Using The route Command

The biggest reason for manipulating the routing table on a server is to create a firewall. For instance, let's say we're running an Application layer firewall on a server located between the demilitarized zone (DMZ) and the internal network.

This scenario would mean the routing that's happening on the server or hosts located in the DMZ wouldn't be able to reach the internal network's hosts and vice versa. To circumvent this problem, we would need to employ both static and default routing because running routing protocols on hosts and servers wouldn't be a good solution for today's networks.

To view the routing table on a Windows device, use the `route print` command, as shown below.

```
C:\Users\clarusway>route print
===========================================================================
Interface List
 14...9c 5c 8e ce d9 c9 ......Intel(R) I211 Gigabit Network Connection
 18...9c 5c 8e ce d9 ca ......Intel(R) Ethernet Connection (2) I219-V
 15...76 c6 3b 00 62 86 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...76 c6 3b 00 6a 86 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...74 c6 3b 00 62 86 ......Broadcom 802.11ac Network Adapter
  1...........................Software Loopback Interface 1
 17...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.22     35
        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
      192.168.1.0    255.255.255.0         On-link      192.168.1.22    291
     192.168.1.22  255.255.255.255         On-link      192.168.1.22    291
    192.168.1.255  255.255.255.255         On-link      192.168.1.22    291
        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      192.168.1.22    291
  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      192.168.1.22    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 17    331 ::/0                     On-link
  1    331 ::1/128                  On-link
 17    331 2001::/32                On-link
 17    331 2001:0:2851:782c:148e:f3fd:6aff:55b8/128
                                    On-link
 10    291 fe80::/64                On-link
 17    331 fe80::/64                On-link
 17    331 fe80::148e:f3fd:6aff:55b8/128
                                    On-link
 10    291 fe80::19ac:8efb:2c6e:f512/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    291 ff00::/8                 On-link
 17    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

In this output, you can see that each of the routes was added automatically when the system booted up. To see all the options available with the route command, type `route`.

route Command Options

To add a route to your routing table, use the following syntax:

```
route [-f] [-p] [Command] [Destination] [mask Netmask] [Gateway] [metric Metric]
```

- `-f`: Using this command with any of the options like add, change, or delete will clear the routing table of all entries that aren't host routes, the loopback network route or routes, and any multicast routes
- `-p`: If you use this with the add command, the individual route will be added to the Registry and then used to initialize the IP routing table whenever TCP/IP is started. Important to remember is that by default, the routes you've statically added won't remain in the routing table the next time TCP/IP boots. And if you use `-p` with the `print` command, you'll get shown a list of the persistent routes that are stored in the Registry location of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes`.

Now, let's take a look at how and when you would use the route command. The below table shows the command options available and what they do when you are using the route command with them.

Command	Purpose
add	Adds a route
change	Modifies an existing route
delete	Deletes a route (or routes)
print	Prints a route (or routes)

Here's a description of some other tasks you can accomplish via the rest of the command's options:

- `Destination`: This will give you the network destination of a given route. If the host bits of the network address are set to 0, it will be depicted with the destination's IP network address, an IP address for a specific host route, or the default route of `0.0.0.0`.
- `mask netmask`: This will provide you with the subnet mask that's associated with the destination network. The default destination subnet mask is `0.0.0.0`, and typically you'll see `255.255.255.255` representing a host route.
- `Gateway`: The gateway depends on the network address and subnet mask. It defines the next-hop IP address. For routes located on a local subnet, the gateway address maps directly to a particular interface. If the destination is on a remote network, the gateway IP address will direct packets to the router.
- `metric`: Metric refers to the cost of a given route from the sender to the receiver device, and it has a value between 1 and 9999. Devices use this value to choose the best, or most efficient, routes among those in its routing table—the route with the lowest value wins. This decision can also include factors like the number of hops and the speed, reliability, and available bandwidth of the path being considered.
- `if interface`: This tool depends on information from the gateway address and determines the interface index for the specific interface that needs to receive the data. You can get a list of interfaces along with their relevant interface indexes by typing the route print command.
- `/?`: Using this will allow you to view help at the command prompt.

Some Examples of The route Command

It is recommended that you spend some time practicing them on a nonproduction server.

- To display the entire IP routing table, type:

