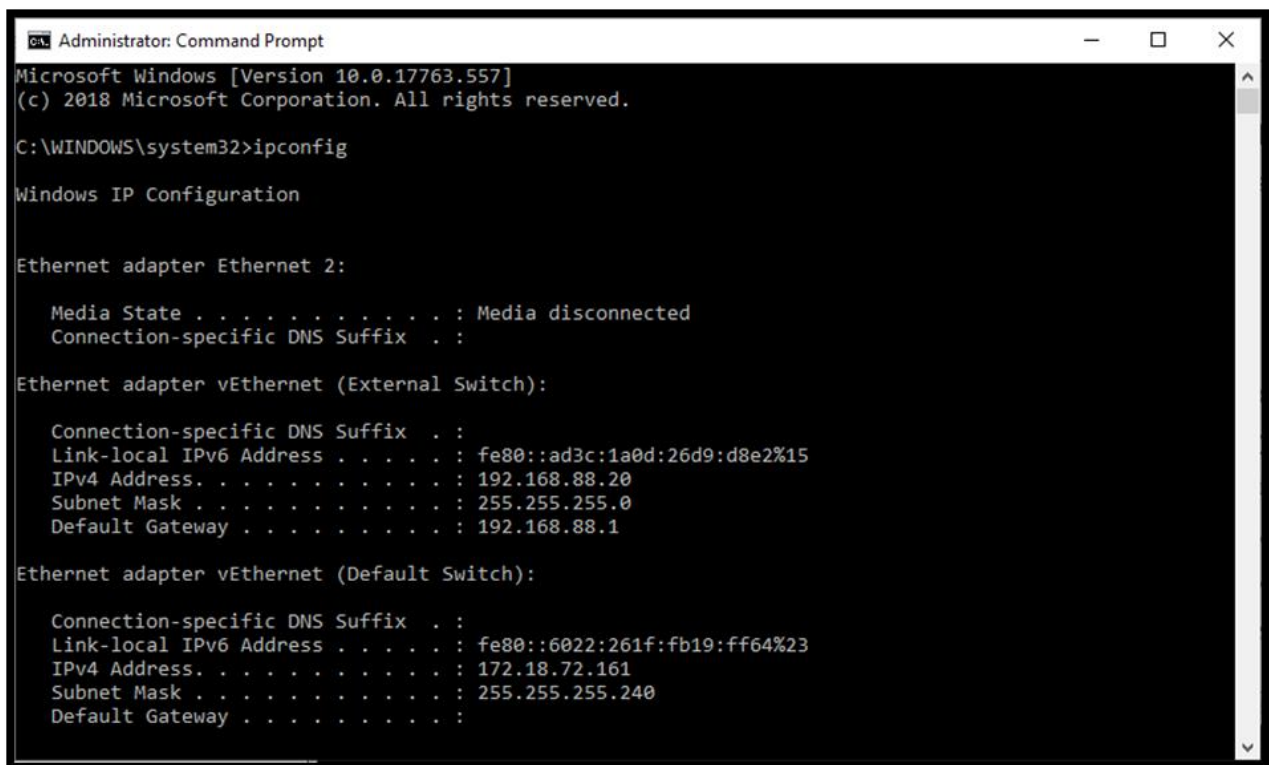


## 1.4 Basic Network Utilities

Now that you know what IP addresses and URLs are, you need to become familiar with some basic network utilities. Certain network utilities can be executed from a command prompt (Windows) or from a shell (Unix/Linux). Many people are already familiar with Windows, so let's focus on how to execute the commands from the Windows command-prompt perspective. However, these utilities are available in all operating systems.

