

## CLARK COLLINS

### ITC 250 LABORATORY REPORT – HW 2

#### **INTRODUCTION:**

This lab report covers the steps necessary to perform network troubleshooting using open source and built in operating system tools. This report lays out the necessary equipment and software to perform the steps of these processes. The steps are laid out in order and should be able to be followed by anyone old enough to read and follow directions. Good!

#### **OBJECTIVE:**

The purpose of this lab is to learn basic syntax for Windows and/or Unix commands. By following this procedure, you will be able to better manage and maintain your company's network. The beginning of this report goes over good open source tools that can be used to analyze network traffic. It is vital to know what data and devices are on your network in order to ensure proper security. By the end of this lab you will be able to tell what devices are connected to the network and when they are sending and receiving data. Good!

#### **EQUIPMENT LIST:**

The following equipment is required to perform this lab:

1. A Windows or Unix computer running ideally Windows Vista or higher and at least Unix (Mac OSX version 10.0 and above).
2. Administrative access to the machine is required.
3. Keyboard/Mouse
4. Internet connectivity (wired or wireless)

### **ACTIVITY 1:**

Selecting network analyzing tools.

After looking at more than a dozen network tools, I have gone over the list and picked out the ones that I personally find the most user-friendly, robust, and ideally, open source. Below you will find a spreadsheet listing my findings.

<b>Product</b>	<b>Cost</b>	<b>Details</b>	<b>My Ranking (1-10) Higher is Better</b>
Wireshark	Free or Paid	One of the most powerful, still considered a network tool standard by many in the IT field.	8, no longer entirely free, but still offers many great features such as
Angry IP Scanner	OpenSource	Offers portable edition, ping checks, NetBIOS info, hostname resolutions	7, less overall features than Wireshark, but entirely free
JDSU Network Analyzer	Tiered model, with a free base edition	In depth network analysis on top of everything that Wireshark and Angry IP offer. Scalable as well.	9, Great UI, tons of features, can get costly.
Microsoft Network Monitor	Free	Made by Microsoft, offers similar functions as the others, but not as scalable like JDSU for larger networks.	7, Free with limited functionality. Other tools offer better UI.

Good!

### **BLOCK DIAGRAM:**

Not Applicable to this Report.

### **ACTIVITY 2 PROCEDURE:**

- 1) Begin by opening your start menu and typing in run.exe. You can also use the hotkey WIN+R to open the run command. A third option is to type cmd in the start menu of Windows if you are on Windows 7-10.
- 2) **Activity 2A**
  - a) Type these commands into the command prompt and use your tool of choice (windows snipping tool is built into windows Vista through Windows 10, it is available in the start menu by typing "Snipping Tool" This will allow you to save images of what you have run in the command prompt)
    - i) Netstat
    - ii) Netstat -e
    - iii) Netstat ?
    - iv) Netstat -rn

3) **Activity 2B**

- a) The same process as Activity 2A Applies here. Type these commands into the command prompt and take printscreens of the results.
  - i) ipconfig /all
  - ii) ipconfig /renew
  - iii) ipconfig /release
  - iv) ipconfig /flushdns
  - v) ipconfig /displaydns
  - vi) ipconfig /registerdns
  - vii) ipconfig /showclassid
  - viii) ipconfig /setclassid

4) **Activity 2C**

- a) Follow the same process as the previous 2 typing these commands and saving/logging the results
  - i) Ping [www.mit.edu](http://www.mit.edu)
  - ii) Ping -n 10 [www.mit.edu](http://www.mit.edu)
  - iii) Ping [www.microsoft.edu](http://www.microsoft.edu)
  - iv) Ping [www.ucla.edu](http://www.ucla.edu)
  - v) Ping [www.Purdue.edu](http://www.Purdue.edu)

5) **Activity 2D**

- a) Follow the same process as the previous 3 typing these commands and saving/logging the results
  - i) Arp-a

6) **Activity 2E**

- a) Follow the same process as the previous 4 typing these commands and saving/logging the results
  - i) Route
  - ii) Route print
  - iii) Route print -4
  - iv) Route print -6

