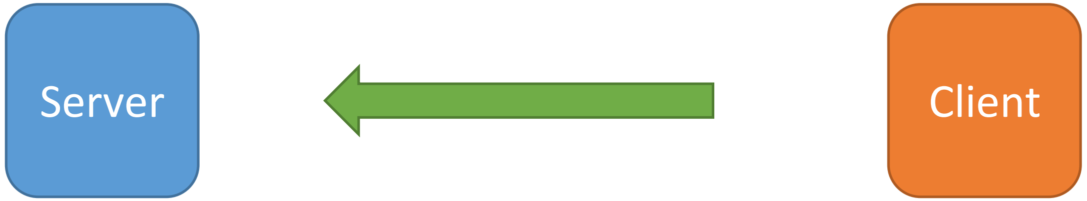
Intro to networking

Core essentials of networking

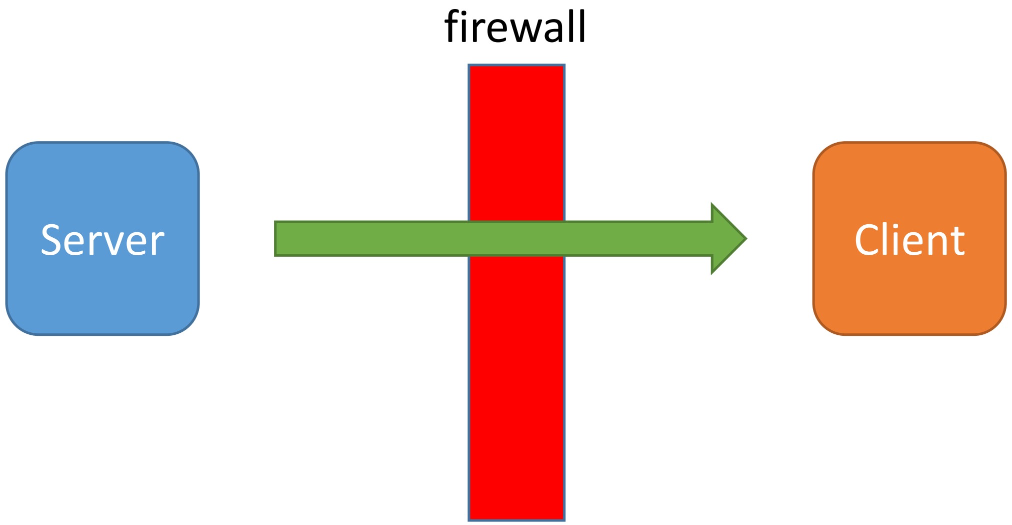
Simple network program

- Consists of 2 parts:
- A server and a client
- The server program must be started first and waits, or, listens for the client program to connect



Reverse Connection RATs

- It is also possible to have the server connect to the client as in the case of Reverse-Connection-RATs
- Reverse RATs are used to bypass firewall or router limitations



Location of Server and Client

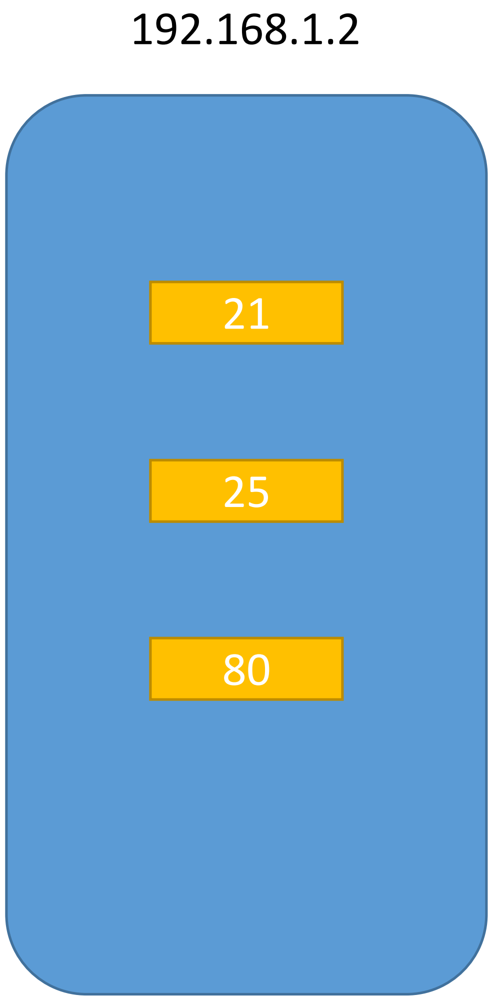
- Usually the server program resides on one computer whilst the client resides on another
- Both can be on the same Local Area Network (LAN), or ,on the Internet
- Also, both can also reside on the same computer, for testing purposes

Remotely executing commands

- After server and client has established a connection, client will send a command to the server.
- Upon receiving the command, the server will execute it.
- Example commands: display message ‘Hello world’, beep, shutdown, reboot, activate hardware, create files, delete files, run programs, etc…
- Any commands that could ordinarily be executed by a user sitting in front of a computer.

