**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](http://www.mit.edu)
    - Ping –n 10 [www.mit.edu](http://www.mit.edu)
    - Ping [www.microsoft.com](http://www.microsoft.com)
    - Ping [www.UCLA.edu](http://www.UCLA.edu)
    - Ping [www.purdue.edu](http://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](http://www.mit.edu)
    - Tracert [www.microsoft.edu](http://www.microsoft.edu)
    - Tracert [www.purdue.edu](http://www.purdue.edu)
    - Tracert www.iu.edu

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

**DATA:**

* **Activity 2A:**

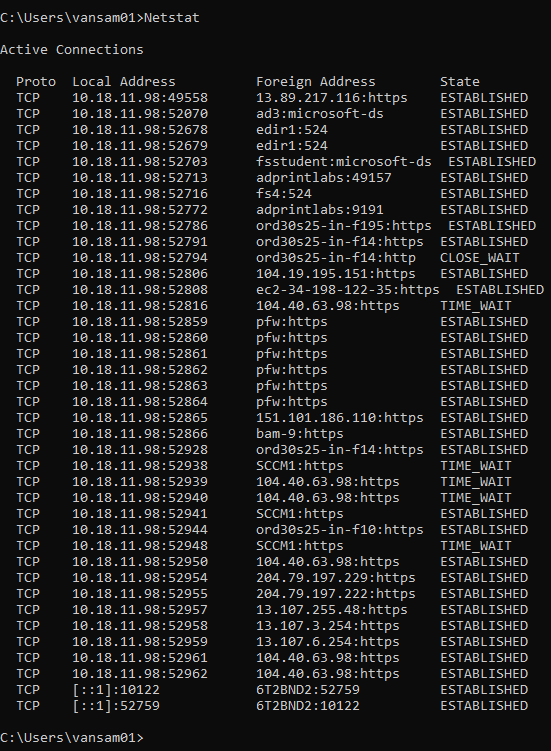


Figure 1: Netstat Command Results

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!

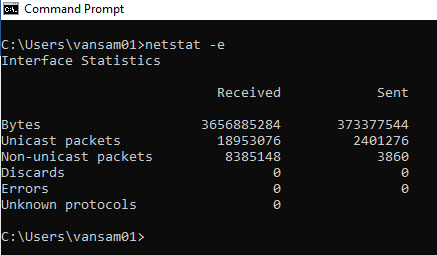


Figure 2: Netstat -e Command Results

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\*\****

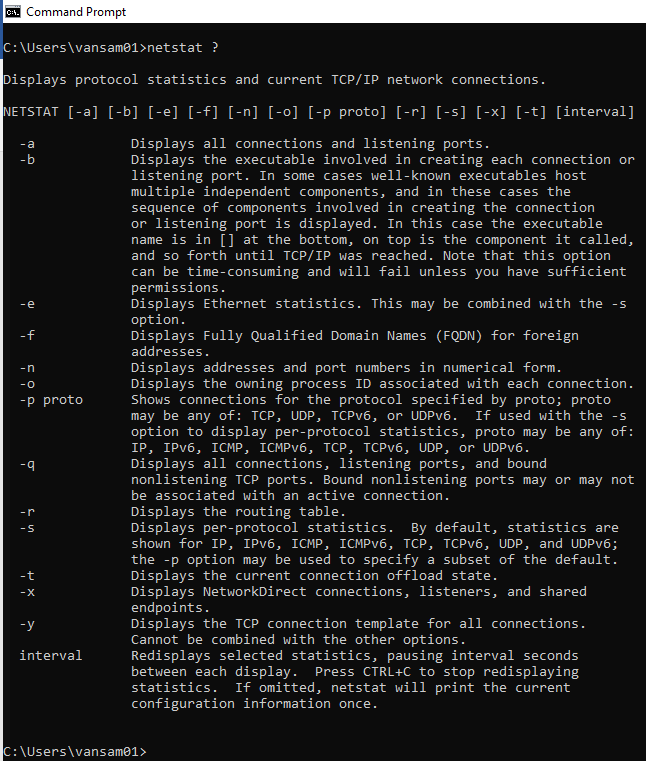


Figure 3: Netsat ? Command Results

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.

