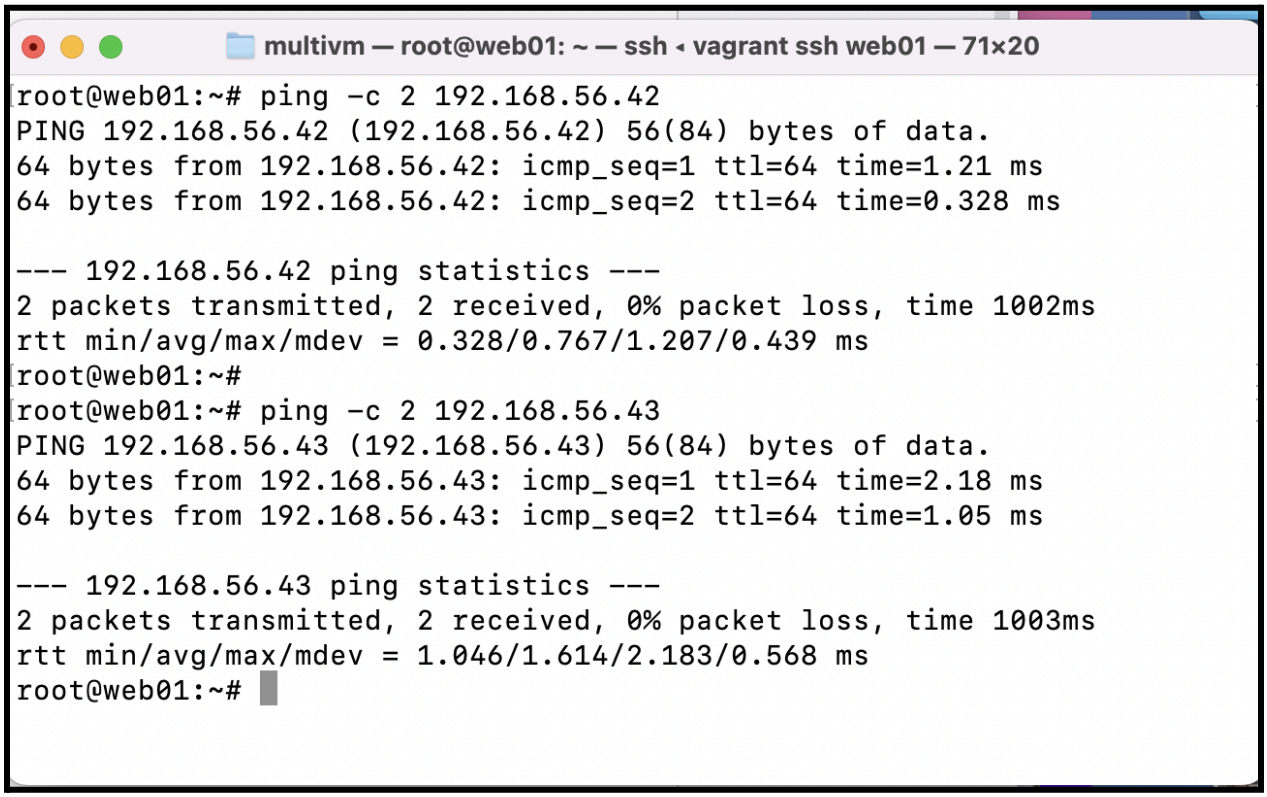
Networking Commands

aakansha@M2 multivm % pwd
/Users/aakansha/Desktop/vms/multivm
aakansha@M2 multivm % vagrant ssh web01

Ping Command

The `ping` command is used to test the connectivity between your computer and a remote device. It sends ICMP echo requests and measures how long it takes to receive a response, helping you check network status and diagnose connection issues.



root@web01:~# ping -c 4 web02
ping: web02: Temporary failure in name resolution
root@web01:~#