IP Addresses vs Port Numbers

- IP (Internet Protocol) Address is the address of the house
- Port numbers are the people who live in the house
- IP address is the address of the computer
- Port numbers are the server processes running in the computer
- There can be more than one server process running on a single computer.
- Therefore, for each IP address, the can be more than 1 port number.



Local Area Network (LAN) vs Internet

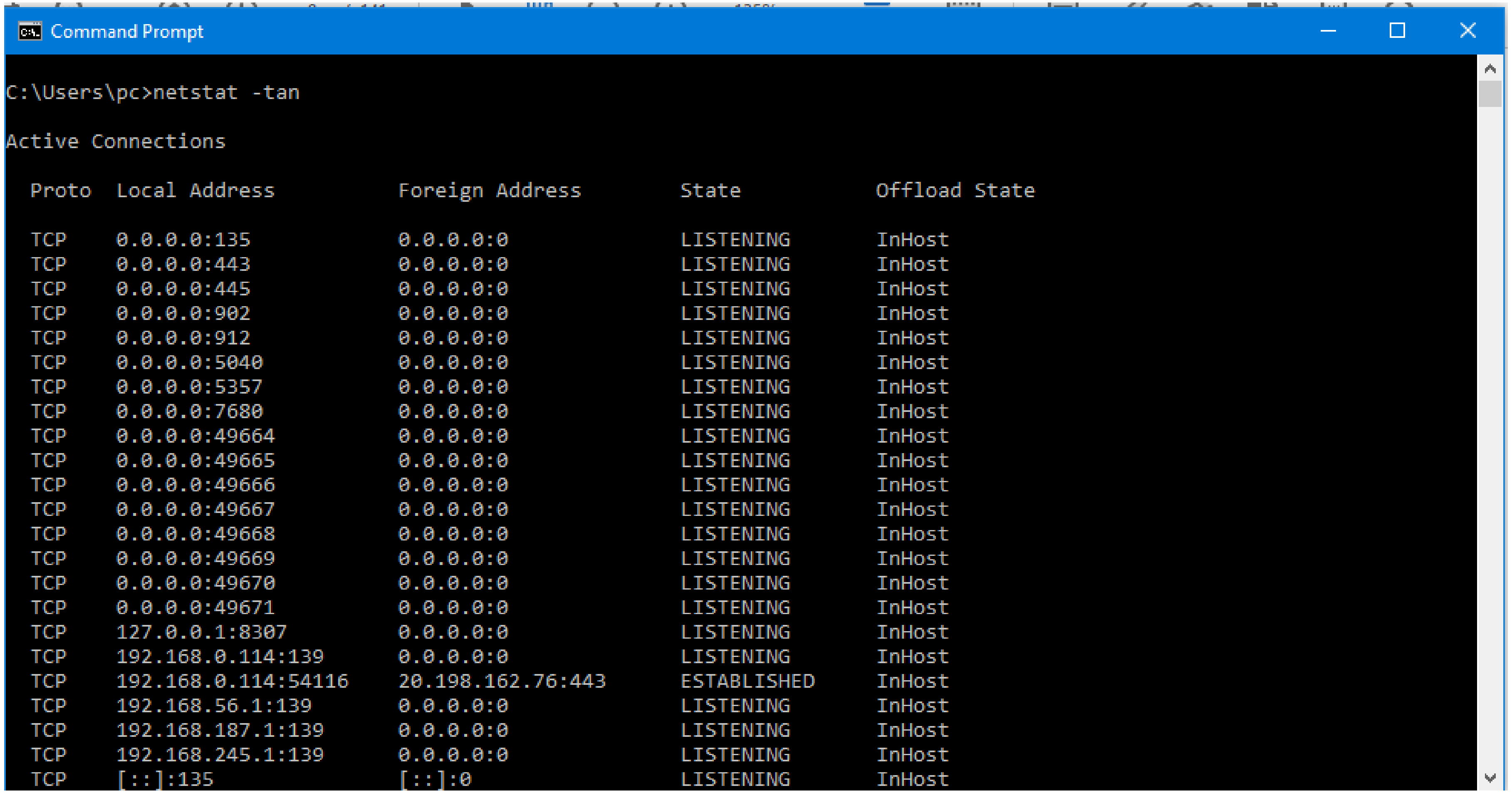
- IP addresses eg, 192.168.x.1 to 192.168.x.254 are reserved for LAN use. The x refers to numbers from 1 to 255.
- 127.0.0.1 is also known as the loopback address. It refers to the local computer.
- For the Internet, the IP addresses are assigned by your Internet Service Provider (ISP) when a user connects to the Internet with a modem
- Therefore a computer can have multiple IP addresses

Port numbers aka sockets

- Range from 1 to 65536
- But, 1 to 1024 are reserved for special use, eg, 21 is FTP, 23 is telnet server, 25 is SMTP, 80 is HTTP (Web Server)
- Any number above 1024, we can use for writing network programs.