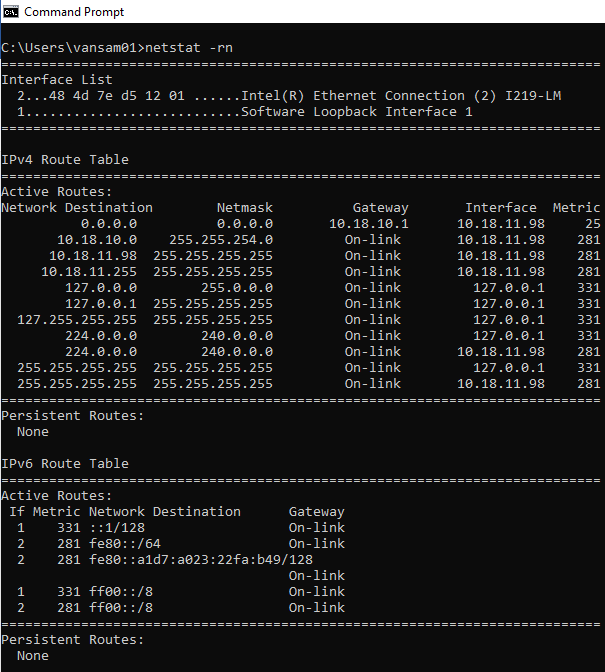


Figure 4: Netstat -rn Command Results

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 no need to be routed. They are addresses that can be resolved locally. Very good

* **Activity 2B:**

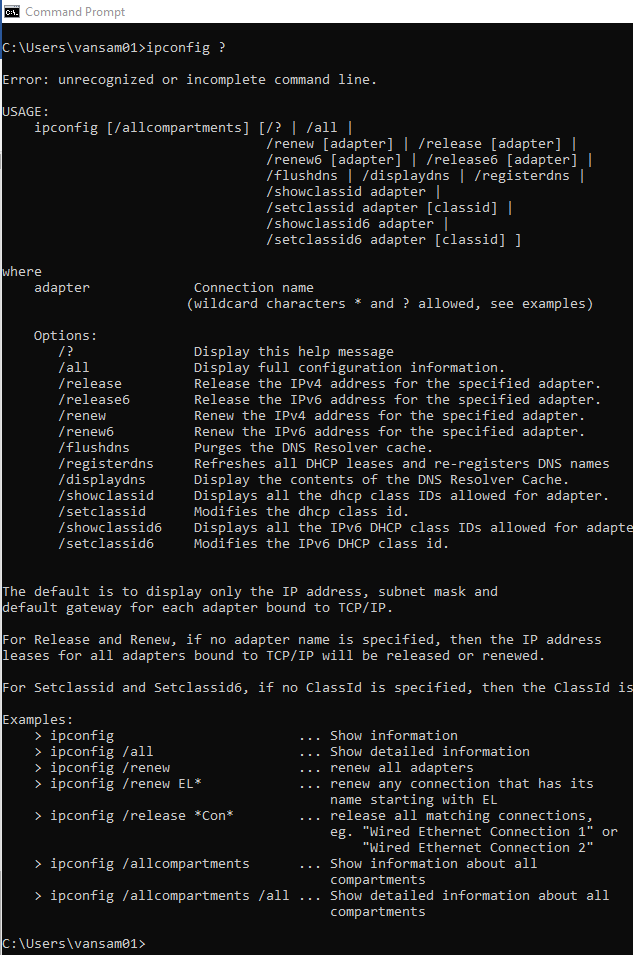


Figure 5: Ipconfig ? Command Results

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:**



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.

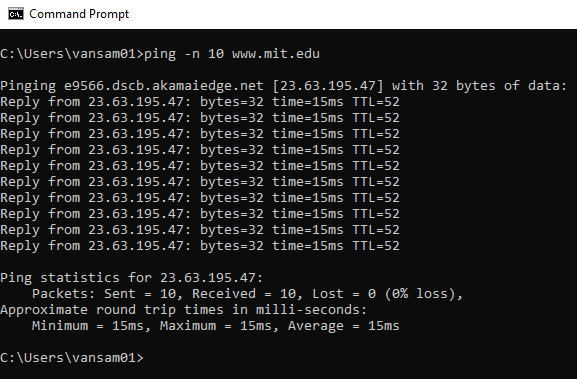


Figure 7: Ping -n 10 www.mit.edu Command Results

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!