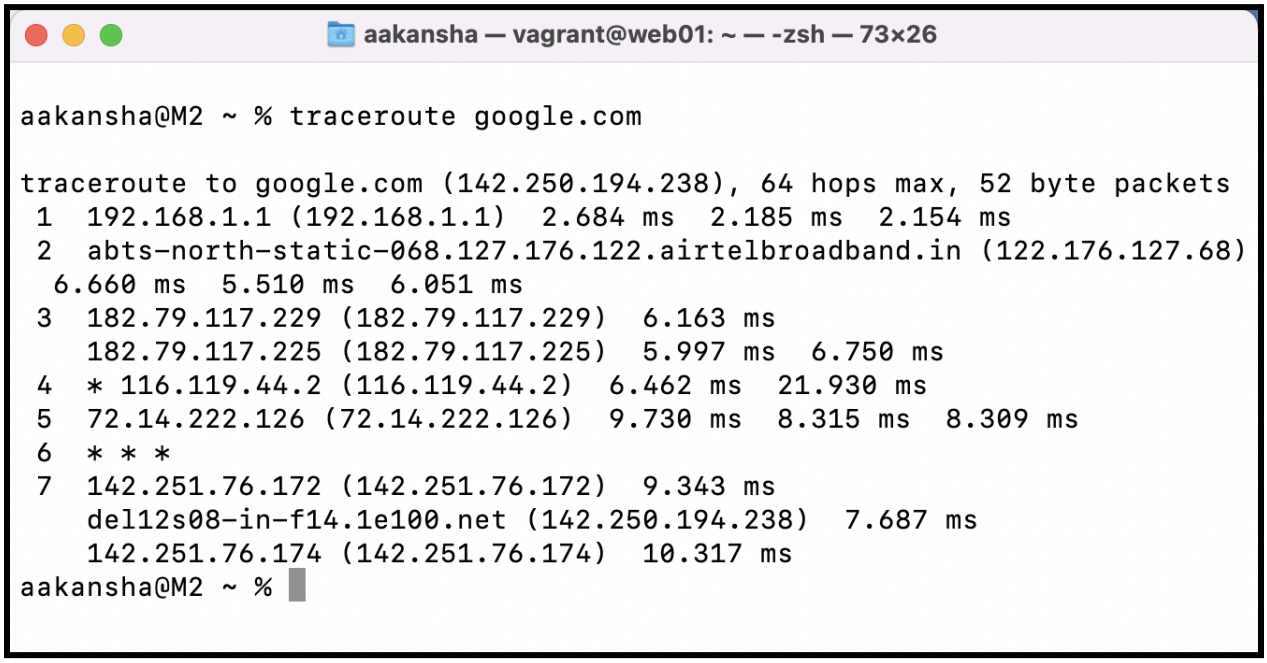
Resolve this by adding entry in the /etc/hosts file:
root@web01:~# vim /etc/hosts

multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 71×26

```
root@web01:~# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 vagrant

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.2.1 web01 web01

192.168.56.43 db01
192.168.56.42 web02

root@web01:~# ping -c 4 web02
PING web02 (192.168.56.42) 56(84) bytes of data.
64 bytes from web02 (192.168.56.42): icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from web02 (192.168.56.42): icmp_seq=2 ttl=64 time=0.833 ms
64 bytes from web02 (192.168.56.42): icmp_seq=3 ttl=64 time=0.915 ms
64 bytes from web02 (192.168.56.42): icmp_seq=4 ttl=64 time=0.866 ms

--- web02 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.833/0.953/1.201/0.145 ms
root@web01:~#
```

Traceroute(in Mac) / Tracert(in Windows)

`Traceroute` (in Mac) and `Tracert` (in Windows) are network diagnostic commands that trace the path data takes from your device to a target server. They display the sequence of routers and show the response times for each hop, helping to identify network bottlenecks or delays. This is useful for troubleshooting connectivity issues across different networks.



