

LABORATORY REPORT:
ITC-25000: Web Systems Homework #1
Austin VanSumeren

Grade 100/100

INTRODUCTION:

This lab reports covers the steps and instructions necessary to perform general TCP/IP network monitoring and management commands via the Command Prompt program on most Window based PCs. This report will show many of the most common commands entered into the Command Prompt program, their uses, and what information is generated from using them. The understanding of each command and its uses will be beneficial to those seeking to become more knowledgeable of their computers. Following the steps in this lab will allow even those with relatively little computer networking experiencing to grasp a better understanding of these important commands. Excellent!

OBJECTIVE:

The purpose of this lab is to obtain the knowledge necessary to use common TCP/IP network management commands. By following and using these commands appropriately users will be able to do a number of tasks including, traffic monitoring, troubleshooting network access, adding new hosts to the network, and more. This lab touches on network management commands using the netstat command that can be used to check network configuration and monitor a system's TCP/IP network. It also touches on the uses and need for the IPCONFIG command to detect bad IP addresses, incorrect subnet masks, and improper addresses. Finally, the lab will teach the uses of the Ping command, which verifies whether a remote host can be reached. By the end of this lab, users will be able to appropriately use TCP/IP networking commands to diagnose, troubleshoot, and configure a system's TCP/IP network. Excellent!

EQUIPMENT LIST:

The following equipment is required to perform this lab:

- A Windows or Unix based computer running Windows Vista or higher and at least Unix (Mac OSX version 10.0 and above.)
- Administrative access to the computer for use of the Command Prompt program.
- Keyboard and mouse
- Internet connection (wired or wireless).

My PC:

- Dell Inspiron 17-7778
- Windows 10 Home
- Intel Core i7-6500U CPU

BLOCK DIAGRAM:

Not applicable for this lab.

PROCEDURE:

- **Activity 1:** Search the internet for three “network analyzer” products. After you compile three, create a table, and show the feature comparison of the three. Finally, choose one that you feel would be best for a small company of two-hundred of employees and prepare a recommendation. Very good

Product	Cost	Details	Rating (Out of 10)
Solar winds	Free or Paid	Easy to use and navigate. Highly trusted amongst the IT community. Highly configurable.	5/10. Though a terrific program, may be too difficult for a small company to manage. Though its ease of use would be beneficial, the number of option may be too much.
Wireshark	Free or Paid	Powerful, highly trusted amongst IT community, Live and offline analysis, multiplatform	9/10. The best option for the small company. Powerful and its ease of use make it ideal. The basic structure of the program will allow the company to grow and learn, will allow them to upgrade once they are ready.
Network Analyzer Sniffer Tool (NAST)	Paid	Not routinely developed, great for capturing network traffic,	3/10. Though ease of use, the fact it is not maintained well and it being a paid program makes this option ineffective for the company.

- **Activity 2:** Open a Command Prompt on your computer, or you may click your start menu, type in ‘run.exe’. A third option is to type ‘cmd’ in the start menu of your Windows based computer.
 - **Activity 2A:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Netstat
 - Netstat -e
 - Netstat ?
 - Netstat -rn
 - **Activity 2B:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Ipconfig ?
 - **Activity 2C:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Ping www.mit.edu
 - Ping -n 10 www.mit.edu
 - Ping www.microsoft.com
 - Ping www.UCLA.edu

- Ping www.purdue.edu
- **Activity 2D:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Arp -a
- **Activity 2E:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Route
 - Route print
 - Route print -4
 - Route print -6
- **Activity 2F:** Enter the following commands, copy the displayed results, and explain why the results are obtained:
 - Tracert www.mit.edu
 - Tracert www.microsoft.edu
 - Tracert www.purdue.edu
 - Tracert www.iu.edu

*****Next Image Too Large To Fit Into This Space, Please See Next Page*****

DATA:

- **Activity 2A:**

```
C:\Users\vansam01>Netstat
Active Connections

Proto Local Address           Foreign Address         State
TCP   10.18.11.98:49558       13.89.217.116:https    ESTABLISHED
TCP   10.18.11.98:52070       ad3:microsoft-ds      ESTABLISHED
TCP   10.18.11.98:52678       edir1:524              ESTABLISHED
TCP   10.18.11.98:52679       edir1:524              ESTABLISHED
TCP   10.18.11.98:52703       fsstudent:microsoft-ds ESTABLISHED
TCP   10.18.11.98:52713       adprintlabs:49157     ESTABLISHED
TCP   10.18.11.98:52716       fs4:524                ESTABLISHED
TCP   10.18.11.98:52772       adprintlabs:9191      ESTABLISHED
TCP   10.18.11.98:52786       ord30s25-in-f195:https ESTABLISHED
TCP   10.18.11.98:52791       ord30s25-in-f14:https ESTABLISHED
TCP   10.18.11.98:52794       ord30s25-in-f14:http  CLOSE_WAIT
TCP   10.18.11.98:52806       104.19.195.151:https  ESTABLISHED
TCP   10.18.11.98:52808       ec2-34-198-122-35:https ESTABLISHED
TCP   10.18.11.98:52816       104.40.63.98:https    TIME_WAIT
TCP   10.18.11.98:52859       pfw:https              ESTABLISHED
TCP   10.18.11.98:52860       pfw:https              ESTABLISHED
TCP   10.18.11.98:52861       pfw:https              ESTABLISHED
TCP   10.18.11.98:52862       pfw:https              ESTABLISHED
TCP   10.18.11.98:52863       pfw:https              ESTABLISHED
TCP   10.18.11.98:52864       pfw:https              ESTABLISHED
TCP   10.18.11.98:52865       151.101.186.110:https ESTABLISHED
TCP   10.18.11.98:52866       bam-9:https            ESTABLISHED
TCP   10.18.11.98:52928       ord30s25-in-f14:https ESTABLISHED
TCP   10.18.11.98:52938       SCCM1:https            TIME_WAIT
TCP   10.18.11.98:52939       104.40.63.98:https    TIME_WAIT
TCP   10.18.11.98:52940       104.40.63.98:https    TIME_WAIT
TCP   10.18.11.98:52941       SCCM1:https            ESTABLISHED
TCP   10.18.11.98:52944       ord30s25-in-f10:https ESTABLISHED
TCP   10.18.11.98:52948       SCCM1:https            TIME_WAIT
TCP   10.18.11.98:52950       104.40.63.98:https    ESTABLISHED
TCP   10.18.11.98:52954       204.79.197.229:https  ESTABLISHED
TCP   10.18.11.98:52955       204.79.197.222:https  ESTABLISHED
TCP   10.18.11.98:52957       13.107.255.48:https   ESTABLISHED
TCP   10.18.11.98:52958       13.107.3.254:https    ESTABLISHED
TCP   10.18.11.98:52959       13.107.6.254:https    ESTABLISHED
TCP   10.18.11.98:52961       104.40.63.98:https    ESTABLISHED
TCP   10.18.11.98:52962       104.40.63.98:https    ESTABLISHED
TCP   [::1]:10122            6T2BND2:52759         ESTABLISHED
TCP   [::1]:52759            6T2BND2:10122         ESTABLISHED

C:\Users\vansam01>
```

Figure 1: Netstat Command Results

Why these results were obtained: The netstat command provides information and statistics about protocols in use and current TCP/IP network connections. TIME_WAIT indicates that local endpoint (this side) has closed the connection. The connection is being kept around so that any delayed packets can be matched to the connection and handled appropriately. CLOSE_WAIT indicates that the remote endpoint (other side of the connection) has closed the connection. Very good!

```
C:\Users\vansam01>netstat -e
Interface Statistics

                Received                Sent
Bytes           3656885284           373377544
Unicast packets 18953076                2401276
Non-unicast packets 8385148                3860
Discards        0                       0
Errors          0                       0
Unknown protocols 0
```

C:\Users\vansam01>

Figure 2: Netstat -e Command Results

Why these results were obtained: The netstat -e command provides information about Ethernet statistics. This information is always changing. This information was taken from the moment the connection was made

****Next Image Too Large To Fit Into This Space, Please See Next Page****

```
Command Prompt
C:\Users\vansam01>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.

C:\Users\vansam01>
```