7) **Activity 2F**

- a) Follow the same process as the previous 5 typing these commands and saving/logging the results
  - i) Tracert [www.mit.edu](http://www.mit.edu)
  - ii) Tracert [www.microsoft.edu](http://www.microsoft.edu)
  - iii) Tracert [www.Purdue.edu](http://www.Purdue.edu)
  - iv) Tracert [www.iu.edu](http://www.iu.edu)

## ACTIVITY 2A DATA:

The following screen captures link back directly to the commands in the procedure portion of this report. The “netstat” command shows the active connections between the PC and host and the related connection from that host. In my case, I am on my work PC so it shows the other connection on the network. The second image shows the “netstat -e” connection which displays what is currently connected to the LAN either wired or wireless. “Netstat ?” shows the common commands that can be used in conjunction with netstat. “Netstat -rn” displays the information for routing both on IPV6 and IPV4.

```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

H:\>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    10.250.1.149:49497       ec2-52-53-150-232:https ESTABLISHED
TCP    10.250.1.149:49634       10.250.1.100:8009      ESTABLISHED
TCP    10.250.1.149:49707       msnbot-65-52-108-205:https ESTABLISHED
TCP    10.250.1.149:49719       sea14:http             ESTABLISHED
TCP    10.250.1.149:50392       atl14s78-in-f10:https  CLOSE_WAIT
TCP    10.250.1.149:52971       APP16:microsoft-ds     ESTABLISHED
TCP    10.250.1.149:53183       SVR-IM:5222            ESTABLISHED
TCP    10.250.1.149:53195       162.125.7.3:https      CLOSE_WAIT
TCP    10.250.1.149:53247       162.125.7.7:https      CLOSE_WAIT
TCP    10.250.1.149:53264       lax28s01-in-f170:https CLOSE_WAIT
TCP    10.250.1.149:53612       a104-92-129-159:https  CLOSE_WAIT
TCP    10.250.1.149:53613       a104-92-129-159:https  CLOSE_WAIT
TCP    10.250.1.149:53614       a104-92-129-159:https  CLOSE_WAIT
TCP    10.250.1.149:53615       a23-205-126-12:https   CLOSE_WAIT
TCP    10.250.1.149:53616       104.18.55.167:http      CLOSE_WAIT
TCP    10.250.1.149:53618       a23-205-126-12:https   CLOSE_WAIT
TCP    10.250.1.149:53621       a104-92-129-159:https  CLOSE_WAIT
TCP    10.250.1.149:53899       ord36s04-in-f13:https  CLOSE_WAIT
TCP    10.250.1.149:54122       DC:49168               ESTABLISHED
TCP    10.250.1.149:55774       10.250.1.132:8009      ESTABLISHED
TCP    10.250.1.149:56794       ord36s04-in-f13:https  CLOSE_WAIT
TCP    10.250.1.149:57022       162.125.34.129:https   ESTABLISHED
TCP    10.250.1.149:57383       r-54-45-234-77:http    CLOSE_WAIT
TCP    10.250.1.149:57469       162.125.18.133:https   ESTABLISHED
TCP    10.250.1.149:57486       ec2-34-197-126-3:https CLOSE_WAIT
TCP    10.250.1.149:57513       ms-c3po:8081           ESTABLISHED
TCP    10.250.1.149:57659       lax17s05-in-f13:https  CLOSE_WAIT
TCP    10.250.1.149:57660       lax28s01-in-f170:https CLOSE_WAIT
TCP    10.250.1.149:57769       40.97.119.82:https     ESTABLISHED
TCP    10.250.1.149:57770       40.97.119.82:https     ESTABLISHED
TCP    10.250.1.149:57816       40.97.129.114:https    ESTABLISHED
TCP    10.250.1.149:57817       40.97.129.114:https    ESTABLISHED
TCP    10.250.1.149:57869       lax17s15-in-f74:https  CLOSE_WAIT