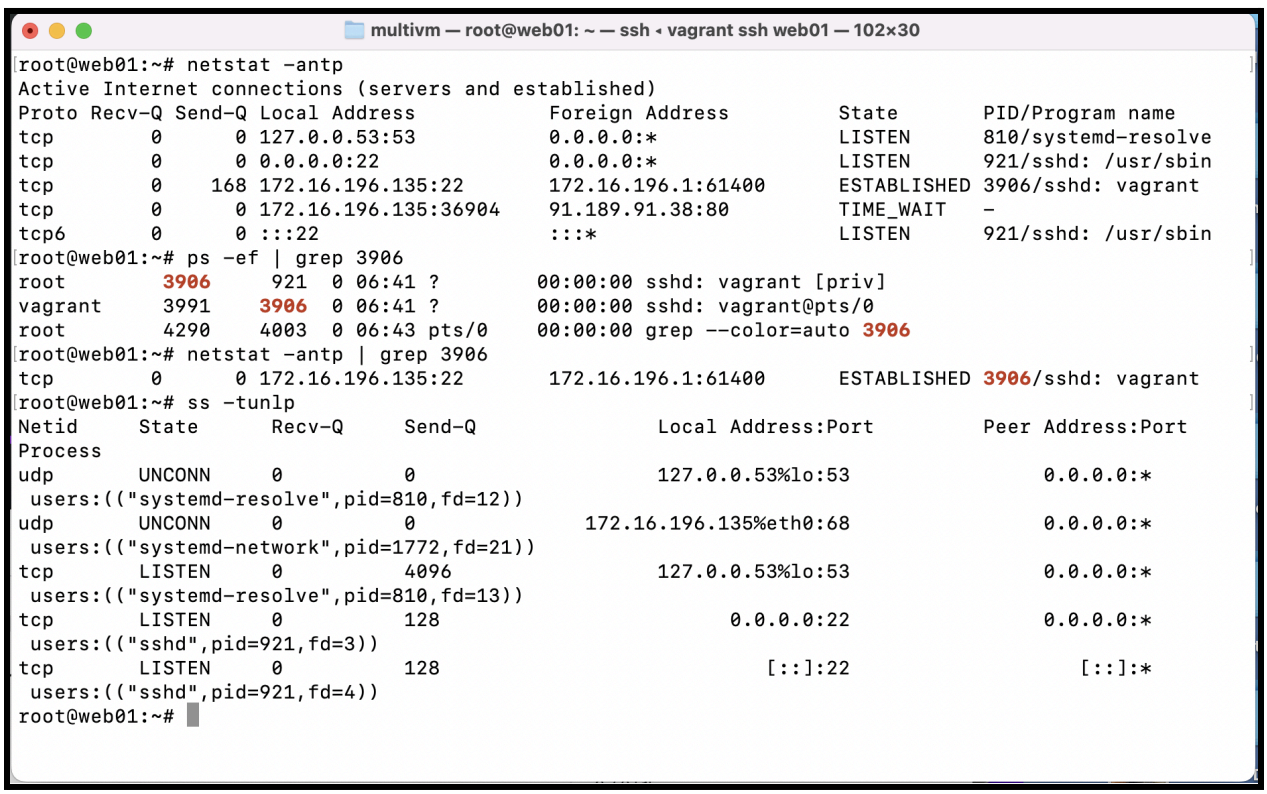
Netstat

The `netstat` command provides detailed information about network connections, routing tables, and interface statistics for network troubleshooting.

The `netstat -antp` command displays detailed network statistics, specifically:

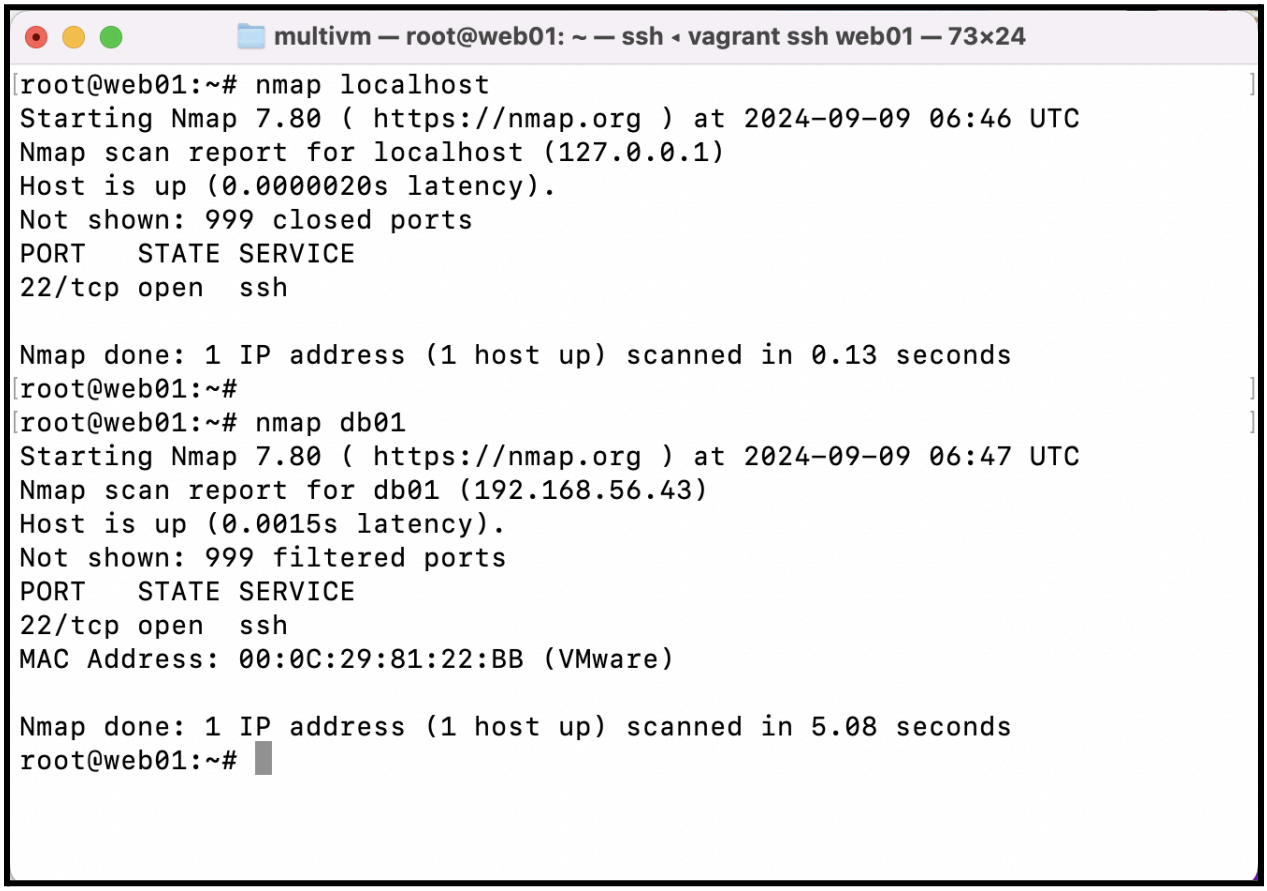
- **-a:** Shows all active connections and listening ports.
- **-n:** Displays addresses and port numbers in numerical form.
- **-t:** Focuses on TCP connections.
- **-p:** Shows the process ID (PID) and the program name associated with each connection.