Figure 3: Netsat ? Command Results

Why these results were obtained: The netstat ? command will display the netstat command syntax. This is helpful if the user forgets what command performs a certain action.

```

C:\Users\vansam01>netstat -rn
=====
Interface List
 2...48 4d 7e d5 12 01 .....Intel(R) Ethernet Connection (2) I219-LM
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.18.10.1       10.18.11.98      25
10.18.10.0                 255.255.254.0    On-link          10.18.11.98      281
10.18.11.98                255.255.255.255  On-link          10.18.11.98      281
10.18.11.255               255.255.255.255  On-link          10.18.11.98      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          10.18.11.98      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          10.18.11.98      281
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331  ::1/128                On-link
2    281  fe80::/64              On-link
2    281  fe80::a1d7:a023:22fa:b49/128
                                On-link
1    331  ff00::/8              On-link
2    281  ff00::/8              On-link
=====

Persistent Routes:
None

```

Figure 4: Netstat -rn Command Results

Why these results were obtained: The netstat -rn command displays the routing table and displays the addresses and port numbers in numerical form. Gateways listed as on-link, because they do not need to be routed. They are addresses that can be resolved locally. [Very good](#)

- **Activity 2B:**

```

C:\Users\vansam01>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

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

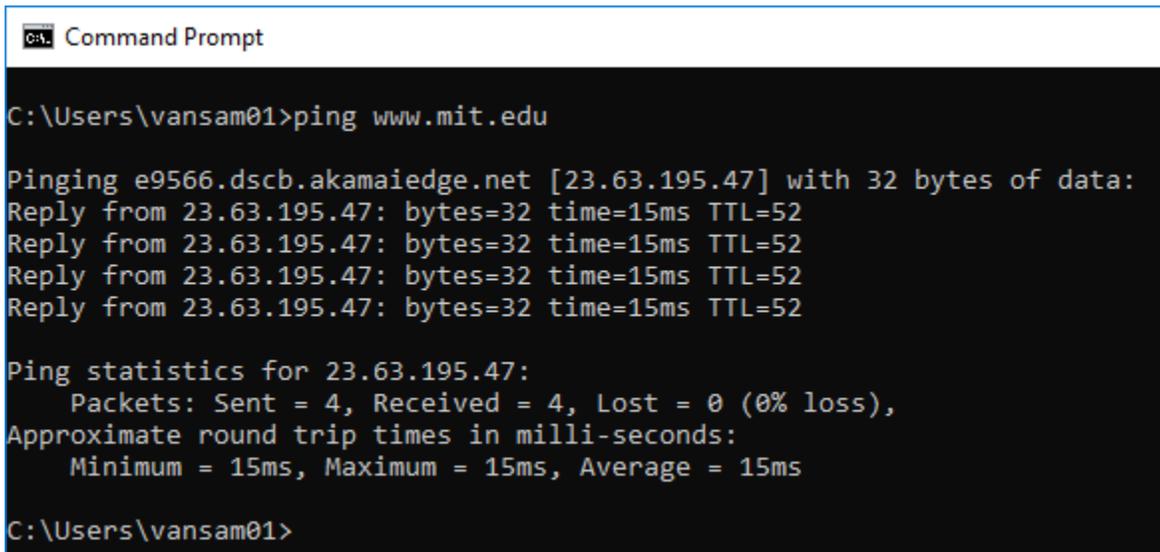
C:\Users\vansam01>

```

Figure 5: Ipconfig ? Command Results

Why these results were obtained: The ipconfig ? command will display the help page for using the ipconfig command. It shows all possible usages of ipconfig and what the command will d