TCP    10.250.1.149:57885       lax28s01-in-f165:https ESTABLISHED
TCP    10.250.1.149:57890       162.125.34.137:https   CLOSE_WAIT
TCP    10.250.1.149:57911       a104-89-73-143:https   CLOSE_WAIT
TCP    10.250.1.149:57916       a23-222-212-250:https  ESTABLISHED
TCP    10.250.1.149:57917       a23-222-212-250:https  ESTABLISHED
TCP    10.250.1.149:57918       a23-222-212-250:https  ESTABLISHED
TCP    10.250.1.149:57920       a96-6-54-233:https     ESTABLISHED
TCP    10.250.1.149:57921       162.125.3.4:https      CLOSE_WAIT
TCP    10.250.1.149:57934       DC1:microsoft-ds       ESTABLISHED
TCP    10.250.1.149:57959       162.125.7.3:https      CLOSE_WAIT
TCP    10.250.1.149:57961       lax17s34-in-f10:https  ESTABLISHED
TCP    10.250.1.149:57962       lax17s34-in-f10:https  ESTABLISHED
TCP    10.250.1.149:57966       40.97.164.162:https    TIME_WAIT
TCP    10.250.1.149:57967       40.97.164.162:https    TIME_WAIT
TCP    10.250.1.149:57968       40.97.130.178:https    TIME_WAIT
TCP    10.250.1.149:57969       13.76.219.191:https    TIME_WAIT
TCP    10.250.1.149:57970       40.97.126.194:https    TIME_WAIT
TCP    10.250.1.149:57971       13.78.188.147:https    TIME_WAIT
TCP    10.250.1.149:57972       104.40.28.30:https     TIME_WAIT
TCP    10.250.1.149:57973       13.107.21.200:https    ESTABLISHED
TCP    10.250.1.149:57974       13.107.21.200:https    ESTABLISHED
TCP    10.250.1.149:57975       104.40.28.30:https     TIME_WAIT
TCP    10.250.1.149:57976       a23-202-233-152:http   TIME_WAIT
TCP    10.250.1.149:57977       a23-202-232-103:https  ESTABLISHED
TCP    10.250.1.149:57978       52.161.21.245:https    ESTABLISHED
TCP    10.250.1.149:57979       sea02-003:http         TIME_WAIT
TCP    10.250.1.149:57981       40.97.121.34:https     ESTABLISHED
TCP    10.250.1.149:57982       40.97.130.178:https    ESTABLISHED
TCP    10.250.1.149:57983       40.97.130.178:https    ESTABLISHED
TCP    10.250.1.149:57984       r-56-41-234-77:http    TIME_WAIT
TCP    10.250.1.149:57985       40.97.130.178:https    ESTABLISHED
TCP    10.250.1.149:57986       40.97.164.162:https    ESTABLISHED
TCP    10.250.1.149:58338       ord36s02-in-f173:https CLOSE_WAIT
TCP    10.250.1.149:58384       pl-in-f125:5222        ESTABLISHED
TCP    10.250.1.149:58522       DC:49168               ESTABLISHED
TCP    10.250.1.149:63505       40.97.162.162:https    ESTABLISHED
TCP    10.250.1.149:64985       in-in-f188:5228        ESTABLISHED
TCP    10.250.1.149:65407       10.250.1.137:8009      ESTABLISHED
TCP    10.250.1.149:65533       mail:5001              ESTABLISHED
TCP    127.0.0.1:53234          CLARK-MAINSTAY:53235   ESTABLISHED
TCP    127.0.0.1:53235          CLARK-MAINSTAY:53234   ESTABLISHED
TCP    127.0.0.1:53237          CLARK-MAINSTAY:53238   ESTABLISHED
TCP    127.0.0.1:53238          CLARK-MAINSTAY:53237   ESTABLISHED
TCP    127.0.0.1:53245          CLARK-MAINSTAY:53246   ESTABLISHED
TCP    127.0.0.1:53246          CLARK-MAINSTAY:53245   ESTABLISHED
```

```
Command Prompt

H:\>netstat -e
Interface Statistics


```

	Received	Sent
Bytes	804315024	4050979192
Unicast packets	60789436	12499276
Non-unicast packets	7568832	316100
Discards	0	0
Errors	0	0
Unknown protocols	0	

```
H:\>
```

```
Command Prompt

H:\>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.

H:\>
```