### 1.4.1 Ipconfig

The first thing you should do is to get information about your own system. To accomplish this, you must get a command prompt. In Windows, you can do this by going to the Start menu, selecting All Programs, and then choosing Accessories. You can also go to Start, Run, and type cmd to get a command prompt. In Windows 10 you must go to Search and type cmd. Now, you should be able to type in ipconfig. (You could input the same command in UNIX or Linux by typing in ifconfig from the shell.) After typing in ipconfig (ifconfig in Linux), you should be able to see something similar to the screenshot below.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of the 'ipconfig' command. The output is as follows:

```
Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (External Switch):

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ad3c:1a0d:26d9:d8e2%15
    IPv4 Address. . . . . : 192.168.88.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.88.1

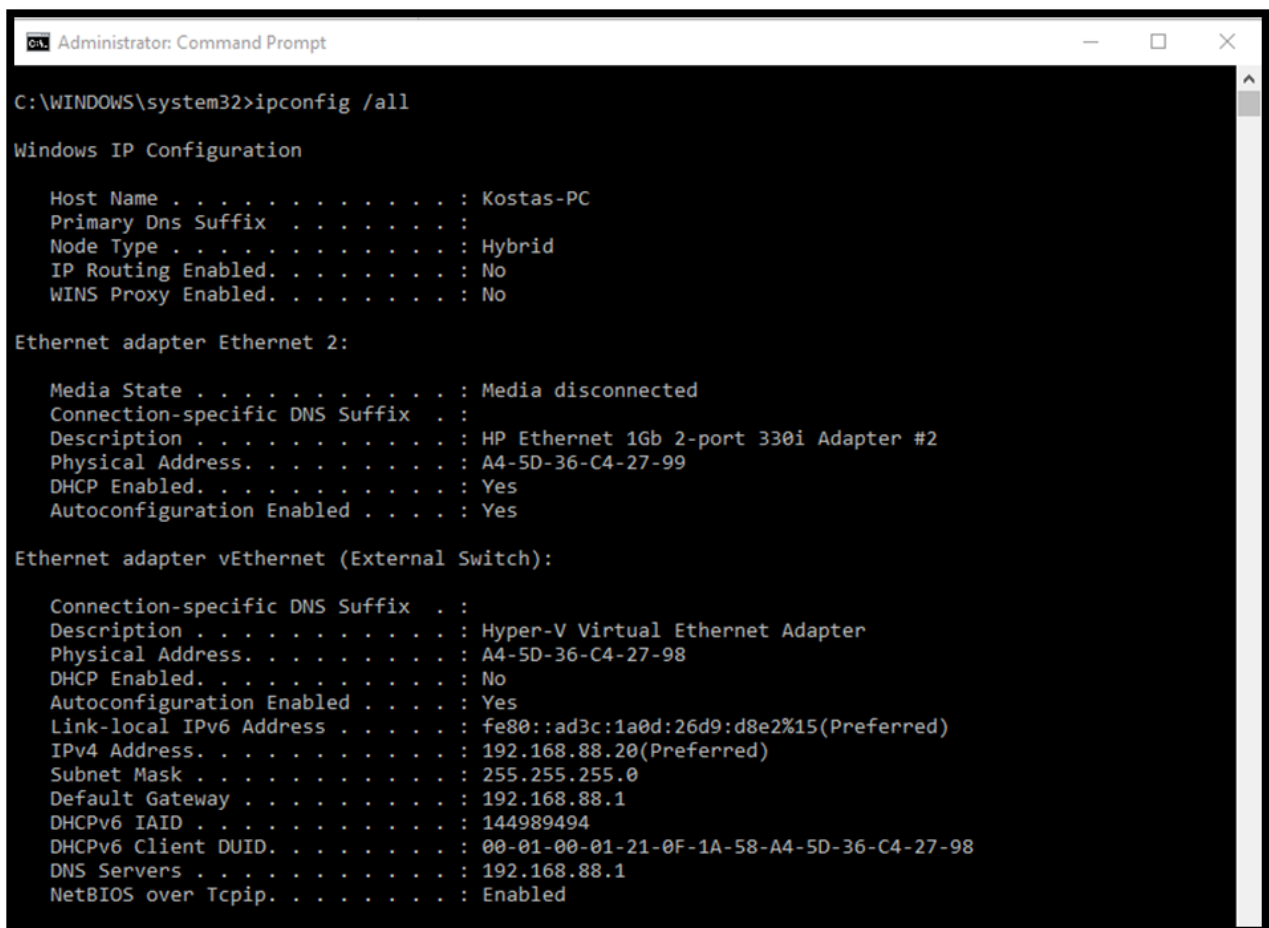
Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6022:261f:fb19:ff64%23
    IPv4 Address. . . . . : 172.18.72.161
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . :
```

This command provides you with information about your connection to a network (or to the Internet). Most importantly, you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the ipconfig command is the first step in determining your system's

network configuration. Most commands including ipconfig have a number of parameters, or flags, which can be passed to the commands to make the computer behave in a certain way. You can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark: -?.