- **Activity 2C:**



```
Command Prompt

C:\Users\vansam01>ping www.mit.edu

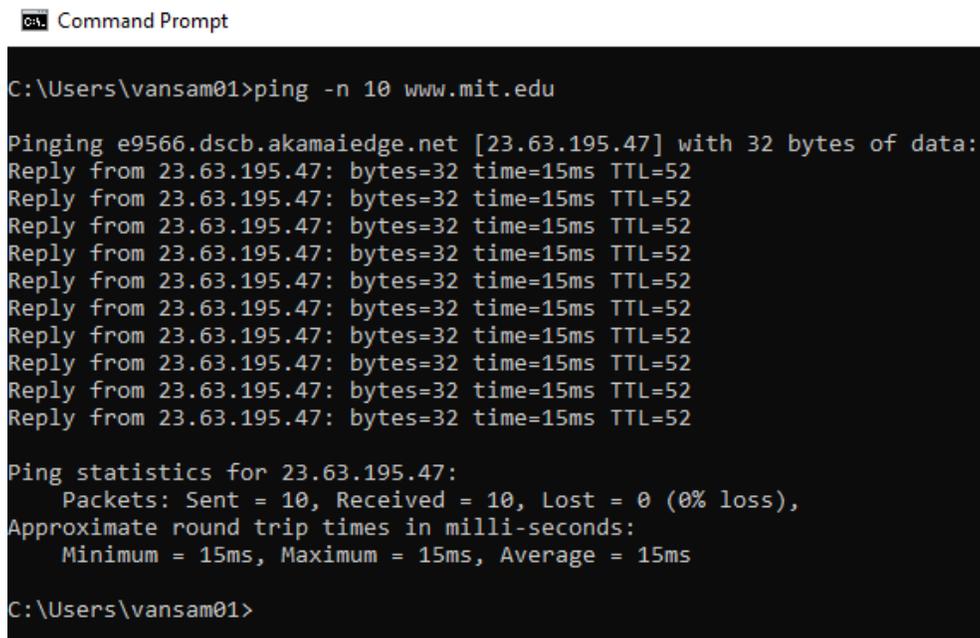
Pinging e9566.dscb.akamaiedge.net [23.63.195.47] with 32 bytes of data:
Reply from 23.63.195.47: bytes=32 time=15ms TTL=52

Ping statistics for 23.63.195.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 15ms, Average = 15ms

C:\Users\vansam01>
```

Figure 6: Ping www.mit.edu Command Results

Why these results were obtained: The ping command sent an Internet Control Message Protocol (ICMP) Echo Request message to the destination and waited for a response. Simply put, we verified that the computer can communicate to another computer over the network. The results state we sent four packets, all of which were received at an average of 15ms.



```
Command Prompt

C:\Users\vansam01>ping -n 10 www.mit.edu

Pinging e9566.dscb.akamaiedge.net [23.63.195.47] with 32 bytes of data:
Reply from 23.63.195.47: bytes=32 time=15ms TTL=52

Ping statistics for 23.63.195.47:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 15ms, Average = 15ms

C:\Users\vansam01>
```

Figure 7: Ping -n 10 www.mit.edu Command Results

Why these results were obtained: The ping -n 10 command was used so that we would receive a designated number of replies from www.mit.edu, in this case 10. The results state that we sent ten packets, all of which were received at an average of 15ms. Very good!

```
Command Prompt

C:\Users\vansam01>ping www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.53.232.243] with 32 bytes of data:
Reply from 23.53.232.243: bytes=32 time=14ms TTL=56

Ping statistics for 23.53.232.243:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 14ms, Average = 14ms

C:\Users\vansam01>
```

Figure 8: Ping www.microsoft.com Command Results

Why these results were obtained: The ping command sent an Internet Control Message Protocol (ICMP) Echo Request message to the destination and waited for a response. Simply put, we verified that the computer can communicate to another computer over the network. The results state we sent four packets, all of which were received at an average of 14ms. [Very good](#)

```
Command Prompt

C:\Users\vansam01>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=57ms TTL=46

Ping statistics for 164.67.228.152:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 57ms, Average = 57ms

C:\Users\vansam01>
```