Checking IP and port numbers

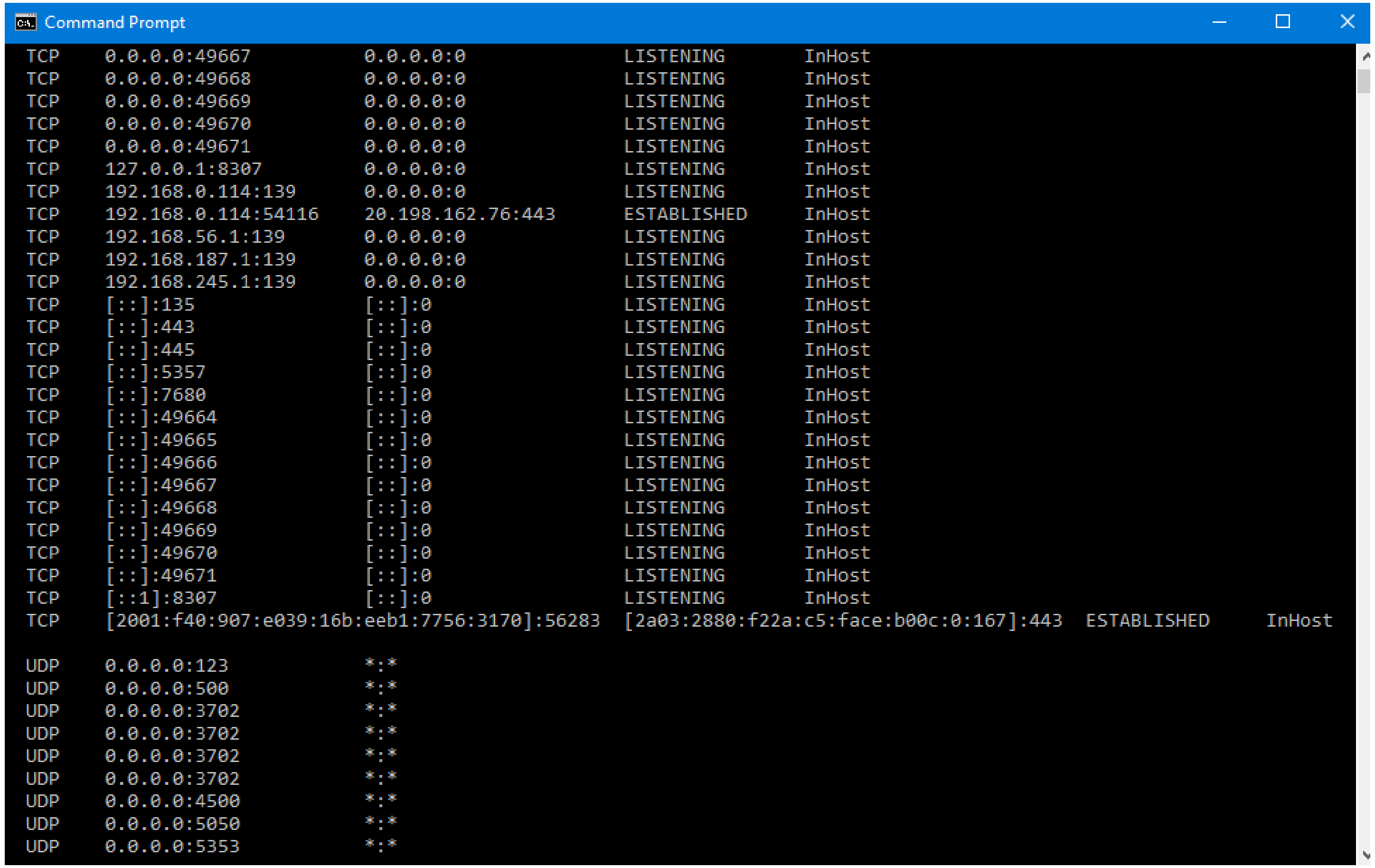
- To see the IP addresses and port numbers, open a cmd prompt, and issue the following command:
- C:\netstat –tan
- You should see something like this:



```
C:\Users\pc>netstat -tan

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
```