This command is useful for monitoring active network connections and diagnosing network-related issues.



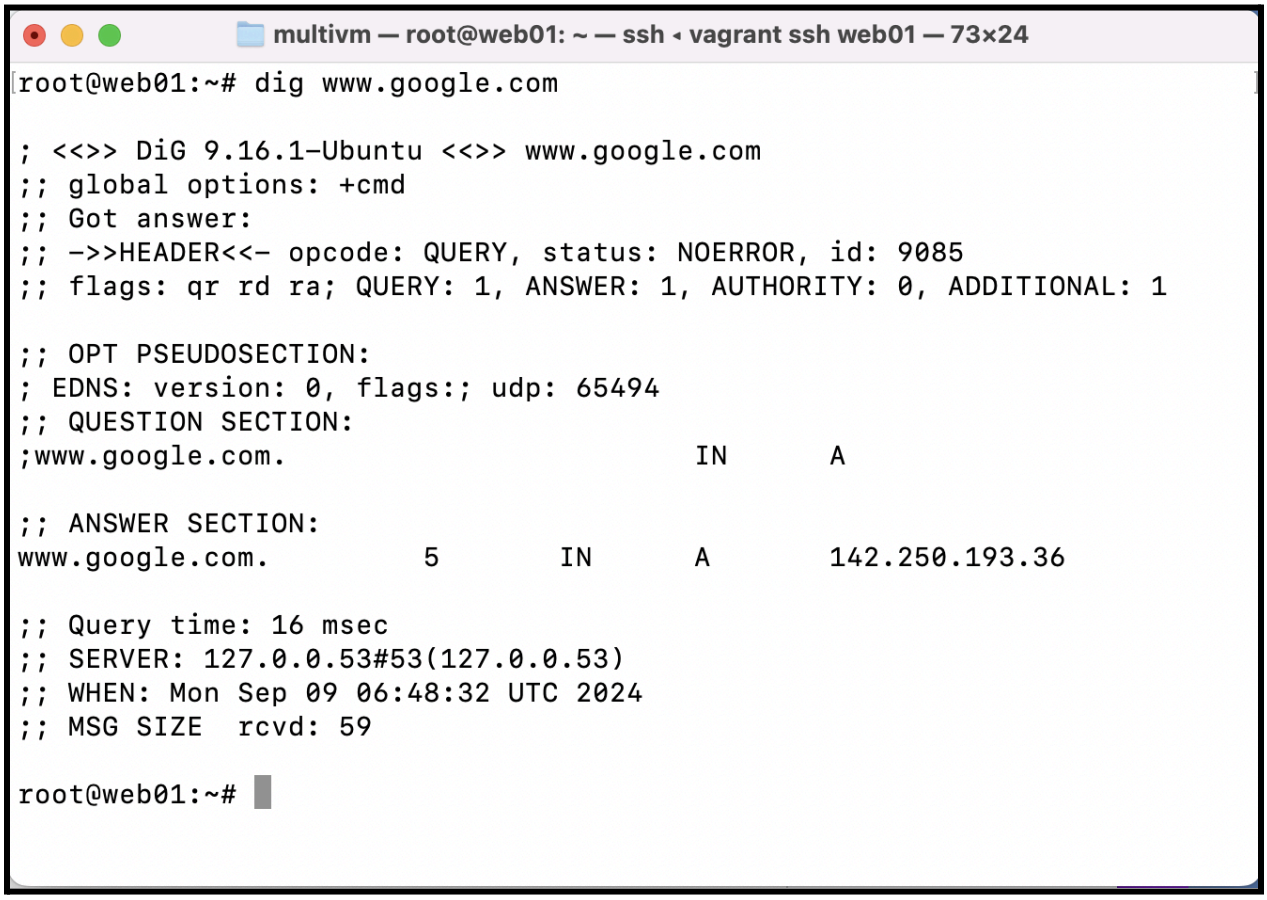
Nmap

Nmap (Network Mapper) is a powerful tool used for network discovery and security auditing, capable of scanning ports, detecting services, and identifying vulnerabilities on remote hosts.



Dig

The `dig` (Domain Information Groper) command is a DNS lookup tool used to query DNS servers for information about hostnames, IP addresses, and DNS records, helping troubleshoot DNS-related issues.



Nslookup

`nslookup` is a command-line tool used to query DNS servers for domain name or IP address information, helping troubleshoot DNS resolution issues.

```
multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 73×24
root@web01:~# nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.193.36
Name:   www.google.com
Address: 2404:6800:4002:81a::2004

root@web01:~#
```

Route

The `route` command displays or modifies the IP routing table, helping you manage the paths that network traffic takes when traveling through different networks. It's useful for configuring static routes and diagnosing network issues.

```
multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 84×24
root@web01:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.196.2    0.0.0.0         UG    100    0        0 eth0
172.16.196.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
172.16.196.2    0.0.0.0         255.255.255.255 UH    100    0        0 eth0
192.168.56.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
root@web01:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 eth0
172.16.196.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
_gateway        0.0.0.0         255.255.255.255 UH    100    0        0 eth0
192.168.56.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
root@web01:~#
```

Arp

The ARP command interfaces with the ARP cache maintained by the kernel. This cache stores mappings between IP addresses and MAC addresses, which the kernel uses to route packets to the correct hardware addresses on a local network.

```
multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 84×24
root@web01:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.196.1             ether   1e:57:dc:e7:97:65   C                     eth0
172.16.196.254           ether   00:50:56:e3:e3:5e   C                     eth0