Figure 9: Ping www.ucla.edu Command Results

Why these results were obtained: The ping command sent an Internet Control Message Protocol (ICMP) Echo Request message to the destination and waited for a response. Simply put, we verified that the computer can communicate to another computer over the network. The results state we sent four packets, all of which were received at an average of 57ms. The round trip time is quite longer than previous URLs as the packets had to be sent a great distance. [Very good](#)

```
CA Command Prompt
C:\Users\vansam01>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=7ms TTL=249

Ping statistics for 128.210.7.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 7ms, Average = 7ms

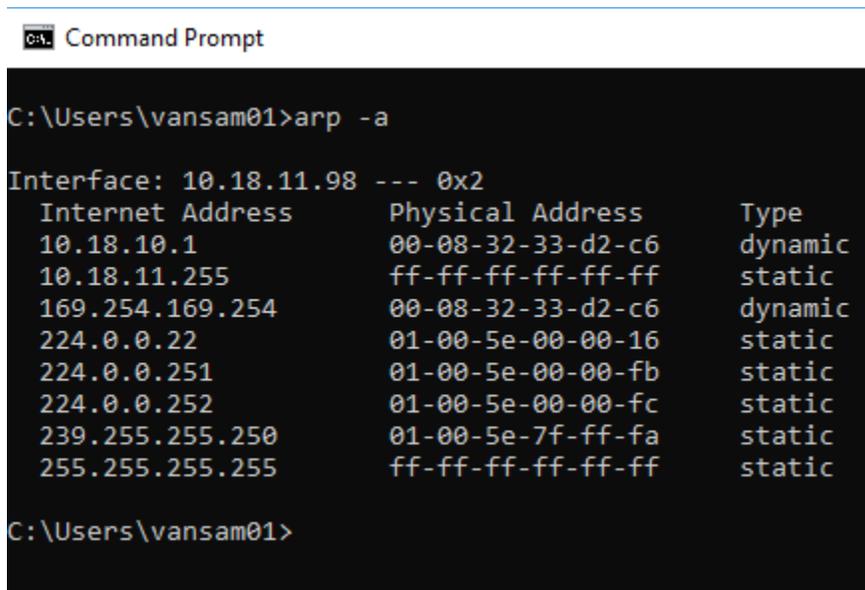
C:\Users\vansam01>
```

Figure 10: Ping www.purdue.edu Command Results

Why these results were obtained: The ping command sent an Internet Control Message Protocol (ICMP) Echo Request message to the destination and waited for a response. Simply put, we verified that the computer can communicate to another computer over the network. The results state we sent four packets, all of which were received at an average of 7ms. The fastest of all previous pings. This is due to the packets having to travel a much shorter distance. [Very good](#)

****Next Image Too Large To Fit Into This Space, Please See Next Page****

- **Activity 2D:**



```
Command Prompt
C:\Users\vansam01>arp -a
Interface: 10.18.11.98 --- 0x2
  Internet Address      Physical Address      Type
  10.18.10.1            00-08-32-33-d2-c6    dynamic
  10.18.11.255          ff-ff-ff-ff-ff-ff    static
  169.254.169.254       00-08-32-33-d2-c6    dynamic
  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
C:\Users\vansam01>
```

Figure 11: Arp -a Command Results

Why these results were obtained: The ARP command displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. Adding the -a, displays current ARP cache tables for all interfaces. [Very good](#)

****Next Image Too Large To Fit Into This Space, Please See Next Page****

- **Activity 2E:**

Note: The following command was too large to capture with the Snipping Tool. Results were copied and pasted

C:\Users\vansam01>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

Why these results were obtained: route command is used to view and manipulate the IP routing table in both Unix-like and Microsoft Windows operating systems.

*****Next Image Too Large To Fit Into This Space, Please See Next Page*****

```

C:\Users\vansam01>route print
=====
Interface List
 2...48 4d 7e d5 12 01 .....Intel(R) Ethernet Connection (2) I219-LM
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
 0.0.0.0                    0.0.0.0          10.18.10.1       10.18.11.98      25
 10.18.10.0                 255.255.254.0    On-link          10.18.11.98      281
 10.18.11.98                255.255.255.255  On-link          10.18.11.98      281
 10.18.11.255               255.255.255.255  On-link          10.18.11.98      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          10.18.11.98      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          10.18.11.98      281
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
 1   331  ::1/128                On-link
 2   281  fe80::/64              On-link
 2   281  fe80::a1d7:a023:22fa:b49/128
                                On-link
 1   331  ff00::/8               On-link
 2   281  ff00::/8               On-link
=====

Persistent Routes:
None