TCP vs UDP

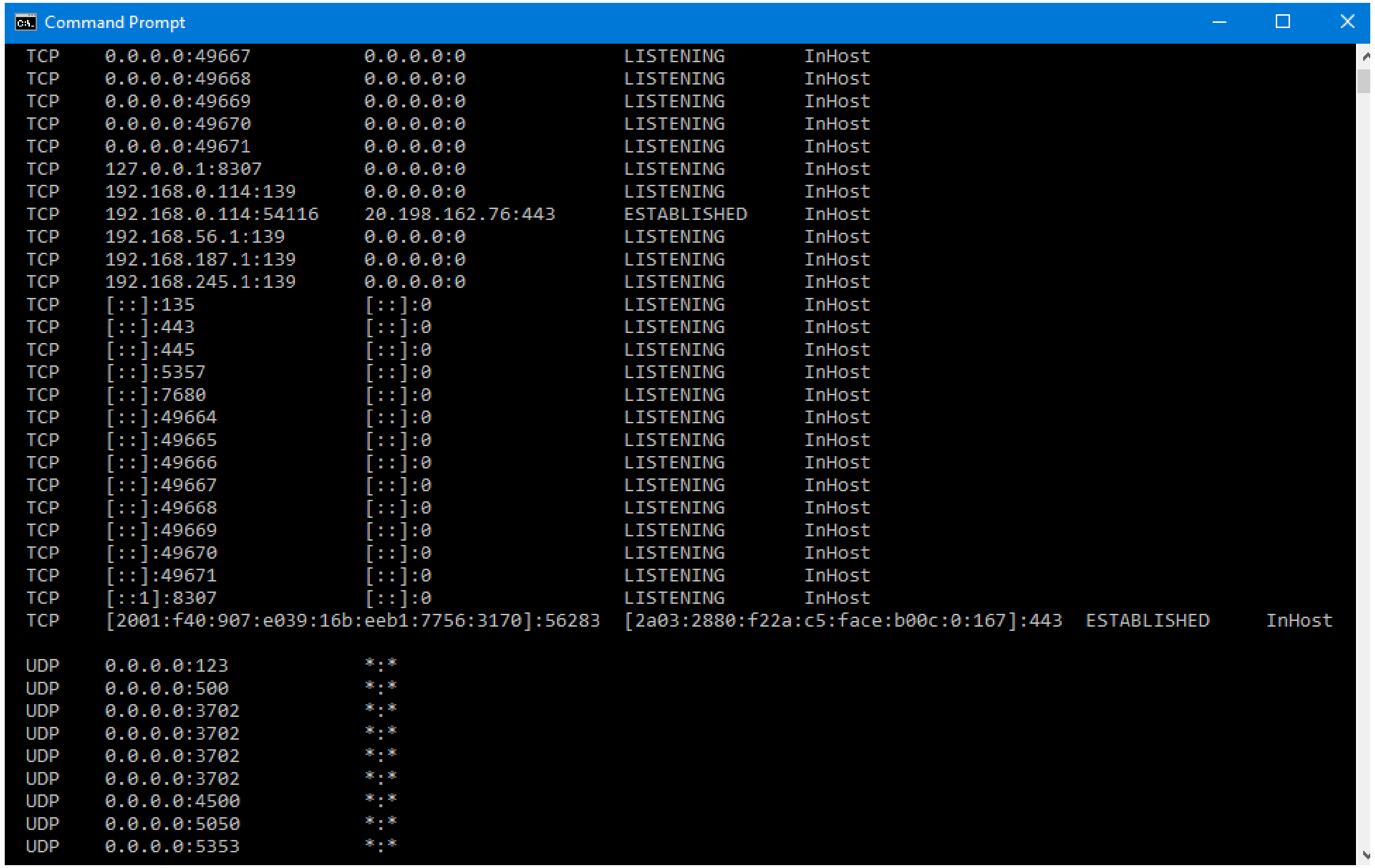
- TCP (Transmission Control Protocol) is a protocol used to establish connections with other computer on the Internet
- When a client wants to talk to the server, it will follow the protocol of TCP to try to establish a connection first.
- If a connection is established successfully, then the client and server can talk



```
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:5357              [::]:0                 LISTENING       InHost
  TCP    [::]:7680              [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49667             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49669             [::]:0                 LISTENING       InHost
  TCP    [::]:49670             [::]:0                 LISTENING       InHost
  TCP    [::]:49671             [::]:0                 LISTENING       InHost
  TCP    [::1]:8307             [::]:0                 LISTENING       InHost
  TCP    [2001:f40:907:e039:16b:eeb1:7756:3170]:56283  [2a03:2880:f22a:c5:face:b00c:0:167]:443  ESTABLISHED     InHost

  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
```

TCP vs UDP (2)