```
route print
```

- To add a default route with the default gateway address `192.168.10.1`, type:

```
route add 0.0.0.0 mask 0.0.0.0 192.168.10.1
```

- To add a route to the destination `10.1.1.0` with the subnet mask `255.255.255.0` and the next-hop address `10.2.2.2`, type:

```
route add 10.1.1.0 mask 255.255.255.0 10.2.2.2
```

- If you want to add a persistent route to the destination `10.100.0.0` with the subnet mask `255.255.0.0` and the next-hop address `10.2.0.1`, type:

```
route -p add 10.100.0.0 mask 255.255.0.0 10.2.0.1
```

- If you want to delete the route to the destination `10.100.0.0` with the subnet mask `255.255.0.0`, enter:

```
route delete 10.100.0.0 mask 255.255.0.0
```

- If you want to change the next-hop address of a route with the destination `10.100.0.0` and the subnet mask `255.255.0.0` from `10.2.0.1` to `10.7.0.5`, type:

```
route change 10.100.0.0 mask 255.255.0.0 10.7.0.5
```

The netstat Utility

Using `netstat` is a great way to check out the inbound and outbound TCP/IP connections on your machine. You can also use it to view packet statistics like how many packets have been sent and received, the number of errors, and so on. When used without any options, `netstat` produces output similar to the following, which shows all the outbound TCP/IP connections. This utility is a great tool to use to determine the status of outbound web connections. Take a look:

```
C:\Users\clarusway>netstat

Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.22:49812     ec2-35-157-203-133:https  ESTABLISHED
  TCP    192.168.1.22:49824     ed-in-f188:5228        ESTABLISHED
  TCP    192.168.1.22:50322     server-99-86-243-78:https  ESTABLISHED
  TCP    192.168.1.22:50918     54.239.31.91:https     ESTABLISHED
  TCP    192.168.1.22:51180     aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.1.22:51211     ec2-18-205-93-210:https  ESTABLISHED
  TCP    192.168.1.22:51212     ec2-52-202-62-236:https  CLOSE_WAIT
  TCP    192.168.1.22:51213     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51214     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51215     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51216     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51281     aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.1.22:51318     52.46.68.59:https      ESTABLISHED
  TCP    192.168.1.22:51346     ec2-3-225-75-90:https  ESTABLISHED
  TCP    192.168.1.22:51377     52.114.128.43:https    ESTABLISHED
  TCP    192.168.1.22:51391     aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.1.22:61298     ec2-52-202-62-228:https  ESTABLISHED
  TCP    192.168.1.22:61317     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:61320     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:61330     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:62010     51.105.249.228:https   ESTABLISHED
```

The **Proto column** lists the protocol being used. The **Local Address** column lists the source address and the source port (source socket). The **Foreign Address** column lists the address of the destination machine (the hostname if it's been resolved). If the destination port is known, it will show up as a well-known port. The **State column** indicates the status of each connection. This column shows statistics only for TCP connections because the *User Datagram Protocol (UDP)* establishes no virtual circuit to the remote device. Usually, this column indicates **ESTABLISHED** when a TCP connection between your computer and the destination computer has been established.

> **Tip:**
> - If the address of either your computer or the destination computer can be found in the HOSTS file on your computer, the destination computer's name, rather than the IP address, will show up in either the Local Address or Foreign Address column.

The output of the `netstat` utility depends on the switch. By using the `netstat /?` command, we can see the options available to us.

```
C:\Users\clarusway>netstat /?