```

Figure 12: Route print Command Results

Why these results were obtained: Route print will print a rote. Since we did not define a specific route, all active routes were printed to the screen. Here we show eleven distinctive IPv4 routes and several IPv6 routes. Very good

```
Command Prompt
C:\Users\vansam01>route print -4
=====
Interface List
 2...48 4d 7e d5 12 01 .....Intel(R) Ethernet Connection (2) I219-LM
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.18.10.1       10.18.11.98      25
10.18.10.0                 255.255.254.0    On-link          10.18.11.98      281
10.18.11.98                255.255.255.255  On-link          10.18.11.98      281
10.18.11.255               255.255.255.255  On-link          10.18.11.98      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          10.18.11.98      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          10.18.11.98      281
=====
Persistent Routes:
None
```

Figure 13: Route print -4 Command Results

Why these results were obtained: Route print -4 will print routes, force using IPv4. Meaning, we only print the routes that are of IPv4.

```
Command Prompt
C:\Users\vansam01>route print -6
=====
Interface List
 2...48 4d 7e d5 12 01 .....Intel(R) Ethernet Connection (2) I219-LM
 1.....Software Loopback Interface 1
=====

IPv6 Route Table
=====
Active Routes:
  If Metric Network Destination      Gateway
  1     331  ::1/128           On-link
  2     281 fe80::/64         On-link
  2     281 fe80::a1d7:a023:22fa:b49/128
                                     On-link
  1     331 ff00::/8         On-link
  2     281 ff00::/8         On-link
=====

Persistent Routes:
None
```

Figure 14: Route print -6 Command Results

Why these results were obtained: Route print -6 will print routes, force using IPv6. Meaning, we only print the routes that are of IPv6.

- **Activity 2F:**

```

ca. Command Prompt

C:\Users\vansam01>tracert www.mit.edu

Tracing route to e9566.dscb.akamaiedge.net [23.79.196.238]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    10.18.10.1
  2   1 ms     1 ms     1 ms     192.168.18.254
  3  <1 ms    <1 ms    <1 ms    10.255.0.254
  4   1 ms     1 ms     1 ms     149.164.180.90
  5   7 ms     7 ms     7 ms     149.164.255.6
  6   8 ms     8 ms     9 ms     tel-210-c9006-01-te0-0-0-3.tcom.purdue.edu [192.5.40.65]
  7   9 ms     9 ms     9 ms     indiana-gigapop-ctc-internet-151.tcom.purdue.edu [192.5.40.82]
  8   9 ms     9 ms     9 ms     et-3-1-0.1235.rtr.ll.indiana.gigapop.net [64.57.21.174]
  9   9 ms     9 ms     9 ms     et-8-0-0.1235.rtsw.indi.net.internet2.edu [64.57.21.173]
 10  13 ms    13 ms    13 ms    ae-5.4079.rtsw.chic.net.internet2.edu [162.252.70.152]
 11  13 ms    13 ms    13 ms    ae-5.0.rtsw2.eqch.net.internet2.edu [64.57.20.109]
 12  14 ms    14 ms    14 ms    64.57.20.110
 13  14 ms    14 ms    14 ms    ae11.er1.ord7.us.zip.zayo.com [64.125.21.217]
 14  65 ms    79 ms    50 ms    208.184.110.254.IPYX-073920-910-ZY0.above.net [208.184.110.254]
 15  14 ms    14 ms    14 ms    a23-79-196-238.deploy.static.akamaitechnologies.com [23.79.196.238]

Trace complete.

```

Figure 15: Tracert www.mit.edu Command Results

Why these results were obtained: The tracert command is used to display the details of the path the packet takes to get from the send device to its destination. From our results, we show it took twelve paths, varying from under one millisecond to seventy-nine milliseconds to reach its intended destination. [Very good](#)

```

ca. Command Prompt

C:\Users\vansam01>tracert www.microsoft.com

Tracing route to e13678.dspb.akamaiedge.net [23.53.232.243]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    10.18.10.1
  2   2 ms     5 ms     7 ms     192.168.18.254
  3  <1 ms    <1 ms    <1 ms    10.255.0.254
  4   1 ms     1 ms     1 ms     149.164.180.90
  5   1 ms     1 ms     1 ms     50.235.241.85
  6   1 ms     1 ms     1 ms     68.86.188.253
  7   1 ms     <1 ms    <1 ms     96.108.120.5
  8   5 ms     5 ms     5 ms     96.108.120.65
  9  17 ms    16 ms    16 ms    be-3-ar01.area4.il.chicago.comcast.net [68.86.188.181]
 10  16 ms    16 ms    16 ms    be-1-ar01.elmhurst.il.chicago.comcast.net [69.139.200.233]
 11  15 ms    15 ms    15 ms    a23-53-232-243.deploy.static.akamaitechnologies.com [23.53.232.243]

Trace complete.