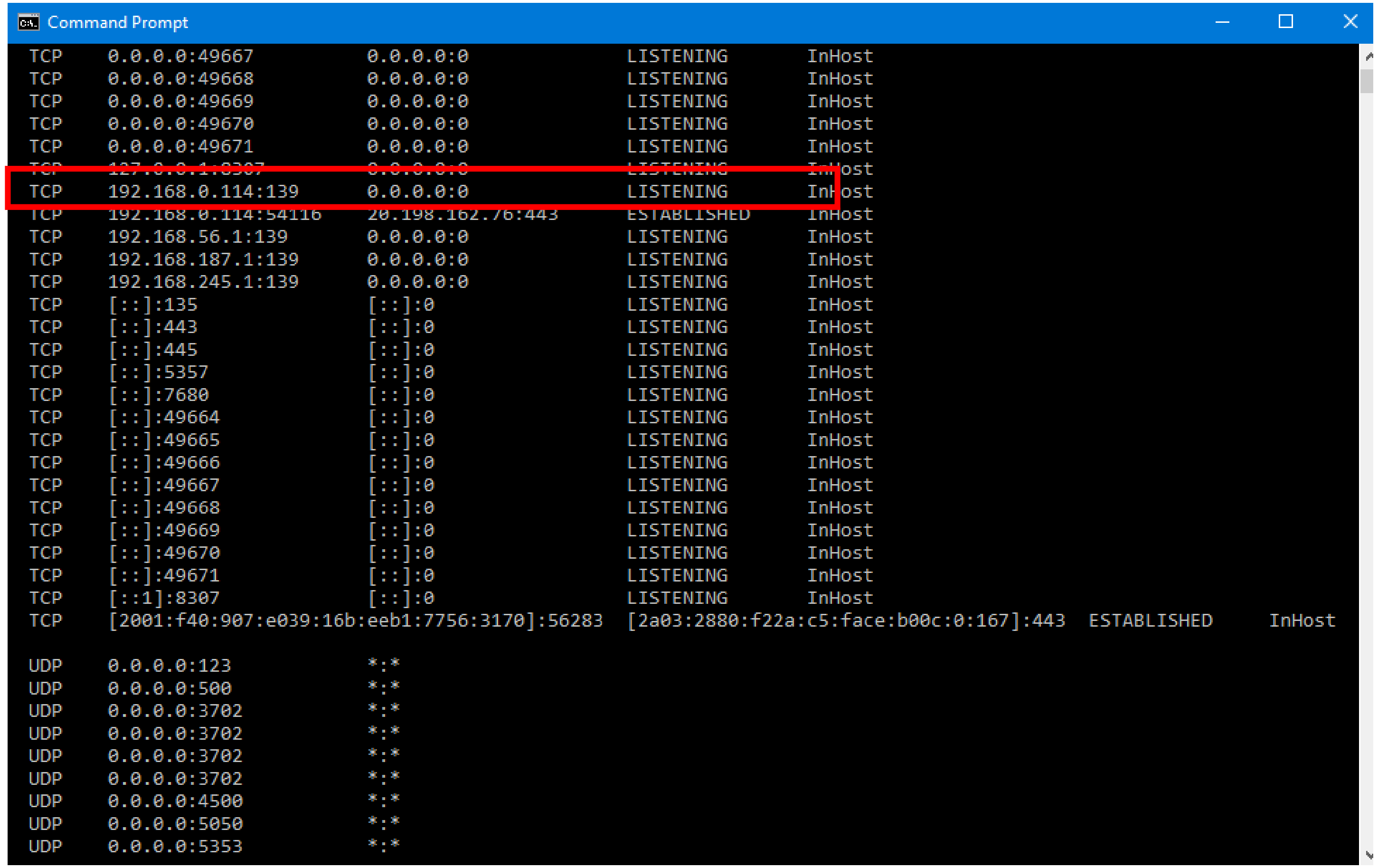
- UDP (User Datagram Protocol) is another protocol used for communication on the Internet.
- But unlike TCP, the client need not establish a connection with the server. The client just sends the message.
- If the server was not listening, then the message is lost



```
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:5357              [::]:0                 LISTENING       InHost
  TCP    [::]:7680              [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49667             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49669             [::]:0                 LISTENING       InHost
  TCP    [::]:49670             [::]:0                 LISTENING       InHost
  TCP    [::]:49671             [::]:0                 LISTENING       InHost
  TCP    [::1]:8307             [::]:0                 LISTENING       InHost
  TCP    [2001:f40:907:e039:16b:eeb1:7756:3170]:56283  [2a03:2880:f22a:c5:face:b00c:0:167]:443  ESTABLISHED     InHost

  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
```