As you can see, you might use a number of options to find out different details about your computer's configuration. The most commonly used method would probably be ipconfig/all.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The command "C:\WINDOWS\system32>ipconfig /all" has been entered. The output displays the Windows IP Configuration details, including Host Name (Kostas-PC), Primary Dns Suffix, Node Type (Hybrid), IP Routing Enabled (No), and WINS Proxy Enabled (No). It then lists two Ethernet adapters: "Ethernet adapter Ethernet 2:" and "Ethernet adapter vEthernet (External Switch):". The first adapter shows Media State as "Media disconnected", Description as "HP Ethernet 1Gb 2-port 330i Adapter #2", Physical Address as "A4-5D-36-C4-27-99", DHCP Enabled (Yes), and Autoconfiguration Enabled (Yes). The second adapter shows Connection-specific DNS Suffix, Description as "Hyper-V Virtual Ethernet Adapter", Physical Address as "A4-5D-36-C4-27-98", DHCP Enabled (No), Autoconfiguration Enabled (Yes), Link-local IPv6 Address as "fe80::ad3c:1a0d:26d9:d8e2%15(Preferred)", IPv4 Address as "192.168.88.20(Preferred)", Subnet Mask as "255.255.255.0", Default Gateway as "192.168.88.1", DHCPv6 IAID as "144989494", DHCPv6 Client DUID as "00-01-00-01-21-0F-1A-58-A4-5D-36-C4-27-98", DNS Servers as "192.168.88.1", and NetBIOS over Tcpip as "Enabled".

```
Administrator: Command Prompt

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : Kostas-PC
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet 2:

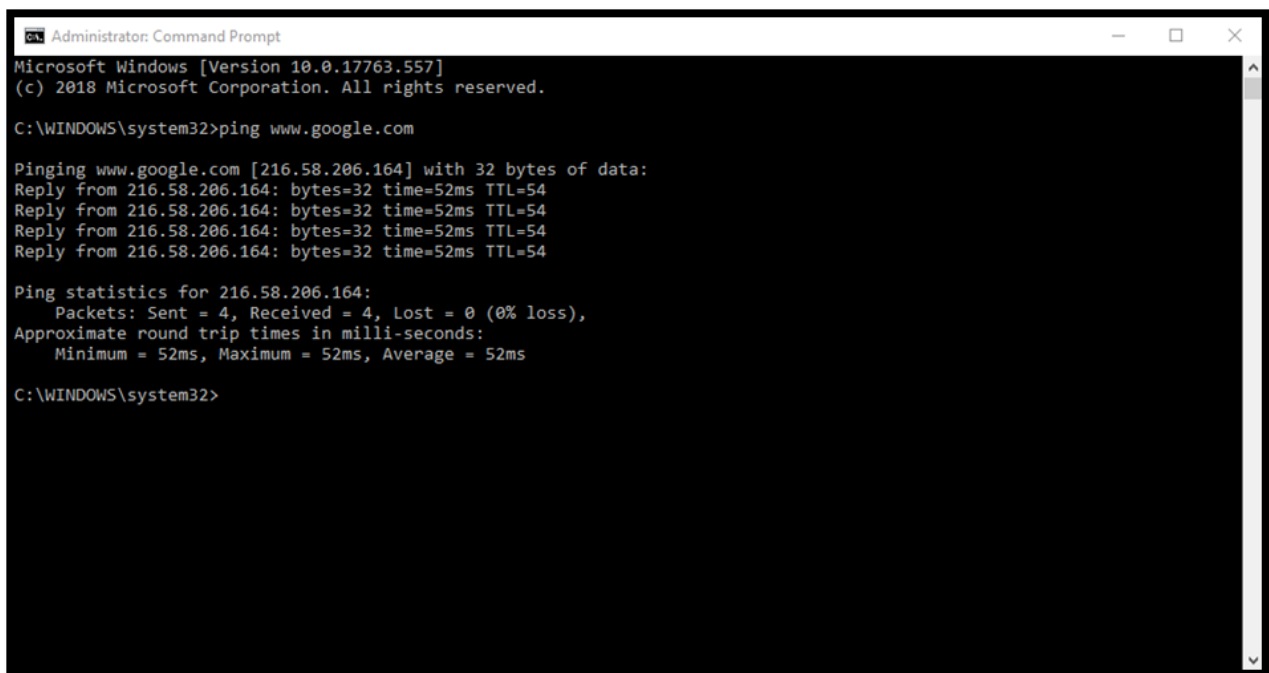
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : HP Ethernet 1Gb 2-port 330i Adapter #2
    Physical Address. . . . . : A4-5D-36-C4-27-99
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (External Switch):

    Connection-specific DNS Suffix . :
    Description . . . . . : Hyper-V Virtual Ethernet Adapter
    Physical Address. . . . . : A4-5D-36-C4-27-98
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::ad3c:1a0d:26d9:d8e2%15(Preferred)
    IPv4 Address. . . . . : 192.168.88.20(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.88.1
    DHCPv6 IAID . . . . . : 144989494
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-0F-1A-58-A4-5D-36-C4-27-98
    DNS Servers . . . . . : 192.168.88.1
    NetBIOS over Tcpip. . . . . : Enabled
```

