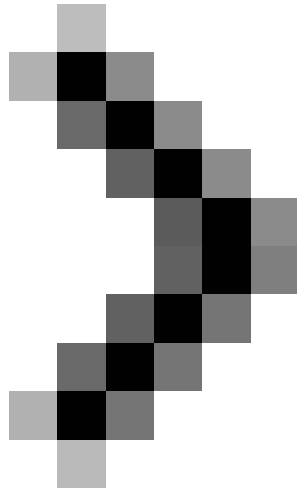
This section will continue the series on troubleshooting connection problems by checking the output of the TRACERT command.



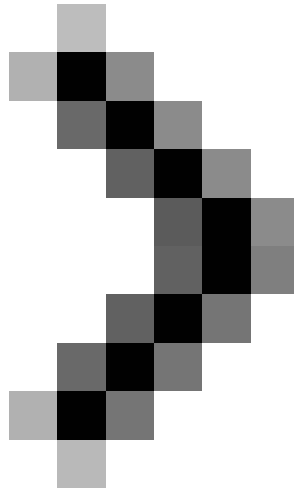
Troubleshoot network connectivity problems (Part 1)



Troubleshoot network connectivity problems (Part 2)

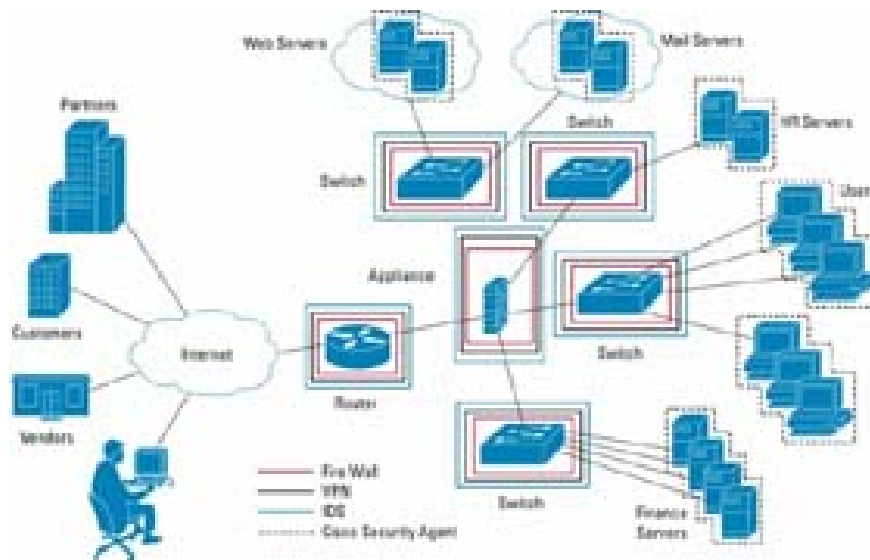


Troubleshoot network connectivity problems (Part 3 )



## Troubleshoot network connectivity problems (Part 4)

*Brien M. Posey*



**Network Administration** - In the previous part of this series, we introduced the TRACERT command, which can be used to diagnose connectivity issues between local hosts and hosts on networks from far away. In that section, I talked a little bit about the TRACERT command, so this section will continue the discussion by showing you how to interpret the results of this command.

For that purpose, we have executed the *TRACERT* against *www.espn.com* domain. The reason why we chose this particular domain is because it is one of those sites that we know easily and that does not block ICMP traffic. You can see the output of the command below. We will reference this output throughout the rest of the lesson.

```
C: UsersAdministrator> TRACERT www.espn.com
```

output with up to 30 jumps.

```
1 2 ms 1 ms  
2 10 ms 10 ms 9 ms 208.104.224.1  
3 9 ms 9 ms 9 ms 208.104.1.13  
4 9 ms 8 ms 9 ms 208.104.0.13  
5 10 ms 9 ms 10 ms 208.104.0.1  
6 11 ms 14 ms 10 ms 165.166.125.193  
7 11 ms 10 ms 11 ms gig-1-1-3.core01.ncchr1.infoave.net [165.166.22.61]  
8 31 ms 31 ms 30 ms 64.200.130.17  
9 38 ms 39 ms 40 ms hrndva1wcx2-pos15-3-oc48.wcg.net [64.200.240.213]  
10 31 ms 31 ms 31 ms 64.200.249.170  
11 31 ms 30 ms 31 ms 4.68.110.5  
12 48 ms 35 ms 35 ms vlan99.csw4.Washington1.Level3.net [4.68.17.254]  
13 32 ms 31 ms 33 ms ae-92-92.ebr2.Washington1.Level3.net [4.69.134.157]  
14 60 ms 53 ms 54 ms ae-2.ebr3.Chicago1.Level3.net [4.69.132.69]  
15 86 ms 71 ms 70 ms ae-3.ebr2.Denver1.Level3.net [4.69.132.61]  
16 137 ms 103 ms 102 ms ae-2.ebr2.Seattle1.Level3.net [4.69.132.53]  
17 95 ms 95 ms 95 ms ae-23-52.car3.Seattle1.Level3.net [4.68.105.36]  
18 94 ms 95 ms 95 ms WALT-DISNEY.car3.Seattle1.Level3.net [4.71.152.22]  
19 * * * Request timed out.  
20 97 ms 95 ms 98 ms 199.181.132.250  
Trace complete.
```

If you look at the output of the above command, you will see that each output line has a number of different information. The first part found on the leftmost side of each line is the number of hops. As we discussed in the previous section, the *TRACERT* will work by sending a ping request to a specific host. Initially, the TTL value is set to 1. This value ensures that the request will fail after the first hop. Jump information is available and then the ICMP request is retransmitted, but for now the value is set to 2. This process is repeated, the TTL value is increased by 1 until when reaching the destination host. By doing so, *TRACERT* can report on how many hops the request has made to reach the remote host. If you look at the last line in the output, then it will start with the number 20. This number represents the 20 steps that have been taken to reach the destination host.