TCP/IP Protocol

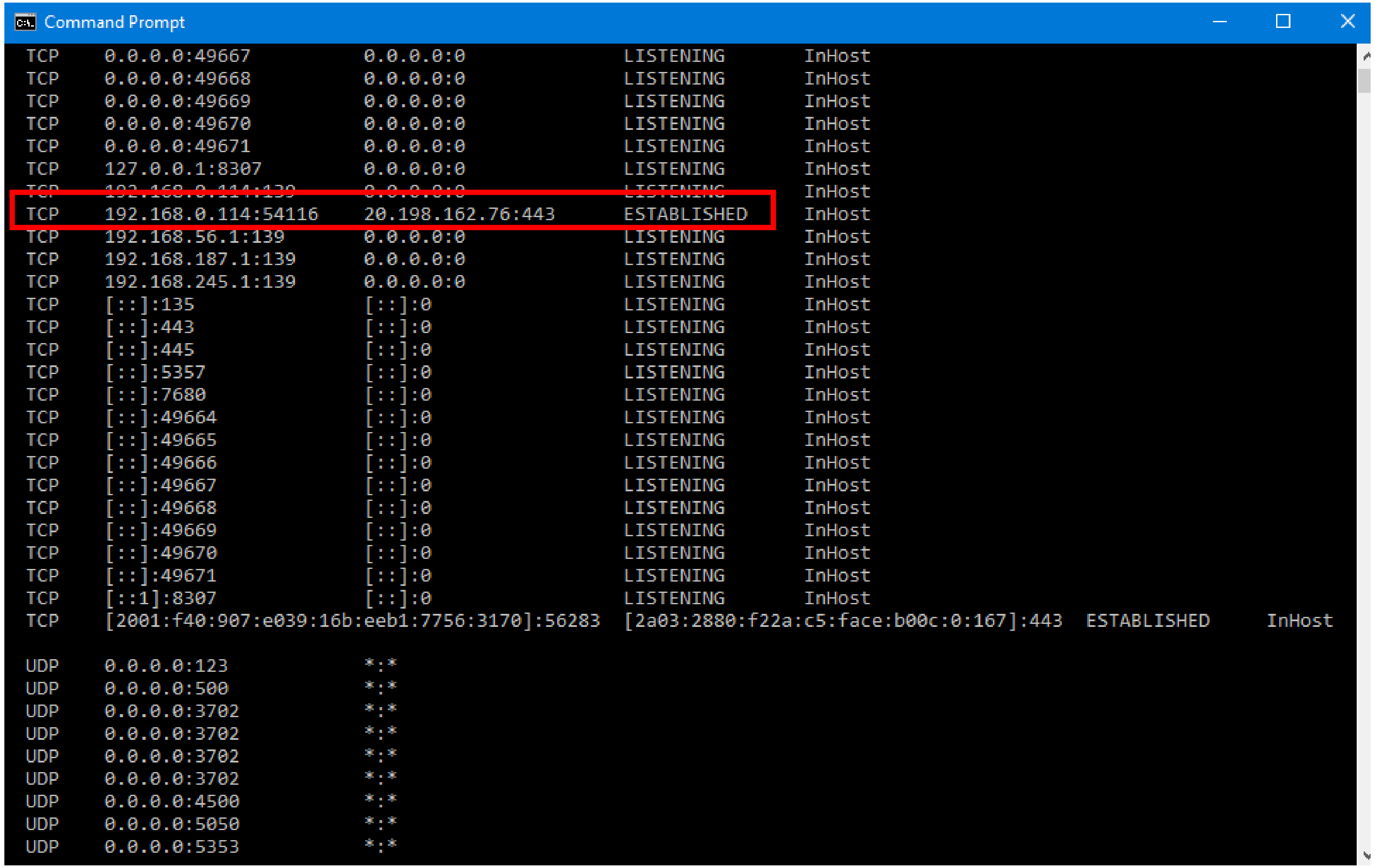
- Both TCP and UDP belongs to the TCP/IP protocol.
- Note that the IP address is followed by the Port number and separated by a colon (:)
- 192.168.0.114:139
- In the above case, 192.168.0.114 is the IP address and port 139 is the NetBios port – used for windows networking



```
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:5357              [::]:0                 LISTENING       InHost
  TCP    [::]:7680              [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49667             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49669             [::]:0                 LISTENING       InHost
  TCP    [::]:49670             [::]:0                 LISTENING       InHost
  TCP    [::]:49671             [::]:0                 LISTENING       InHost
  TCP    [::1]:8307             [::]:0                 LISTENING       InHost
  TCP    [2001:f40:907:e039:16b:eeb1:7756:3170]:56283  [2a03:2880:f22a:c5:face:b00c:0:167]:443  ESTABLISHED     InHost

  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
```

