**Network Troubleshooting**

Troubleshooting network problems is something that you will often encounter if you haven't already. We are going to practice some of the previously discussed tools, that can help you isolate, troubleshoot and fix problems in your network.

Suppose you need to perform an Internet search, but your web browser can not find [google.com](http://google.com/), saying the host is unknown. Let's proceed step by step to fix this.

1. First make certain your network is properly configured. If your Ethernet device is up and running, running **ifconfig** should display something like:

**student:/tmp> /sbin/ifconfig**

**eno167777 Link encap:Ethernet HWaddr 00:0C:29:BB:92:C2**

**inet addr:192.168.1.14 Bcast:192.168.1.255 Mask:255.255.255.0**

**inet6 addr: fe80::20c:29ff:febb:92c2/64 Scope:Link**

**UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1**

**RX packets:3244 errors:0 dropped:0 overruns:0 frame:0**

**TX packets:2006 errors:0 dropped:0 overruns:0 carrier:0**

**collisions:0 txqueuelen:1000**

**RX bytes:4343606 (4.1 Mb) TX bytes:169082 (165.1 Kb)**

**lo Link encap:Local Loopback**

**inet addr:127.0.0.1 Mask:255.0.0.0**

**inet6 addr: ::1/128 Scope:Host**

**UP LOOPBACK RUNNING MTU:65536 Metric:1**

**RX packets:0 errors:0 dropped:0 overruns:0 frame:0**

**TX packets:0 errors:0 dropped:0 overruns:0 carrier:0**

**collisions:0 txqueuelen:0**

**RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)**

On older systems you probably will see a less cryptic name than **eno167777**, like **eth0**, or for a wireless connection, you might see something like **wlan0** or **wlp3s0**. You can also show your **IP** address with:

**student:/tmp> ip addr show**

**1: lo: mtu 65536 qdisc noqueue state UNKNOWN group default**

**link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00**

**inet 127.0.0.1/8 scope host lo**

**valid\_lft forever preferred\_lft forever**

**inet6 ::1/128 scope host**

**valid\_lft forever preferred\_lft forever**

**2: eno16777736: mtu 1500 qdisc pfifo\_fast state \**

**UP group default qlen 1000**

**link/ether 00:0c:29:bb:92:c2 brd ff:ff:ff:ff:ff:ff**

**p inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic eno16777736**

**valid\_lft 84941sec preferred\_lft 84941sec**

**inet 192.168.1.15/24 brd 192.168.1.255 scope global secondary dynamic eno16777736**

**valid\_lft 85909sec preferred\_lft 85909sec**

**inet6 fe80::20c:29ff:febb:92c2/64 scope link**

**valid\_lft forever preferred\_lft forever**

Does the IP address look valid? Depending on where you are using this from, it is most likely a Class C IP address; in the above this is **192.168.1.14**

If it does not show a device with an **IP** address, you may need to start or restart the network and/or **NetworkManager**. Exactly how you do this depends on your system. For most distributions one of these commands will accomplish this:

**student:/tmp> sudo systemctl restart NetworkManager**

**student:/tmp> sudo systemctl restart network**

**student:/tmp> sudo service NetworkManager restart**

**student:/tmp> sudo service network restart**

If your device was up but had no **IP** address, the above should have helped fix it, but you can try to get a fresh address with:

**student:/tmp> sudo dhclient eth0**

substituting the right name for the Ethernet device.

1. If your interface is up and running with an assigned **IP** address and you still can not reach [google.com](http://google.com/), we should make sure you have a valid hostname assigned to your machine, with **hostname**:

**student:/tmp> hostname**

**openSUSE**

It is rare you would have a problem here, as there is probably always at least a default hostname, such as **localhost**.

1. When you type in a name of a site such as [google.com](http://google.com/), that name needs to be connected to a known IP address. This is usually done employing the **DNS** sever (**D**omain **N**ame **S**ystem)

First, see if the site is up and reachable with **ping**:

**student:/tmp> sudo ping -c 3 google.com**

**PING google.com (216.58.216.238) 56(84) bytes of data.**

**64 bytes from ord31s22-in-f14.1e100.net (216.58.216.238): icmp\_seq=1 ttl=51 time=21.7 ms**

**64 bytes from ord31s22-in-f14.1e100.net (216.58.216.238): icmp\_seq=2 ttl=51 time=23.8 ms**

**64 bytes from ord31s22-in-f14.1e100.net (216.58.216.238): icmp\_seq=3 ttl=51 time=21.3 ms**

**--- google.com ping statistics ---**

**3 packets transmitted, 3 received, 0% packet loss, time 2002ms**

**rtt min/avg/max/mdev = 21.388/22.331/23.813/1.074 ms**

Note:

* + We have used **sudo** for **ping**; recent **Linux** distributions have required this to avoid clueless or malicious users from flooding systems with such queries.
  + We have used **-c 3** to limit to 3 packets; otherwise **ping** would run forever until forcibly terminated, say with **CTRL-C**.