The next three pieces of information on each line show the amount of time it takes to reach the router or host that each line represents. If you look at the entire list you will see that time links gradually increase in each jump. There are two things that you really need to know about the time links shown here.

First, there are three distinct time periods displayed for each jump. As mentioned earlier, tracing is based on the concept of sending many ICMP requests. When we work with the ping command above in this series, you saw the ping command always returns 4 different values to evaluate the packet. The same concept is also applied to trace routes, except for the time period of requests that are evaluated three times instead of four.

The second thing is that you need to know about the number of replies, an asterisk indicates that a request has been timed out. This may or may not show us the problem, depending on how the asterisk appears. Looking at the jump at 19 in the output above you will see that all three response time values are represented by asterisks. When you see these three asterisks in a row, it means that the device on which the command is executing a ping in the firewall has been configured to reject ICMP packets, which will cause timeouts and The last column will display from Request Timed Out.

It should be noted that Trace route will also display three asterisks when the destination device is not reachable. So what's the difference between a site that blocks ICMP packets and a failed link?

With a little attention you will see that a failed link will look like what you see when a router or host blocks ICMP requests. When a failure occurs, you will not see an error message appear. In fact, the process will end with a standard Trace Complete message.

There are two signs when a link failure appears. A sign is not in the trace problem, every result is returned times out. Another sign of a link failure is that the TRACERT will perform all 30 hops. None of these conditions ensure that a link failure occurs even when they appear together. For example, the tested Web site (www.brienposey.com) is currently working well, and still runs the TRACERT with it, both of which appear, see the output below:

Use *TRACERT* for www.brienposey.com [24.235.10.4]

up to 30 steps:

```
 1 1 ms 1 ms
 2 8 ms 12 ms 8 ms 208.104.224.1
 3 9 ms 8 ms 9 ms 208.104.1.9
 4 10 ms 9 ms 8 ms 208.104.0.9
 5 10 ms 12 ms 11 ms 208.104.0.5
 6 12 ms 10 ms 9 ms 165.166.18.1
 7 15 ms 23 ms 13 ms gig2-2-1.c01.scclma.infoave.net [165.166.22.17]
 8 13 ms 12 ms 13 ms 66.192.166.9
 9 31 ms 30 ms * peer-01-ge-0-0-0-1.asbn.twtelecom.net [64.129.249.10]
10 56 ms 57 ms 55 ms bb2-p6-0.ipltin.sbcglobal.net [151.164.242.59]
11 55 ms 53 ms 55 ms ded2-g8-0.ipltin.sbcglobal.net [151.164.42.159]
12 59 ms 56 ms 56 ms Winnet-1148485.cust-rtr.ameritech.net [66.73.221.254]
13 64 ms 63 ms 68 ms 216-24-2-237.ip.win.net [216.24.2.237]
14 68 ms 68 ms 64 ms fa0-0.cust-gw2.noc.win.net [216.24.30.69]
15 * * * Request timed out.
16 * * * Request timed out.
17 * * * Request timed out.
18 * * * Request timed out.
19 * * * Request timed out.
20 * * * Request timed out.
21 * * * Request timed out.
22 * * * Request timed out.
23 * * * Request timed out.
24 * * * Request timed out.
25 * * * Request timed out.
```

```
26 * * * Request timed out.  
27 * * * Request timed out.  
28 * * * Request timed out.  
29 * * * Request timed out.  
30 * * * Request timed out.  
Trace complete.
```

If you look at the output as you see the output above, you can see that the link failure has appeared, but it is not so sure. The only way to make sure is to run the *TRACERT* on multiple pages and see if you see the same type of results. Please note that the higher the number of hops, the farther the target device you perform is away from you. The farther a failure is, the harder it is to diagnose because tests for other sites can use other routes. When you perform tests on multiple sites, you will have to look at the many routes that have been used to distinguish whether the missing link appears.

The last information displayed on each line is the information that distinguishes the router or host that responded to the ICMP request. The *TRACERT* command will distinguish each host or router by name when possible, but you will not always have the names of these routers. For example, if you look at the output above, you will see that half of the routers are distinguished by name, while others are not.

What you can see here is that the host you are tracing will not always be displayed in the correct name. For example, if you look at the beginning of the output of the first example above, you will see that we entered the command *TRACERT WWW.ESPN.COM*. Immediately after doing so, the *TRACERT* has processed *www.espn.com* with the address *199.181.132.250*. If you still notice that until the end of the output, you will see that *TRACERT* has reached its destination but does not distinguish the destination by name.

This behavior is not difficult to understand, it is due to design. The reason why we show you this is so that you do not execute the *TRACERT* against a site and should think that the process has failed because the destination host has not been properly represented.

## Conclude

In this section, we have shown you how to decode the output of a *TRACERT* . In the next part of this series, I will show you how to use the *Route* command to check the machine's routing table.

You finished reading the article "**Troubleshoot connectivity problems in the network - Part 5**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.