Displays protocol statistics and current TCP/IP network connections.
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

The -a Switch

When you use the `-a` switch, the netstat utility displays all TCP/IP connections and all UDP connections. Below you can see the output produced by the `netstat -a` command.

```
C:\Users\clarusway>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.22:49812     ec2-35-157-203-133:https  ESTABLISHED
  TCP    192.168.1.22:49824     ed-in-f188:5228        ESTABLISHED
  TCP    192.168.1.22:50322     server-99-86-243-78:https  ESTABLISHED
  TCP    192.168.1.22:51211     ec2-18-205-93-210:https  ESTABLISHED
  TCP    192.168.1.22:51212     ec2-52-202-62-236:https  CLOSE_WAIT
  TCP    192.168.1.22:51213     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51214     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51215     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51216     ec2-18-205-93-141:https  CLOSE_WAIT
  TCP    192.168.1.22:51518     ec2-54-236-84-111:https  ESTABLISHED
  TCP    192.168.1.22:51548     185.11.14.41:http      TIME_WAIT
  TCP    192.168.1.22:51549     185.11.14.41:http      TIME_WAIT
  TCP    192.168.1.22:51550     185.11.14.41:http      TIME_WAIT
  TCP    192.168.1.22:51563     99.86.243.5:https      ESTABLISHED
  TCP    192.168.1.22:51564     ec2-3-225-75-90:https  ESTABLISHED
  TCP    192.168.1.22:51579     52.114.132.73:https    ESTABLISHED
  TCP    192.168.1.22:51585     aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.1.22:51597     server-99-86-245-89:https  ESTABLISHED
  TCP    192.168.1.22:61298     ec2-52-202-62-228:https  ESTABLISHED
  TCP    192.168.1.22:61317     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:61320     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:61330     ec2-3-120-198-117:https  ESTABLISHED
  TCP    192.168.1.22:62010     51.105.249.228:https   ESTABLISHED
  UDP    [fe80::19ac:8efb:2c6e:f512%10]:1900  *:*
  UDP    [fe80::19ac:8efb:2c6e:f512%10]:2177  *:*
  UDP    [fe80::19ac:8efb:2c6e:f512%10]:58133  *:*
```

You can tell that UDP connections in the output are broadcasts because the destination address is listed as * : * (meaning "any address, any port").

The most common use for the `-a` switch is to check the status of a TCP/IP connection that appears to be hung. You can determine if the connection is simply busy or is actually hung and no longer responding.

> **Tip:**
> - The **State** column in the figure has no entry for the UDP rows because UDP is not a connection-oriented protocol and, therefore, has no connection state.

The -e Switch

The `-e` switch displays a summary of all the packets that have been sent over the Network Interface Card (NIC) as of that instant. The Received and Sent columns show packets coming in as well as being sent:

```
C:\Users\clarusway>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     652308520       724669536
Unicast packets             7476729         5597781
Non-unicast packets            6906          240780
Discards                          0               0
Errors                            0               1
Unknown protocols                 0
```

You can use the `-e` switch to display the following categories of statistics:

- **Bytes** - The number of bytes transmitted or received since the computer was turned on. This statistic is useful for finding out if data is actually being transmitted and received or if the network interface isn't doing anything at all.
- **Unicast Packets** - The number of packets sent from or received at this computer. To register in one of these columns, the packet must be addressed directly from one computer to another and the computer's address must be in either the source or destination address section of the packet.

- **Non-unicast Packets** - The number of packets that weren't directly sent from one workstation to another. For example, a broadcast packet is a non-unicast packet. The number of non-unicast packets should be smaller than the number of unicast packets. If the number of non-unicast packets is as high as or higher than that of unicast packets, too many broadcast packets are being sent over your network. Definitely find the source of these packets and make any necessary adjustments to optimize performance.
- **Discards** - The number of packets that were discarded by the NIC during either transmission or reception because they weren't assembled correctly.
- **Errors** - The number of errors that occurred during transmission or reception. (These numbers may indicate problems with the network card.)
- **Unknown Protocols** - The number of received packets that the Windows networking stack couldn't interpret. This statistic only shows up in the Received column because if the computer sent them, they wouldn't be unknown.

Unfortunately, statistics don't mean much unless they can be colored with time information. For example, if the Errors row shows 1 error, is that a problem? It might be if the computer has been on for only a few minutes. Unfortunately, the netstat utility doesn't have a way of indicating how much time has elapsed for these statistics.

