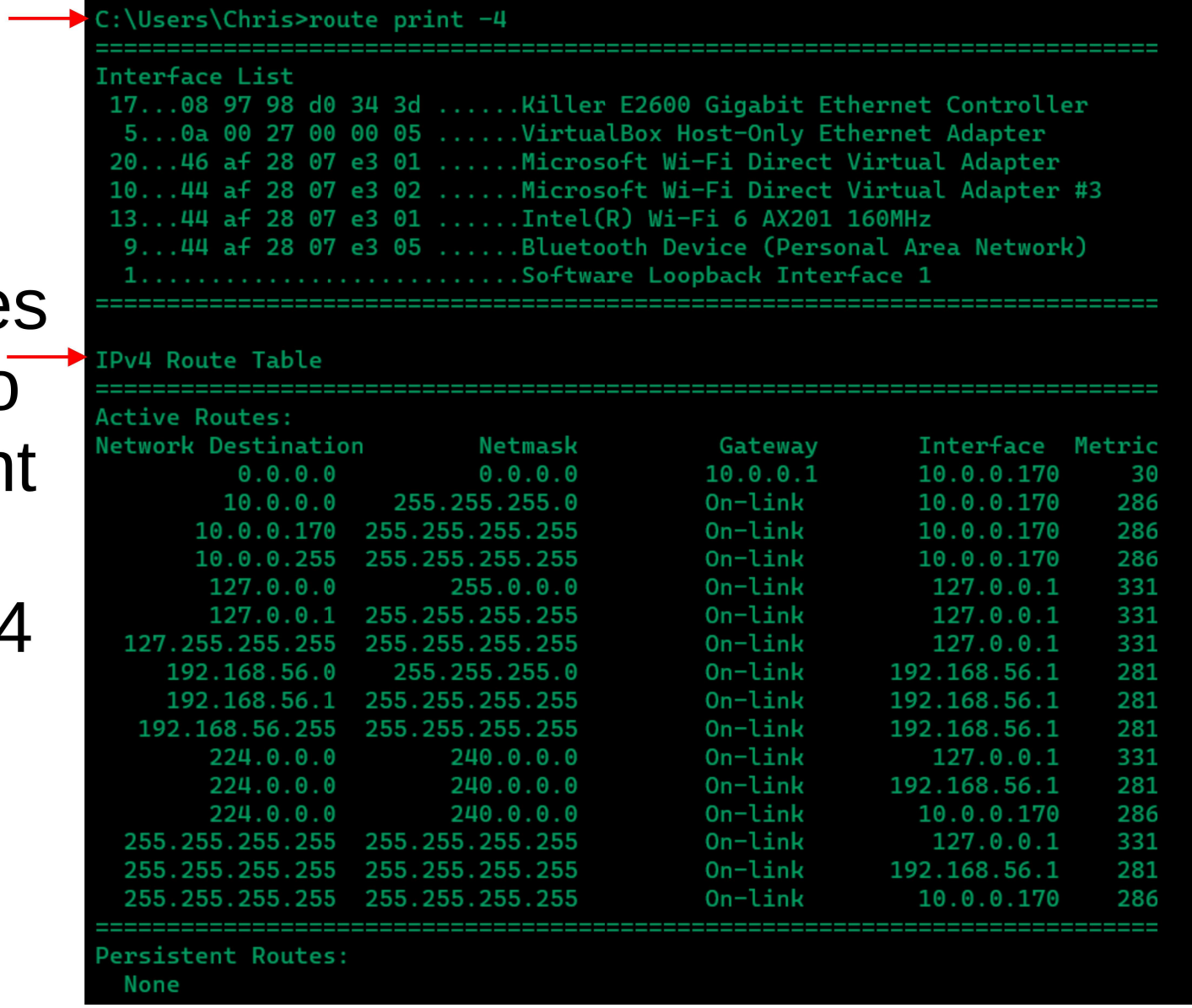
Understanding your network gateway and routing details

Let’s start with the “route” command and lets learn a bit more, so we will input “Route /?”