Command Prompt

H:\>netstat -rn

Interface List

13...40 8d 5c 43 07 94 .....Realtek PCIe GBE Family Controller  
1.....Software Loopback Interface 1

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	10.250.1.1	10.250.1.149	25
10.250.1.0	255.255.255.0		On-link	10.250.1.149	281
10.250.1.149	255.255.255.255		On-link	10.250.1.149	281
10.250.1.255	255.255.255.255		On-link	10.250.1.149	281
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
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	10.250.1.149	281
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	10.250.1.149	281

Persistent Routes:

None

IPv6 Route Table

Active Routes:

If	Metric	Network	Destination	Gateway
1	331	::1/128		On-link
13	281	fe80::/64		On-link
13	281	fe80::309d:7139:3e03:ff85/128		On-link
1	331	ff00::/8		On-link
13	281	ff00::/8		On-link

Persistent Routes:

None

H:\>

### **ACTIVITY 2B DATA:**

There are many uses for the ipconfig commands. They can be used for changing IP addresses, releases IP's, among hundreds of other options. The ipconfig is among the most common commands used in a command prompt, and for good reason. The following images depict, in order, what the lab report had us run.

- 1) ipconfig /all (Displays the full TCP/IP config for all adapters if no adapter/NIC is defined)
- 2) ipconfig /renew (Renews the IP address forcing the router to assign a new one is new policies require it in the router's settings)
- 3) ipconfig /release (releases the current IP address to assign a new one if the current one is not statically assigned by MAC address. This can also result in the same IP being assigned even without a static IP depending on how your router is configured)
- 4) ipconfig /flushdns (Flushes/Wipes the DNS records for that specific address)
- 5) ipconfig /displaydns (Shows the current DNS on that device)
- 6) ipconfig /registerdns (Registers a DNS to that device)
- 7) ipconfig /showclassid (Displays the contents of the DHCP class ID)
- 8) ipconfig /setclassid (Designates a DHCP class ID)

Further Details and References can be found here:

<https://technet.microsoft.com/en-us/library/bb490921.aspx>

```
Command Prompt

H:\>ipconfig ?

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns     Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6    Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is
removed.

Examples:
    > ipconfig          ... Show information
    > ipconfig /all      ... Show detailed information
    > ipconfig /renew     ... renew all adapters
    > ipconfig /renew EL* ... renew any connection that has its
                        name starting with EL
    > ipconfig /release *Con* ... release all matching connections,
                        eg. "Wired Ethernet Connection 1" or
                        "Wired Ethernet Connection 2"
    > ipconfig /allcompartments ... Show information about all
                        compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                        compartments

H:\>
```



Command Prompt

H:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : CLARK-MAINSTAY  
Primary Dns Suffix . . . . . : mss.local  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : mss.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : mss.local  
Description . . . . . : Realtek PCIe GBE Family Controller  
Physical Address. . . . . : 40-8D-5C-43-07-94  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::309d:7139:3e03:ff85%13(Preferred)  
IPv4 Address. . . . . : 10.250.1.149(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Saturday, September 02, 2017 12:01:11 AM  
Lease Expires . . . . . : Friday, September 08, 2017 2:15:47 PM  
Default Gateway . . . . . : 10.250.1.1  
DHCP Server . . . . . : 10.250.1.221  
DHCPv6 IAID . . . . . : 255888732  
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-9D-2E-48-40-8D-5C-43-07-94  
  
DNS Servers . . . . . : 10.250.1.221  
NetBIOS over Tcpip. . . . . : Enabled

H:\>

```
Command Prompt

H:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : CLARK-MAINSTAY
    Primary Dns Suffix . . . . . : mss.local
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : mss.local

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : mss.local
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 40-8D-5C-43-07-94
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::309d:7139:3e03:ff85%13(Preferred)
    IPv4 Address. . . . . : 10.250.1.149(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, September 02, 2017 12:01:11 AM
    Lease Expires . . . . . : Friday, September 08, 2017 2:15:47 PM
    Default Gateway . . . . . : 10.250.1.1
    DHCP Server . . . . . : 10.250.1.221
    DHCPv6 IAID . . . . . : 255888732
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-9D-2E-48-40-8D-5C-43-07-94

    DNS Servers . . . . . : 10.250.1.221
    NetBIOS over Tcpip. . . . . : Enabled

H:\>
```