The -r Switch

You use the `-r` switch to display the current route table for a workstation so that you can see exactly how TCP/IP information is being routed.

```
C:\Users\clarusway>netstat -r
===========================================================================
Interface List
 14...9c 5c 8e ce d9 c9 ......Intel(R) I211 Gigabit Network Connection
 18...9c 5c 8e ce d9 ca ......Intel(R) Ethernet Connection (2) I219-V
 15...76 c6 3b 00 62 86 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...76 c6 3b 00 6a 86 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...74 c6 3b 00 62 86 ......Broadcom 802.11ac Network Adapter
  1...........................Software Loopback Interface 1
 17...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.22     35
        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
      192.168.1.0    255.255.255.0         On-link      192.168.1.22    291
     192.168.1.22  255.255.255.255         On-link      192.168.1.22    291
    192.168.1.255  255.255.255.255         On-link      192.168.1.22    291
        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      192.168.1.22    291
  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      192.168.1.22    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 17    331 ::/0                     On-link
  1    331 ::1/128                  On-link
 17    331 2001::/32                On-link
 17    331 2001:0:2851:782c:148e:f3fd:6aff:55b8/128
                                    On-link
 10    291 fe80::/64                On-link
 17    331 fe80::/64                On-link
 17    331 fe80::148e:f3fd:6aff:55b8/128
                                    On-link
 10    291 fe80::19ac:8efb:2c6e:f512/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    291 ff00::/8                 On-link
 17    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

The -s Switch

Using the `-s` switch displays a variety of TCP, UDP, IP, and ICMP protocol statistics. But be warned—the output you'll get is really long, which may or may not be okay for you.

```
C:\Users\clarusway>netstat -s

IPv4 Statistics

  Packets Received                   = 85199526
  Received Header Errors             = 0
  Received Address Errors            = 113
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 49
  Received Packets Discarded         = 9859
  Received Packets Delivered         = 85614599
  Output Requests                    = 60765459
  Routing Discards                   = 0
  Discarded Output Packets           = 5954
  Output Packet No Route             = 202
  Reassembly Required                = 10
  Reassembly Successful              = 4
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

The -p Switch

Like the `-n` switch, the `-p` switch is a modifier that's usually used with the `-s` switch to specify which protocol statistics to list in the output (IP, TCP, UDP, or ICMP). For example, if you want to view only ICMP statistics, you use the `-p` switch like so:

```
netstat -s -p ICMP
```

The `netstat` utility then displays the ICMP statistics instead of the entire gamut of TCP/IP statistics that the `-s` switch will typically flood you with. For a different example, let's use the `-s` and `-p` switches to retrieve some IPv6 information:

```
C:\Users\clarusway>netstat -s -p IPV6

IPv6 Statistics

  Packets Received                   = 261062
  Received Header Errors             = 0
  Received Address Errors            = 321
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 981
  Received Packets Delivered         = 263904
  Output Requests                    = 244359
  Routing Discards                   = 0
  Discarded Output Packets           = 539
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

The -n Switch

The `-n` switch is a modifier for the other switches. When used with them, it reverses the natural tendency of netstat to use names instead of network addresses. In other words, when you use the `-n` switch, the output always displays network addresses instead of their associated network names. Following is output from the netstat command used with the `netstat -n` command. It's showing the same information but with IP addresses instead of names:

```
C:\Users\clarusway>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.22:49812     35.157.203.133:443     ESTABLISHED
  TCP    192.168.1.22:49824     74.125.143.188:5228    ESTABLISHED
  TCP    192.168.1.22:52352     18.205.93.208:443      ESTABLISHED
  TCP    192.168.1.22:52354     18.205.93.141:443      CLOSE_WAIT
  TCP    192.168.1.22:52355     52.202.62.236:443      CLOSE_WAIT
  TCP    192.168.1.22:52356     18.205.93.141:443      CLOSE_WAIT
  TCP    192.168.1.22:52357     18.205.93.141:443      CLOSE_WAIT
  TCP    192.168.1.22:52358     18.205.93.141:443      CLOSE_WAIT
```