If the result was:

**ping: unknown host google.com**

It is likely that something is wrong with your DNS set-up. (Note on some systems you will never see the unknown host message, but you will get a suspicious result like:

**student:/tmp> sudo ping l89xl28vkjs.com**

**PING l89xl28vkjs.com.site (127.0.53.53) 56(84) bytes of data.**

**64 bytes from 127.0.53.53: icmp\_seq=1 ttl=64 time=0.016 ms**

**...**

where the **127.0.x.x** address is a loop feeding back to the host machine you are on. You can eliminate this as being a valid address by doing:

**student:/tmp> host l89xl28vkjs.com**

**Host l89xl28vkjs.com not found: 3(NXDOMAIN)**

whereas a correct result would look like:

**student:/tmp> host google.com**

**google.com has address 216.58.216.206**

**google.com has IPv6 address 2607:f8b0:4009:80b::200e**

**google.com mail is handled by 20 alt1.aspmx.l.google.com.**

**google.com mail is handled by 10 aspmx.l.google.com.**

**google.com mail is handled by 30 alt2.aspmx.l.google.com.**

**google.com mail is handled by 40 alt3.aspmx.l.google.com.**

**google.com mail is handled by 50 alt4.aspmx.l.google.com.**

The above command utilizes the **DNS** server configured in **/etc/resolv.conf** on your machine. If you wanted to override that you could do:

**host 8.8.8.8**

**8.8.8.8.in-addr.arpa domain name pointer google-public-dns-a.google.com.**

**student@linux:~> host google.com 8.8.8.8**

**Using domain server:**

**Name: 8.8.8.8**

**Address: 8.8.8.8#53**

**Aliases:**

**google.com has address 216.58.216.110**

**google.com has IPv6 address 2607:f8b0:4009:804::1002**

**...\**

where we have used the publicly available **DNS** server provided by **Google** itself. (Using this or another public server can be a good trick sometimes if your network is up but **DNS** is ill; in that case you can also enter it in **resolv.conf**.)

Note that there is another file, **/etc/hosts**, where you can associate names with **IP** addresses, which is used **before** the **DNS** server is consulted. This is most useful for specifying nodes on your local network.

You could also use the **dig** utility if you prefer:

**student:/tmp> dig google.com**

**; <<>> DiG 9.9.5-rpz2+rl.14038.05-P1 <<>> google.com**

**;; global options: +cmd**

**;; Got answer:**

**;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29613**

**;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 1**

**;; OPT PSEUDOSECTION:**

**; EDNS: version: 0, flags:; MBZ: 1c20 , udp: 1280**

**;; QUESTION SECTION:**

**;google.com. IN A**

**;; ANSWER SECTION:**

**google.com. 244 IN A 173.194.46.67**

**google.com. 244 IN A 173.194.46.65**

**google.com. 244 IN A 173.194.46.71**

**google.com. 244 IN A 173.194.46.73**

**google.com. 244 IN A 173.194.46.69**

**google.com. 244 IN A 173.194.46.68**

**google.com. 244 IN A 173.194.46.64**

**google.com. 244 IN A 173.194.46.72**

**google.com. 244 IN A 173.194.46.70**

**google.com. 244 IN A 173.194.46.66**

**google.com. 244 IN A 173.194.46.78**

**;; Query time: 22 msec**

**;; SERVER: 192.168.1.1#53(192.168.1.1)**

**;; WHEN: Mon Apr 20 08:58:58 CDT 2015**

**;; MSG SIZE rcvd: 215**

1. Suppose **host** or **dig** fail to connect the name to an **IP** address. There are many reasons **DNS** can fail, some of which are:
   * The **DNS** server is down. In this case try **ping**ing it to see if it is alive (you should have the **IP** address in **/etc/resolv.conf**.
   * The server can be up and running, but **DNS** may not be currently available on the machine.
   * Your **route** to the **DNS** server may not be correct.