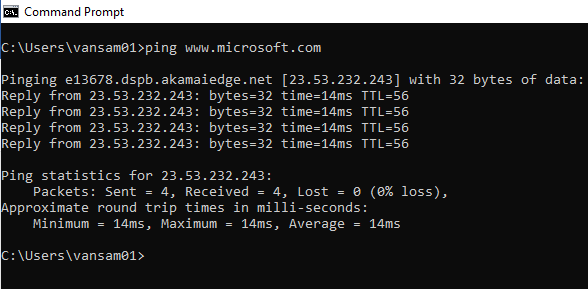


Figure 8: Ping www.microsoft.com Command Results

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

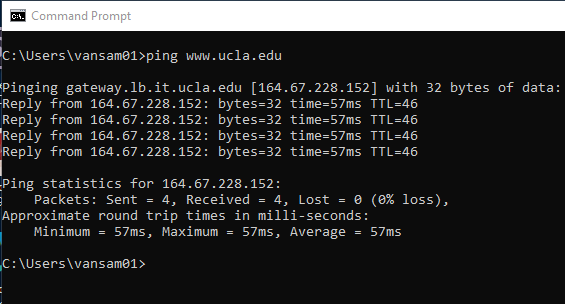


Figure 9: Ping www.ucla.edu Command Results

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

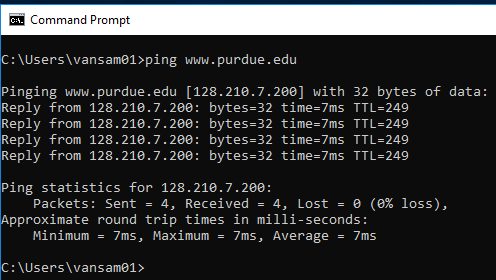


Figure 10: Ping www.purdue.edu Command Results

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:**

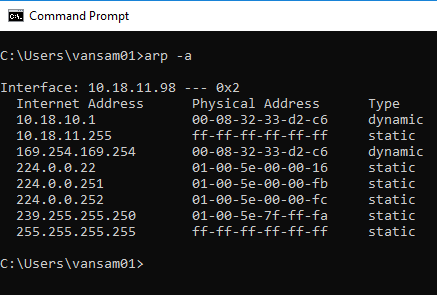


Figure 11: Arp -a Command Results

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\*\****

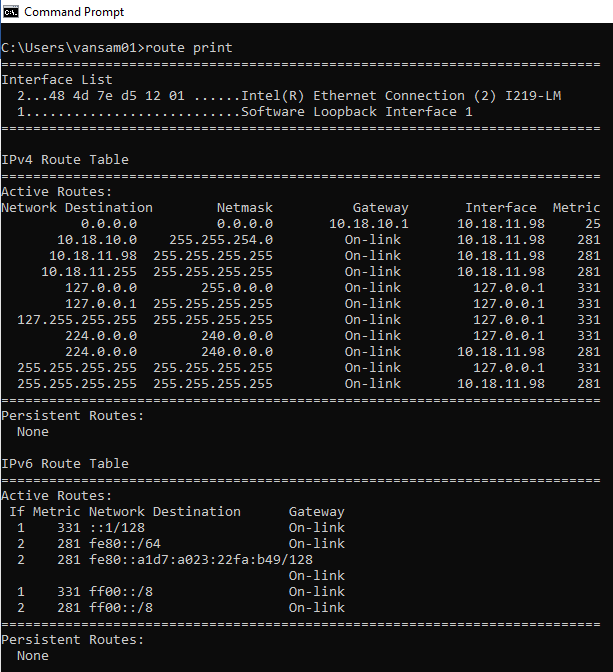


Figure 12: Route print Command Results

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

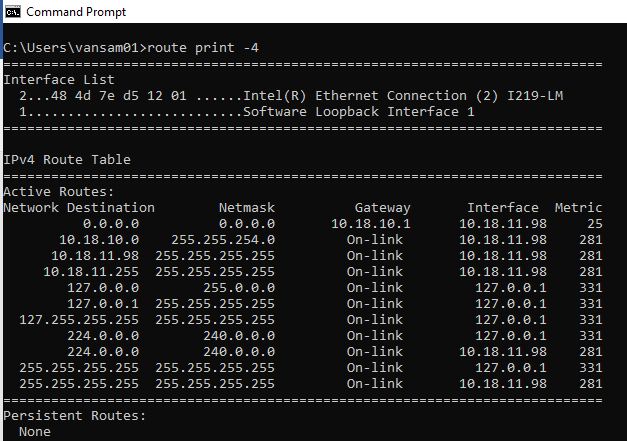


Figure 13: Route print -4 Command Results