The need for client port numbers

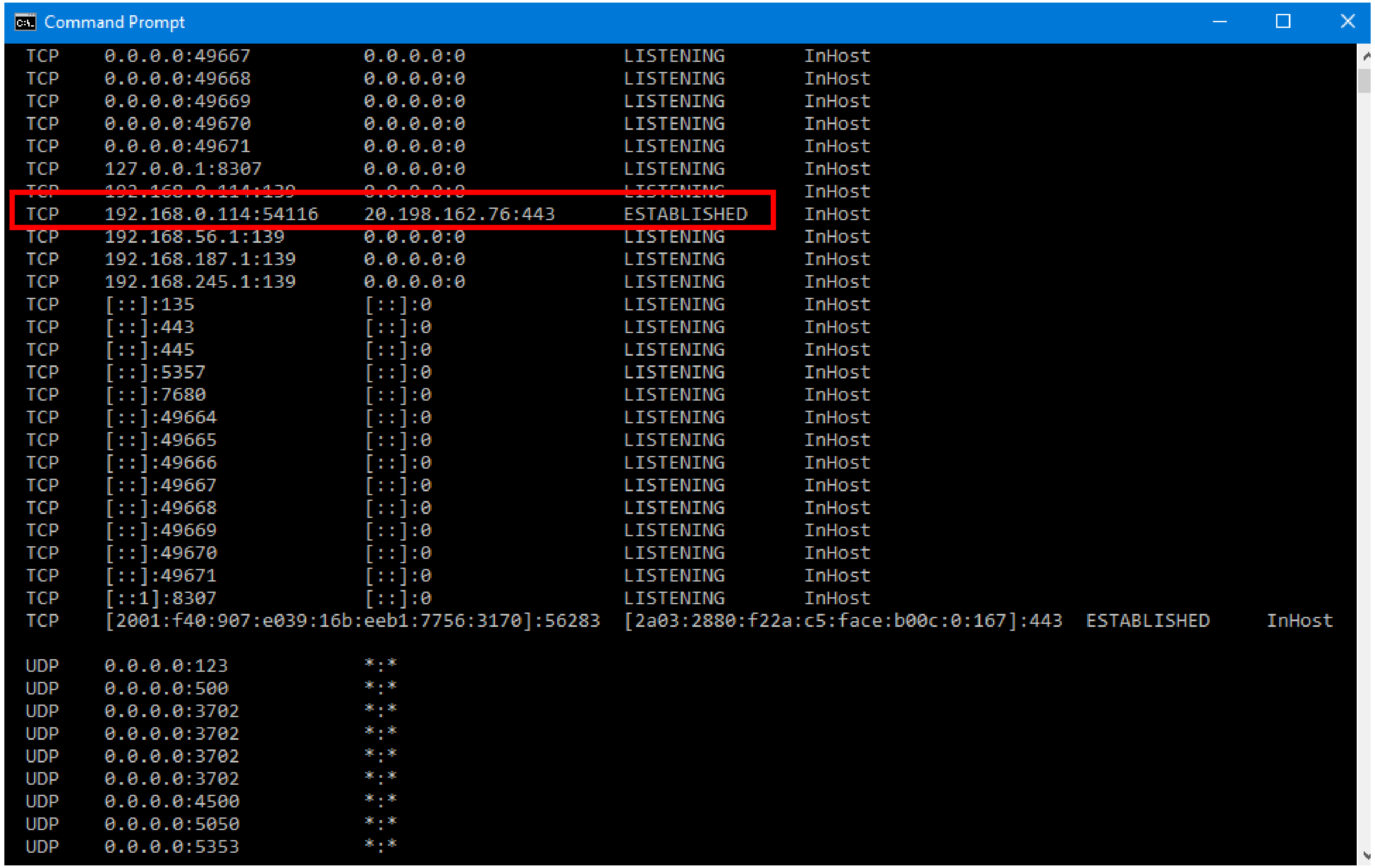
- Note that clients also need port numbers and IP addresses.
- Consider the connection outlined in red below:



```
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:5357              [::]:0                 LISTENING       InHost
  TCP    [::]:7680              [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49667             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49669             [::]:0                 LISTENING       InHost
  TCP    [::]:49670             [::]:0                 LISTENING       InHost
  TCP    [::]:49671             [::]:0                 LISTENING       InHost
  TCP    [::1]:8307             [::]:0                 LISTENING       InHost
  TCP    [2001:f40:907:e039:16b:eeb1:7756:3170]:56283  [2a03:2880:f22a:c5:face:b00c:0:167]:443  ESTABLISHED     InHost

  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
```