#### **ACTIVITY 2C DATA:**

The ping tests to the assorted Domains resulted in similar results. The -n 10 command allows a user to specify how many ping tests are run before stopping. If ping -n is used without a number following it, a continuous ping will be run, this can be useful for testing to see if a connection is not stable, but still online. I did not see any large fluctuations in my tests with ms delays. They were all very consistent and well within a healthy range, which, in my opinion is anything under 50ms. This varies depending on the type of network set up, and whether or not delays are important such as live video feeds, etc. None of these tests involved changing the number of bytes of data sent for the ping tests, I have actually never tried adjusting that and will look into it this weekend to find out more.

```
Command Prompt

H:\>ping www.mit.edu

Pinging e9566.dscb.akamaiedge.net [104.126.14.214] with 32 bytes of data:
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53

Ping statistics for 104.126.14.214:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 52ms, Average = 52ms

H:\>
```

```
Command Prompt

H:\>ping -n 10 www.mit.edu

Pinging e9566.dscb.akamaiedge.net [104.126.14.214] with 32 bytes of data:
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=53ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53
Reply from 104.126.14.214: bytes=32 time=52ms TTL=53

Ping statistics for 104.126.14.214:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 53ms, Average = 52ms

H:\>
```

```
Command Prompt

H:\>ping www.microsoft.com

Pinging e1863.dspb.akamaiedge.net [23.44.161.156] with 32 bytes of data:
Reply from 23.44.161.156: bytes=32 time=60ms TTL=52
Reply from 23.44.161.156: bytes=32 time=60ms TTL=52
Reply from 23.44.161.156: bytes=32 time=59ms TTL=52
Reply from 23.44.161.156: bytes=32 time=60ms TTL=52

Ping statistics for 23.44.161.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 59ms, Maximum = 60ms, Average = 59ms

H:\>
```

```
Command Prompt

H:\>ping www.ucla.edu

Pinging gateway.lb.it.ucla.edu [164.67.228.152] with 32 bytes of data:
Reply from 164.67.228.152: bytes=32 time=100ms TTL=48
Reply from 164.67.228.152: bytes=32 time=100ms TTL=48
Reply from 164.67.228.152: bytes=32 time=101ms TTL=48
Reply from 164.67.228.152: bytes=32 time=100ms TTL=48

Ping statistics for 164.67.228.152:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 100ms, Maximum = 101ms, Average = 100ms

H:\>
```

```
Command Prompt

H:\>ping www.purdue.edu

Pinging www.purdue.edu [128.210.7.200] with 32 bytes of data:
Reply from 128.210.7.200: bytes=32 time=20ms TTL=246
Reply from 128.210.7.200: bytes=32 time=20ms TTL=246
Reply from 128.210.7.200: bytes=32 time=20ms TTL=246
Reply from 128.210.7.200: bytes=32 time=20ms TTL=246

Ping statistics for 128.210.7.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

H:\>
```