How can we test the route? Tracing the route to one of the public name server we mentioned before:

**student@linux:~> sudo traceroute 8.8.8.8**

**traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets**

**1 192.168.1.1 (192.168.1.1) 0.405 ms 0.494 ms 0.556 ms**

**2 10.132.4.1 (10.132.4.1) 15.127 ms 15.107 ms 15.185 ms**

**3 dtr02ftbgwi-tge-0-6-0-3.ftbg.wi.charter.com (96.34.24.122)**

**15.243 ms 15.327 ms 17.878 ms**

**4 crr02ftbgwi-bue-3.ftbg.wi.charter.com (96.34.18.116) 17.667 ms 17.734 ms 20.016 ms**

**5 crr01ftbgwi-bue-4.ftbg.wi.charter.com (96.34.18.108) 22.017 ms 22.359 ms 22.052 ms**

**6 crr01euclwi-bue-1.eucl.wi.charter.com (96.34.16.77) 29.430 ms 22.705 ms 22.076 ms**

**7 bbr01euclwi-bue-4.eucl.wi.charter.com (96.34.2.4) 17.795 ms 25.542 ms 25.600 ms**

**8 bbr02euclwi-bue-5.eucl.wi.charter.com (96.34.0.7) 28.227 ms 28.270 ms 28.303 ms**

**9 bbr01chcgil-bue-1.chcg.il.charter.com (96.34.0.9) 33.114 ms 33.072 ms 33.175 ms**

**10 prr01chcgil-bue-2.chcg.il.charter.com (96.34.3.9) 36.882 ms 36.794 ms 36.895 ms**

**11 96-34-152-30.static.unas.mo.charter.com (96.34.152.30) 42.585 ms 42.326 ms 42.401 ms**

**12 216.239.43.111 (216.239.43.111) 28.737 ms 216.239.43.113 (216.239.43.113)**

**24.558 ms 23.941 ms**

**13 209.85.243.115 (209.85.243.115) 24.269 ms 209.85.247.17 (209.85.247.17)**

**25.758 ms 216.239.50.123 (216.239.50.123) 25.433 ms**

**14 google-public-dns-a.google.com (8.8.8.8) 25.239 ms 24.003 ms 23.795 ms**

Again, this should likely work for you, but what if you only got the first line in the **traceroute** output?

If this happened, most likely your default route is wrong. Try:

**student:/tmp> ip route show**

**efault via 192.168.1.1 dev eno16777736 proto static metric 1024**

**192.168.1.0/24 dev eno16777736 proto kernel scope link src 192.168.1.14**

Most likely this is set to your network interface and the IP address of your router, **DSL**, or Cable Modem. Let's say that it is blank or simply points to your own machine. Here's your problem! At this point, you would need to add a proper default route and run some of the same tests we just did.

Note, an enhanced version of **traceroute** is supplied by **mtr**, which runs continuously (like **top**). Running it with the **--report-cycles** option to limit how long it runs:

**student:/tmp> sudo mtr --report-cycles 3 8.8.8.8**

**My traceroute [v0.85]**

**c7 (0.0.0.0) Mon Apr 20 09:30:41 2015**

**Unable to allocate IPv6 socket for nameserver communication: Address family not supported**

**by protocol Packets Pings**

**Host Loss% Snt Last Avg Best Wrst StDev**

**0.0% 3 0.3 0.3 0.2 0.3 0.0**

**2. 10.132.4.1 0.0% 3 6.3 7.1 6.3 8.4 0.7**

**3. dtr02ftbgwi-tge-0-6-0-3.ftbg.wi. 0.0% 3 6.2 7.5 6.2 10.0 2.1**

**4. dtr01ftbgwi-bue-1.ftbg.wi.charte 0.0% 3 8.9 8.5 6.2 10.4 2.0**

**5. crr01ftbgwi-bue-4.ftbg.wi.charte 0.0% 3 8.9 9.7 8.9 10.4 0.0**

**6. crr01euclwi-bue-1.eucl.wi.charte 0.0% 3 16.5 17.4 14.2 21.5 3.7**

**7. bbr01euclwi-bue-4.eucl.wi.charte 0.0% 3 23.5 22.0 18.2 24.2 3.2**

**8. bbr02euclwi-bue-5.eucl.wi.charte 0.0% 3 18.9 22.7 18.1 31.1 7.2**

**9. bbr01chcgil-bue-1.chcg.il.charte 0.0% 3 22.9 23.0 22.9 23.1 0.0**

**10. prr01chcgil-bue-2.chcg.il.charte 0.0% 3 21.4 24.1 20.8 30.2 5.2**

**11. 96-34-152-30.static.unas.mo.char 0.0% 3 22.6 21.9 20.0 23.3 1.6**

**12. 216.239.43.111 0.0% 3 21.2 21.7 21.2 22.0 0.0**

**13. 72.14.237.35 0.0% 3 21.2 21.0 19.8 21.9 1.0**

**14. google-public-dns-a.google.com 0.0% 3 26.7 23.0 21.0 26.7 3.2**

Hopefully, running through some of these commands helped. It actually helps to see what the correct output for your system looks like. Practice using these commands; it is very likely that you will need them someday.