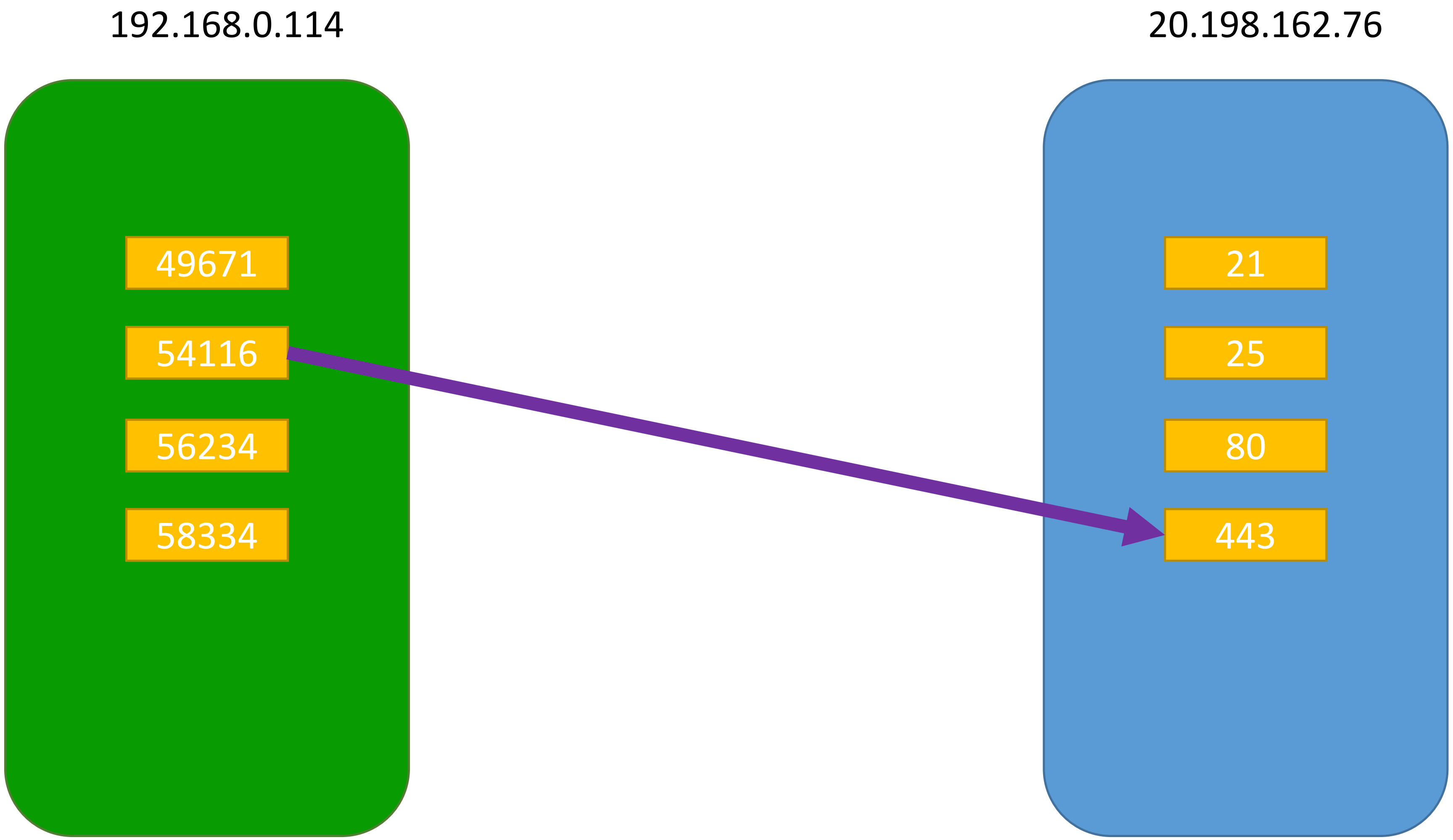
The need for client port numbers

- The local computer with IP address 192.168.0.114 is using port 54116 to connect to port 443 at the remote IP address 20.198.162.76



```
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.0.114:54116    20.198.162.76:443      ESTABLISHED     InHost
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       InHost
  TCP    192.168.187.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:5357              [::]:0                 LISTENING       InHost
  TCP    [::]:7680              [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49667             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49669             [::]:0                 LISTENING       InHost
  TCP    [::]:49670             [::]:0                 LISTENING       InHost
  TCP    [::]:49671             [::]:0                 LISTENING       InHost
  TCP    [::1]:8307             [::]:0                 LISTENING       InHost
  TCP    [2001:f40:907:e039:16b:eeb1:7756:3170]:56283  [2a03:2880:f22a:c5:face:b00c:0:167]:443  ESTABLISHED     InHost

  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
```

IP Addresses vs Port Numbers



Thank you