

Understanding your network gateway and routing details

→ C:\Users\Chris>route /?

→ Manipulates network routing tables.

Let's start with the "route" command and let's 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

```
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.

```
C:\Users\Chris>route print -4
=====
Interface List
17...08 97 98 d0 34 3d .....Killer E2600 Gigabit Ethernet Controller
 5...0a 00 27 00 00 05 .....VirtualBox Host-Only Ethernet Adapter
20...46 af 28 07 e3 01 .....Microsoft Wi-Fi Direct Virtual Adapter
10...44 af 28 07 e3 02 .....Microsoft Wi-Fi Direct Virtual Adapter #3
13...44 af 28 07 e3 01 .....Intel(R) Wi-Fi 6 AX201 160MHz
 9...44 af 28 07 e3 05 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

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
=====
Persistent Routes:
None
```

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

Network ID →

My IP →

Broadcast IP →

Loopback →

???

Multicast →

Broadcast →

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.

```
C:\Users\Chris>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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.

```
C:\Users\Chris>tracert 192.168.56.1
```

```
Tracing route to LAPTOP-5R59DKHF [192.168.56.1]  
over a maximum of 30 hops:
```

```
  1    <1 ms    <1 ms    <1 ms  LAPTOP-5R59DKHF [192.168.56.1]
```

```
Trace complete.
```

```
C:\Users\Chris>tracert 10.0.0.170
```

```
Tracing route to LAPTOP-5R59DKHF.hsd1.co.comcast.net [10.0.0.170]  
over a maximum of 30 hops:
```

```
  1    <1 ms    <1 ms    <1 ms  LAPTOP-5R59DKHF.hsd1.co.comcast.net [10.0.0.170]
```

```
Trace complete.
```


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

```
C:\Users\Chris>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : LAPTOP-5R59DKHF
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hsd1.co.comcast.net
```

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : hsd1.co.comcast.net
Description . . . . . : Killer E2600 Gigabit Ethernet Controller
Physical Address. . . . . : 08-97-98-D0-34-3D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . :
Description . . . . . → VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-05
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::711d:51aa:d0e8:57dc%5(Preferred)
IPv4 Address. . . . . → 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 705298471
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-54-6A-1E-08-97-98-D0-34-3D
NetBIOS over Tcpip. . . . . : Enabled
```