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

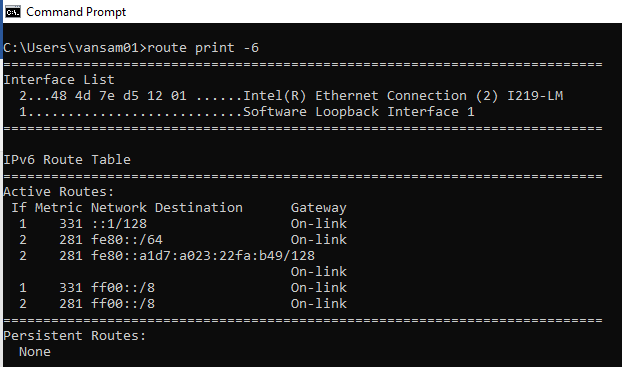


Figure 14: Route print -6 Command Results

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

* **Activity 2F:**

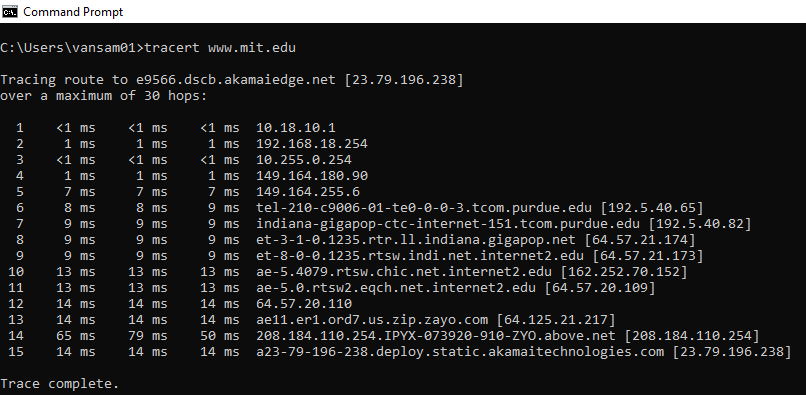


Figure 15: Tracert www.mit.edu Command Results

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

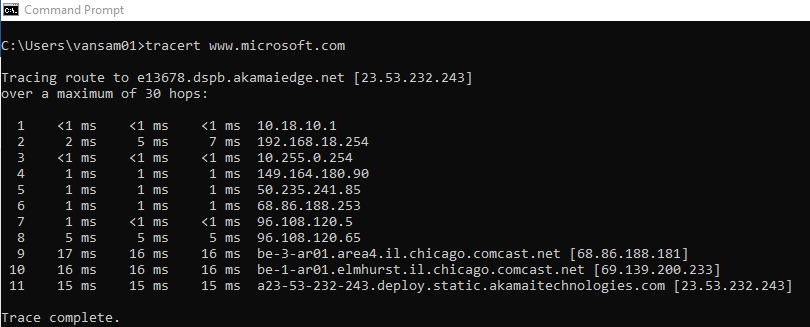


Figure 16: Tracert www.microsoft.com Command Reults

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

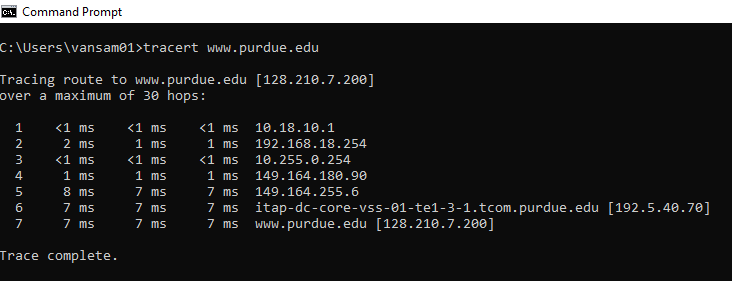


Figure 17: Tracert www.purdue.edu Command Results

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

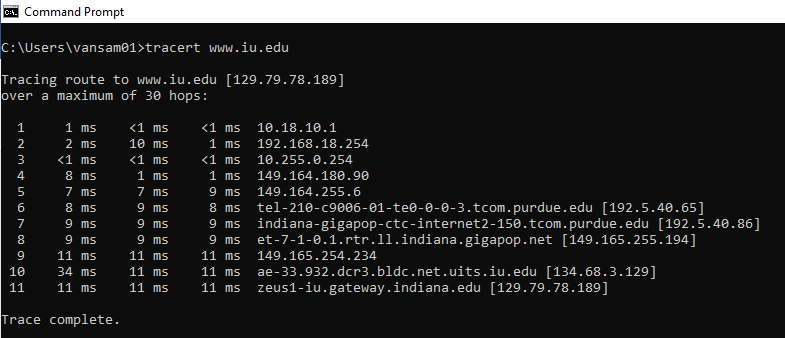


Figure 18: Tracert www.iu.edu Command Results

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