### ACTIVITY 2D DATA:

The “arp” command stands for Address Resolution Protocol. This command displays all local physical connection MAC addresses. This also states the types, whether dynamic or static. It is very useful when trying to find specific devices since MAC (physical addresses) are typically static.

```
Command Prompt
H:\>arp -a

Interface: 10.250.1.149 --- 0xd
Internet Address      Physical Address      Type
10.250.1.1            b0-b2-dc-70-a9-55    dynamic
10.250.1.33           18-68-cb-0d-70-b1    dynamic
10.250.1.39           a4-14-37-fe-9a-e5    dynamic
10.250.1.40           a4-14-37-2e-a4-46    dynamic
10.250.1.41           bc-ad-28-35-d7-1f    dynamic
10.250.1.44           a4-14-37-7b-8d-08    dynamic
10.250.1.45           bc-ad-28-35-d5-f5    dynamic
10.250.1.46           a4-14-37-fe-9a-e3    dynamic
10.250.1.55           00-90-a9-e5-eb-1d    dynamic
10.250.1.60           fc-3f-db-c1-52-74    dynamic
10.250.1.61           30-f7-72-53-ee-d6    dynamic
10.250.1.82           00-15-65-9a-47-19    dynamic
10.250.1.100          f4-f5-d8-a7-f4-ae    dynamic
10.250.1.102          cc-95-d7-50-9c-b1    dynamic
10.250.1.104          50-63-13-c4-02-b6    dynamic
10.250.1.112          b8-27-eb-cd-41-bf    dynamic
10.250.1.116          a4-8d-3b-c0-29-a6    dynamic
10.250.1.124          4c-0b-be-0e-fb-5a    dynamic
10.250.1.126          1c-91-48-74-24-5b    dynamic
10.250.1.127          60-14-b3-7c-bd-35    dynamic
10.250.1.128          bc-83-85-20-cd-79    dynamic
10.250.1.129          1c-1b-0d-63-50-3d    dynamic
10.250.1.130          60-14-b3-7c-bc-c9    dynamic
10.250.1.132          f4-f5-d8-0f-c2-02    dynamic
10.250.1.133          1c-1e-e3-c0-90-8e    dynamic
10.250.1.137          f4-f5-d8-a7-f3-5e    dynamic
10.250.1.138          c0-33-5e-0f-1a-89    dynamic
10.250.1.141          4c-0b-be-2d-7d-b8    dynamic
10.250.1.146          b4-ae-2b-d1-ce-0a    dynamic
10.250.1.147          f4-6d-04-2c-7a-1a    dynamic
10.250.1.152          60-45-cb-7f-97-85    dynamic
10.250.1.153          fc-aa-14-94-55-dc    dynamic
10.250.1.159          74-d4-35-5f-0d-10    dynamic
10.250.1.161          00-90-a9-e5-e9-7a    dynamic
10.250.1.172          fc-aa-14-c2-8a-d3    dynamic
10.250.1.173          b8-97-5a-3b-92-1f    dynamic
10.250.1.179          74-d4-35-5f-0c-ae    dynamic
10.250.1.202          00-15-5d-01-b8-01    dynamic
10.250.1.221          00-15-5d-01-8e-00    dynamic
10.250.1.222          00-15-5d-01-b8-14    dynamic
10.250.1.223          00-15-5d-01-b8-12    dynamic
10.250.1.224          00-15-5d-01-fb-00    dynamic
10.250.1.227          00-15-5d-01-8e-03    dynamic
10.250.1.248          d4-be-d9-d1-20-08    dynamic
10.250.1.250          00-25-90-fc-d7-8a    dynamic
10.250.1.255          ff-ff-ff-ff-ff-ff    static
169.254.211.135      b4-ae-2b-dc-94-c9    dynamic
224.0.0.2            01-00-5e-00-00-02    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

H:\>
```