_gateway                 ether   00:50:56:fc:ea:28   C                     eth0
web02                    ether   00:0c:29:69:d8:78   C                     eth1
db01                     ether   00:0c:29:81:22:bb   C                     eth1
root@web01:~#
```

Mtr

`mtr` (My Traceroute) is a network diagnostic tool that combines the functionality of `traceroute` and `ping` into one. It provides real-time data about the route packets take from your system to a destination and helps diagnose network issues.

```
multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 84×24
                              My traceroute  [v0.93]
web01 (172.16.196.135)                                  2024-09-09T06:57:59+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets               Pings
 Host                                   Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway                             0.0%    43    0.7   0.7   0.3   1.2   0.2
 2. 192.168.1.1                          0.0%    43    7.5   5.0   3.4  11.7   1.8
 3. abts-north-static-068.127.176.122.ai 0.0%    43    6.6  11.9   4.9  63.6  12.7
 4. 182.79.117.225                       0.0%    43    6.8   9.3   4.7  32.7   5.5
 5. 116.119.44.2                         0.0%    42    5.2   9.0   5.2  26.1   4.7
 6. 72.14.222.126                        0.0%    42    9.1   9.0   7.4  11.7   0.9
 7. 142.251.66.177                       0.0%    42    8.3   8.1   6.4  19.3   2.2
 8. 172.253.67.95                        0.0%    42    9.5   8.9   7.5  11.6   0.7
 9. kix05s07-in-f4.1e100.net             0.0%    42    8.5   8.1   7.0   9.8   0.6
```

Telnet

`telnet` is a network protocol and command-line tool used for connecting to remote systems over a network. It allows users to establish a text-based connection to another computer, typically to access services or troubleshoot network issues.

```
multivm — root@web01: ~ — ssh ◂ vagrant ssh web01 — 65×24
root@web01:~# nmap db01
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-09 07:00 UTC
Nmap scan report for db01 (192.168.56.43)
Host is up (0.0011s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:81:22:BB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
root@web01:~# telnet 192.168.56.43 22
Trying 192.168.56.43...
Connected to 192.168.56.43.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.7

Invalid SSH identification string.
Connection closed by foreign host.
root@web01:~#
```

😀...HAPPY LEARNING...😀