Notice it states this is to manipulate the network routing table. However, we are going to use this to only view and not make any modifications

```
C:\Users\Chris>route /?

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f            Clears the routing tables of all gateway entries.  If this is
                used in conjunction with one of the commands, the tables are
                cleared prior to running the command.

  -p            When used with the ADD command, makes a route persistent across
                boots of the system. By default, routes are not preserved
                when the system is restarted. Ignored for all other commands,
                which always affect the appropriate persistent routes.

  -4            Force using IPv4.

  -6            Force using IPv6.

  command       One of these:
                  PRINT     Prints  a route
                  ADD       Adds    a route
                  DELETE    Deletes a route
                  CHANGE    Modifies an existing route
  destination   Specifies the host.
  MASK          Specifies that the next parameter is the 'netmask' value.
  netmask       Specifies a subnet mask value for this route entry.
                If not specified, it defaults to 255.255.255.255.
  gateway       Specifies gateway.
  interface     the interface number for the specified route.
  METRIC        specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
```

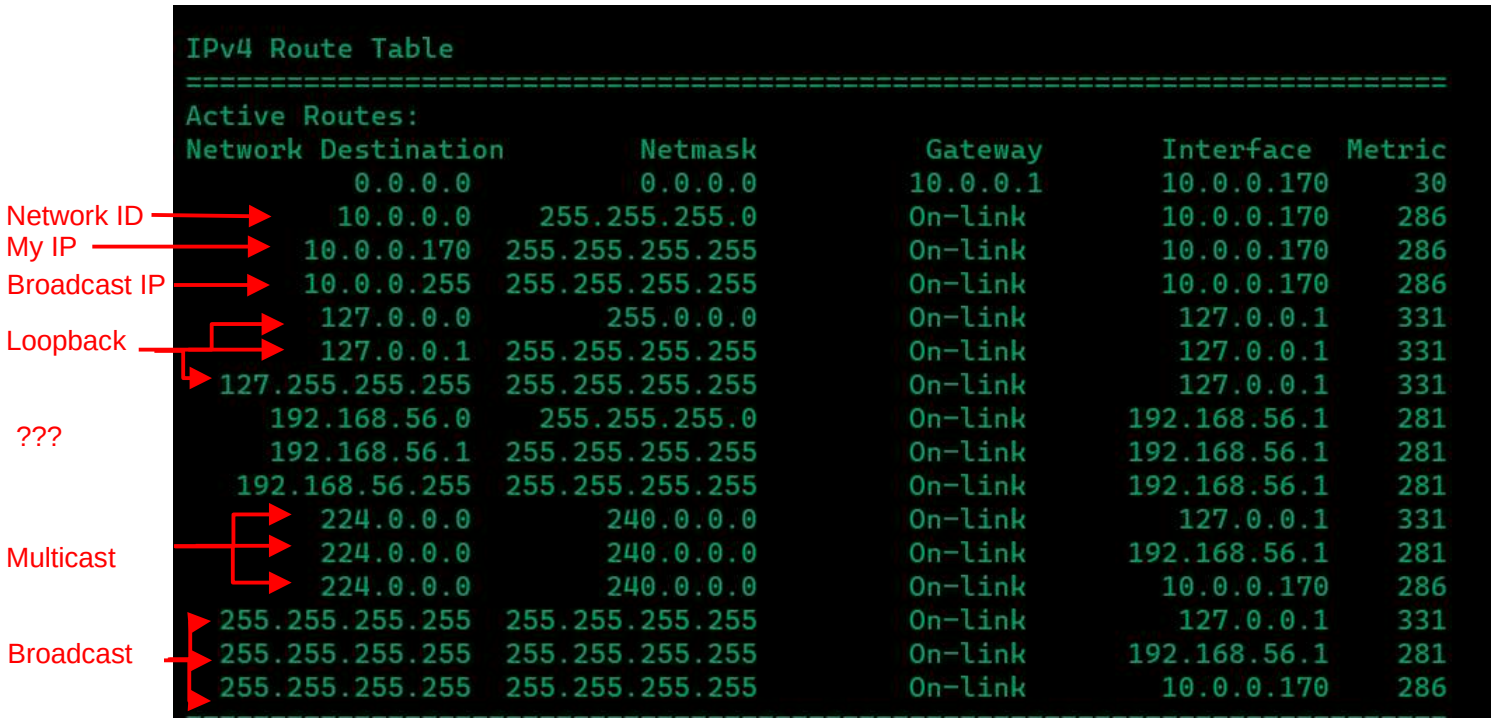
For our purposes we are going to input “route print -4” Which will give us our IPv4 Routing table.