## 1.4.2 Ping

Another common used command is ping. Ping is used to send a test packet or echo packet, to a machine in order to find out whether the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be implemented in elementary hacking techniques. Figure 1-3 shows the command.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of a ping command. The text is as follows:

```
Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.google.com

Pinging www.google.com [216.58.206.164] with 32 bytes of data:
Reply from 216.58.206.164: bytes=32 time=52ms TTL=54
Reply from 216.58.206.164: bytes=32 time=52ms TTL=54
Reply from 216.58.206.164: bytes=32 time=52ms TTL=54
Reply from 216.58.206.164: bytes=32 time=52ms TTL=54

Ping statistics for 216.58.206.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 52ms, Average = 52ms

C:\WINDOWS\system32>
```

The above command shows that a 32-byte echo packet was sent to the destination and returned. The TTL means “time to live.” That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the Internet is a vast conglomerate of interconnected networks. Your packet probably won’t go straight to its destination. It will have to take several hops to get there. As with `ipconfig`, you can type in `ping -?` to find out various ways you can refine your ping.

### 1.4.3 Tracert

The next command is `tracert`. This command is a sort of “ping deluxe.” Tracert does not only inform you whether the packet got there and how long it took, but it also gives you all the necessary information regarding all the intermediate hops it took to get there. (This same command can be executed in Linux or UNIX, but it is called `traceroute` rather than `tracert`.) You can see this utility in Figure 1-4.

```
Administrator: Command Prompt

C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [172.217.17.164]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.1.1
  2   1 ms     1 ms     1 ms     192.168.10.254
  3  24 ms    23 ms    23 ms    192.168.219.254
  4  24 ms    24 ms    24 ms    hu0-5-0-1.400-iag1.lat.cyta-ip.net [195.14.136.115]
  5  24 ms    24 ms    24 ms    hu0-4-0-0-icr1.lyk.cyta-ip.net [195.14.136.246]
  6  24 ms    24 ms    24 ms    hu0-1-1-0-ipr1.lat.cyta-ip.net [195.14.136.249]
  7  53 ms    52 ms    52 ms    google.bix.bg [193.169.198.80]
  8  53 ms    53 ms    53 ms    108.170.250.177
  9  52 ms    52 ms    52 ms    64.233.175.249
 10  52 ms    51 ms    51 ms    sof02s21-in-f164.1e100.net [172.217.17.164]

Trace complete.

C:\WINDOWS\system32>
```

Tracert enables you to see (in milliseconds) the time that the IP addresses of each intermediate step was listed, and how long it took to get to that step. It is very important to be well versed in the steps required to reach a destination.

### 1.4.4 Netstat

Netstat is another interesting command. It is an abbreviation for Network Status. Essentially, this command tells you what connections your computer currently has. Don't panic if you see several connections; This does not mean that someone has hacked your computer. You will see many private IP addresses. This means your network has internal communication going on. You can see this in Figure 1-5.

Certainly, other utilities can be used when working with network communications. However, the four we just examined are the core utilities. These four (ipconfig, ping, tracert, and netstat) are absolutely essential to any network administrator.

```
Administrator: Command Prompt - netstat

C:\WINDOWS\system32>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:11456         Kostas-PC:57627        ESTABLISHED
TCP    127.0.0.1:57565        Kostas-PC:57566        ESTABLISHED
TCP    127.0.0.1:57566        Kostas-PC:57565        ESTABLISHED
TCP    127.0.0.1:57571        Kostas-PC:57572        ESTABLISHED
TCP    127.0.0.1:57572        Kostas-PC:57571        ESTABLISHED
TCP    127.0.0.1:57627        Kostas-PC:11456        ESTABLISHED
TCP    127.0.0.1:58392        Kostas-PC:58393        ESTABLISHED
TCP    127.0.0.1:58393        Kostas-PC:58392        ESTABLISHED
TCP    127.0.0.1:61541        Kostas-PC:61542        ESTABLISHED
TCP    127.0.0.1:61542        Kostas-PC:61541        ESTABLISHED
TCP    192.168.88.20:57504     40.67.254.36:https      ESTABLISHED
TCP    192.168.88.20:57522     13.91.60.30:https       ESTABLISHED
TCP    192.168.88.20:57574     ec2-52-24-160-47:https  ESTABLISHED
TCP    192.168.88.20:57798     wo-in-f125:5222         ESTABLISHED
```