## ACTIVITY 2E DATA:

The route commands display both the virtual and physical NIC's on the PC as well as the active routing tables of the machine the command was run on. You can choose whether or not to define IPV6 and IPV4 by using -4 or -6 at the end of the command.

```
Command Prompt

H:\>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
file NETWORKS.  The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE.  Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed.  The '*' matches any string,
and '?' matches any one char.  Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.

Diagnostic Notes:
  Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
  Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
           The route addition failed: The specified mask parameter is invalid.
           (Destination & Mask) != Destination.

Examples:

> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157*          .... Only prints those matching 157*

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
      destination^      ^mask      ^gateway      metric^      ^
                        Interface^
  If IF is not given, it tries to find the best interface for a given
  gateway.
> route ADD 3ffe::/32 3ffe::1

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2
      CHANGE is used to modify gateway and/or metric only.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32

H:\>
```

```
Command Prompt
H:\>route print
=====
Interface List
 13...40 8d 5c 43 07 94 .....Realtek PCIe GBE Family Controller
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.250.1.1       10.250.1.149     25
10.250.1.0                 255.255.255.0    On-link          10.250.1.149     281
10.250.1.149               255.255.255.255  On-link          10.250.1.149     281
10.250.1.255               255.255.255.255  On-link          10.250.1.149     281
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
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          10.250.1.149     281
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          10.250.1.149     281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1      331 ::1/128 On-link
13     281 fe80::/64 On-link
13     281 fe80::309d:7139:3e03:ff85/128 On-link
1      331 ff00::/8 On-link
13     281 ff00::/8 On-link
=====
Persistent Routes:
None

H:\>
```



```
Command Prompt

H:\>route print -4
=====
Interface List
 13...40 8d 5c 43 07 94 .....Realtek PCIe GBE Family Controller
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
-----
0.0.0.0                    0.0.0.0          10.250.1.1        10.250.1.149     25
10.250.1.0                 255.255.255.0    On-link          10.250.1.149     281
10.250.1.149              255.255.255.255  On-link          10.250.1.149     281
10.250.1.255              255.255.255.255  On-link          10.250.1.149     281
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
224.0.0.0                 240.0.0.0        On-link          127.0.0.1        331
240.0.0.0                 240.0.0.0        On-link          10.250.1.149     281
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          10.250.1.149     281
=====
Persistent Routes:
None

H:\>
```

```
Command Prompt

H:\>route print -6
=====
Interface List
 13...40 8d 5c 43 07 94 .....Realtek PCIe GBE Family Controller
 1.....Software Loopback Interface 1
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
-----
1      331 ::1/128                      On-link
13     281 fe80::/64                    On-link
13     281 fe80::309d:7139:3e03:ff85/128 On-link
1      331 ff00::/8                      On-link
13     281 ff00::/8                      On-link
=====
Persistent Routes:
None

H:\>
```