```

Figure 16: Tracert www.microsoft.com Command Results

Why these results were obtained: The tracert command is used to display the details of the path the packet takes to get from the send device to its destination. From our results, we show it took eleven paths. Varying from under one millisecond to seventeen milliseconds to reach its destination. [Very good](#)

CA. Command Prompt

```
C:\Users\vansam01>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  10.18.10.1
  2   2 ms   1 ms   1 ms  192.168.18.254
  3  <1 ms  <1 ms  <1 ms  10.255.0.254
  4   1 ms   1 ms   1 ms  149.164.180.90
  5   8 ms   7 ms   7 ms  149.164.255.6
  6   7 ms   7 ms   7 ms  itap-dc-core-vss-01-te1-3-1.tcom.purdue.edu [192.5.40.70]
  7   7 ms   7 ms   7 ms  www.purdue.edu [128.210.7.200]

Trace complete.
```

Figure 17: Tracert www.purdue.edu Command Results

Why these results were obtained: The tracert command is used to display the details of the path the packet takes to get from the send device to its destination. From our results, we show it took seven paths, varying from under one millisecond to eight milliseconds to reach its destination. [v](#)

CA. Command Prompt

```
C:\Users\vansam01>tracert www.iu.edu

Tracing route to www.iu.edu [129.79.78.189]
over a maximum of 30 hops:

  1   1 ms  <1 ms  <1 ms  10.18.10.1
  2   2 ms  10 ms   1 ms  192.168.18.254
  3  <1 ms  <1 ms  <1 ms  10.255.0.254
  4   8 ms   1 ms   1 ms  149.164.180.90
  5   7 ms   7 ms   9 ms  149.164.255.6
  6   8 ms   9 ms   8 ms  tel-210-c9006-01-te0-0-0-3.tcom.purdue.edu [192.5.40.65]
  7   9 ms   9 ms   9 ms  indiana-gigapop-ctc-internet2-150.tcom.purdue.edu [192.5.40.86]
  8   9 ms   9 ms   9 ms  et-7-1-0.1.rtr.ll.indiana.gigapop.net [149.165.255.194]
  9  11 ms  11 ms  11 ms  149.165.254.234
 10  34 ms  11 ms  11 ms  ae-33.932.dcr3.blc.net.uits.iu.edu [134.68.3.129]
 11  11 ms  11 ms  11 ms  zeus1-iu.gateway.indiana.edu [129.79.78.189]

Trace complete.
```

Figure 18: Tracert www.iu.edu Command Results

Why these results were obtained: The tracert command is used to display the details of the path the packet takes to get from the send device to its destination. From our results, we show it took eleven paths varying from under one millisecond to thirty-four millisecond to reach its destination. [v](#)

CONCLUSION:

Homework one taught vital information and training in relation to TCP/IP network monitoring and management command. Throughout the lab, the user is taught some of the more well-known commands such as netstat, ping, route, and tracert. The lab added great detail and attention to what each individual command does and what other sub-commands can be performed (netstat, netstat -e). The lab was useful in terms of an introduction to TCP/IP. It offers an insightful refresher to those who have experience within these commands, but also allows beginners to learn these commands at a very informative and relatively easy way.

The lab allowed the user to gain hands on experience entering ipconfig, tracert, ping, route, and netstat commands. It allowed the user to see the information that is produced from these commands in real time and allowed the user to interoperate the data. Allowing the user to enter this information for themselves allows them to be more immersed within the commands.

QUESTIONS/COMMENTS:

I intend to practice and explore the command prompt in more detail. There are far many more different commands and sub-commands that can be used that was not covered in this lab. I feel this would be of a great benefit to me, as I have little experience using commands and interpreting network related information.

[Excellent report!](#)

[100/100](#)



-Austin VanSumeren