We see our network is 10.0.0.0 with a /24 CIDR

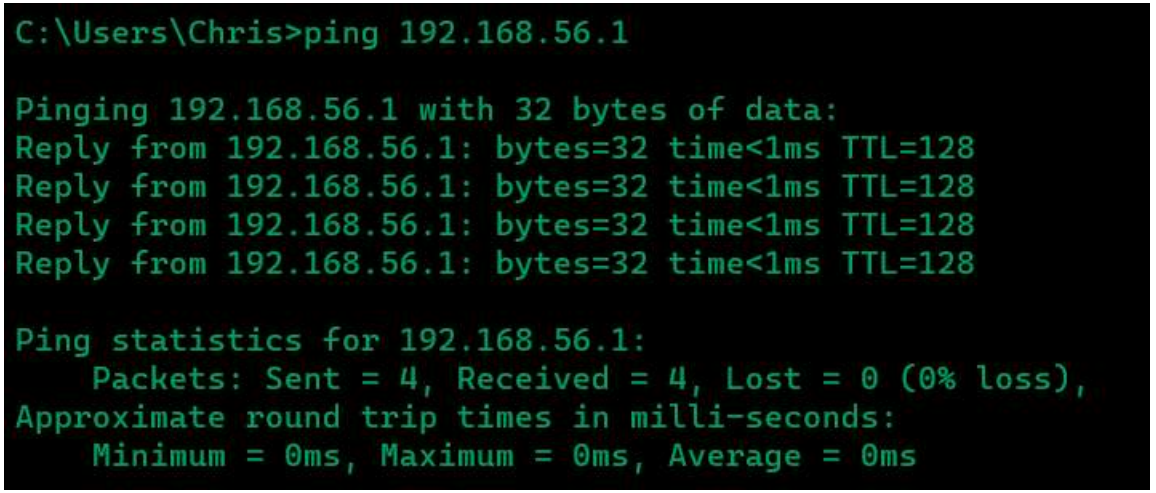
However, I did also notice I had another network that looks to be 192.168.56.0/24

Lets investigate using basic tools




```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.0.1      10.0.0.170     30
         10.0.0.0    255.255.255.0       On-link       10.0.0.170    286
       10.0.0.170  255.255.255.255       On-link       10.0.0.170    286
       10.0.0.255  255.255.255.255       On-link       10.0.0.170    286
        127.0.0.0        255.0.0.0       On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255       On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255       On-link        127.0.0.1    331
      192.168.56.0    255.255.255.0       On-link      192.168.56.1    281
      192.168.56.1  255.255.255.255       On-link      192.168.56.1    281
    192.168.56.255  255.255.255.255       On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0       On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0       On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0       On-link       10.0.0.170    286
  255.255.255.255  255.255.255.255       On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255       On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255       On-link       10.0.0.170    286
```

Out of curiosity I decided to ping the IP. I noticed the TTL=128 which tells us the packets sent but didn’t really go anywhere.



I next went with trace route and it says its me. I then checked my actual IP (10.0.0.170) and that was also me. There was a slight difference but I didn’t fully understand.

I then went with the ipconfig /all and then the aha moment.