## ACTIVITY 2F DATA:

The “tracert” command is used to define which route packets use in transit from the local system to the defined remote system. I noticed that the www.Microsoft.edu address time out because it is not an active Domain since they do not (to my knowledge) operate an educational institute. This is typically a command that is run to see if a website domain is working or not. We use it often at the office at work when a client’s website goes down.

```
Command Prompt - tracert www.microsoft.edu

H:\>tracert www.mit.edu

Tracing route to e9566.dscb.akamaiedge.net [104.89.86.36]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  10.250.1.1
  2   2 ms   2 ms   2 ms  static-184-17-158-105.ftwy.in.frontiernet.net [1
84.17.158.105]
  3   1 ms   2 ms   2 ms  172.76.20.101
  4  10 ms  10 ms   9 ms  74.40.4.77
  5  10 ms  10 ms  11 ms  ae1---0.cbr01.chcg.il.frontiernet.net [74.40.4.1
42]
  6 123 ms 221 ms 217 ms 74.43.94.5
  7  10 ms  10 ms   9 ms  a104-89-86-36.deploy.static.akamaitechnologies.c
om [104.89.86.36]

Trace complete.

H:\>tracert www.microsoft.edu

Tracing route to www.microsoft.edu [198.105.254.114]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  10.250.1.1
  2   2 ms   2 ms   2 ms  static-184-17-158-105.ftwy.in.frontiernet.net [1
84.17.158.105]
  3   2 ms   1 ms   1 ms  172.76.20.101
  4  10 ms   9 ms  10 ms  74.40.4.77
  5  10 ms   9 ms   9 ms  ae1---0.cbr01.chcg.il.frontiernet.net [74.40.4.1
42]
  6  14 ms  23 ms  23 ms  10gigabitethernet4-1.core1.chi1.he.NET [206.223.
119.37]
  7  51 ms  29 ms  22 ms  100ge12-1.core1.mci3.he.net [184.105.81.209]
  8  37 ms  35 ms  38 ms  100ge12-1.core1.den1.he.net [184.105.64.49]
  9  90 ms  84 ms  89 ms  100ge12-1.core1.lax2.he.net [184.105.222.113]
 10  79 ms  78 ms  95 ms  xerocole-inc.gigabitethernet2-9.core1.lax2.he.ne
t [64.62.133.170]
 11  *      *      *      Request timed out.
 12  *      *      *      Request timed out.
 13  *      *      *      Request timed out.
 14  *      *      *      Request timed out.
 15  *      *      *      Request timed out.
```

```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

H:\>tracert www.purdue.edu

Tracing route to www.purdue.edu [128.210.7.200]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    10.250.1.1
  2   2 ms     2 ms     1 ms     static-184-17-158-105.ftwy.in.frontiernet.net [1
84.17.158.105]
  3   1 ms     2 ms     1 ms     172.76.20.101
  4  10 ms    10 ms    10 ms    74.40.4.77
  5  10 ms    10 ms     9 ms    ae1---0.cbr01.chcg.il.frontiernet.net [74.40.4.1
42]
  6  10 ms    10 ms    10 ms    eq-exchange.tr01-chcgil01.transitrail.NET [206.2
23.119.116]
  7   9 ms    10 ms    10 ms    et-2-3-0.212.rtsw.chic.net.internet2.edu [149.16
5.183.5]
  8  11 ms    10 ms    10 ms    et-2-0-0.212.rtr2.chic.indiana.gigapop.net [149.
165.183.4]
  9  14 ms    15 ms    14 ms    indiana-gigapop-ctc-internet-151.tcom.purdue.edu
[192.5.40.82]
 10  19 ms    18 ms    37 ms    tel-210-c9006-01-te0-0-0-0-151.tcom.purdue.edu [
192.5.40.81]
 11  21 ms    20 ms    21 ms    itap-dc-core-vss-01-te2-3-1.tcom.purdue.edu [192
.5.40.90]
 12  20 ms    21 ms    20 ms    128.210.7.200

Trace complete.

H:\>tracert www.iu.edu

Tracing route to www.iu.edu [129.79.78.188]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    10.250.1.1
  2   1 ms     2 ms     1 ms     static-184-17-158-105.ftwy.in.frontiernet.net [1
84.17.158.105]
  3   1 ms     1 ms     2 ms     172.76.20.101
  4  10 ms    10 ms    10 ms    74.40.4.77
  5  10 ms    10 ms    10 ms    ae1---0.cbr01.chcg.il.frontiernet.net [74.40.4.1
42]
  6  46 ms    38 ms    54 ms    equinix-exchange.chi-2.wiscnet.NET [206.223.119.
7]
  7  15 ms    14 ms    15 ms    ae-1.2247.rtr.ictc.indiana.gigapop.net [149.165.
183.89]
  8  15 ms    15 ms    28 ms    ae-4.12.rtr.ll.indiana.gigapop.net [149.165.183.
13]
  9  16 ms    15 ms    15 ms    tge-1-2.12.br.hper.net.uits.iu.edu [149.165.183.
14]
 10  21 ms    20 ms    21 ms    ae-33.932.dcr3.blcd.net.uits.iu.edu [134.68.3.12
9]
 11  16 ms    15 ms    16 ms    zeus2-iu.gateway.indiana.edu [129.79.78.188]

Trace complete.

H:\>
```

## **CONCLUSION:**

This was a useful lab to introduce people to the basics of the command prompt. It shows people how to get vital information about devices on a network as well as the routing tables and physical addresses currently in use. Some of these commands I use on a weekly basis when clients are having trouble connecting or loading webpages as well for issues with connectivity to servers or ipsec tunnels.

To recap on what was covered, the “netstat” command allows for viewing of networking information and monitor TCP/IP network activity. The “ipconfig” command allows for a great number of useful operations involving setting, releasing, renew, and assessing the IP addresses of devices on the network. The “ping” command allows one to assess delay times, and connectivity to remote addresses and domains. The “route” command displays routing tables and is useful when troubleshooting and ensuring efficiency on the network. The “tracert” commands tells you which route specific packets are taking from a host to a destination.

## **QUESTIONS/COMMENTS:**

I intend to delve a little deeper into the command prompt this weekend to get a further grasp of all that it can do. I had not run the netstat commands in quite some time.

GRADE A+