

HOMEWORK 1 LAB ACTIVITY

TCP/IP NETWORK MONITORING AND MANAGEMENT

ITC 250/CPET 499

PROFESSOR PAUL LIN



September 7, 2018

Jared Meyer

## **Objective:**

One objective for this lab is to research, investigate, and compare three different network analyzers with one another. Another objective is to utilize a series of commands to monitor traffic, display and obtain up to date network information, and troubleshoot network related issues. Lastly, to understand what the information obtained means and to have fun discovering what lies in the world of TCP/IP network monitoring and management. Very good

## **Equipment/Parts List:**

**Equipment, very good**

* NP8235 (CLEVO P151SM1) SAGER Laptop
  + The above was used during this lab
* Ethernet Cable (RJ-45, CAT5e) or Wireless Adapter (802.11n)
  + An Ethernet connection was used during this lab
* Internet Service Provider (for live connection to the Internet)
  + Modem-Router to be assumed
  + Internet service was provided by OnlyInternet.net during this lab
* Peripherals (Optional)
  + Wired or Wireless Mouse
  + Wired or Wireless Keyboard

**Software/Applications**

* Windows 7, Windows 8, Windows 8.1, or Windows 10
  + Windows 8.1 was used during this lab
* Word Processing Software
  + Microsoft Office 2013/2016 Professional Plus (Option #1)
    - Office 365 (Option #2)
  + Libre Office (Option #3)
  + OpenOffice (Option #4)
  + Google Docs (Option #5)
* Internet Explorer, Google Chrome, or Mozilla Firefox for browsing
* Command Prompt

## **Block Diagram/Schematics:**

Not applicable.

## **Procedure:**

For Activity 1 of this lab, you are first required to find a “network analyzer” for the CIO of a small company of about 200 employees. The CIO would like the results of your research to be presented in a professional-looking table. The catch is that you must find at least three different products, provide a feature comparison, and a recommendation for the order.

To start, we recommend starting your research from a reputable database with peer reviewed journals such as ebscohost. If you do not have access to such a database, the use of the Google search engine found at [www.google.com](http://www.google.com) is sufficient. To obtain the best results, you should search for “network analyzer”, “network analyzer comparison”, or “best network analyzer”. Note that you may find a mixture of both software based and network based network analyzers. For this lab, we chose to further investigate software based network analyzers and refined our results by adding the words “software-based” to our search. Recommended hosts for such information include TechRepublic, CIO, TechCrunch, TechRadar, and any university based pages you might find. After discovering and investigating several software-based network analyzers, document as many key features as you can for each to be displayed in your table.

To create your table to be presented to the CIO, it is probably best to use a word processing software such as Microsoft Office 2013/2016, Libre Office, or Google Docs. No matter which is chosen, a neat table containing the type of network analyzers, the names of each, and features of each can be designed. To make a table using Microsoft Office 2016, click on the Insert at the top, click the Table icon, and use the mouse to choose how many columns and rows you’d like the table to start with. After clicking in a cell, use CTRL+E to center the text, CTRL+B to bold the text, and click Home > Bullets to create a bulleted list. The overall design and number of rows and columns is left to your discretion. Afterward, remember to prepare a brief summary as to which network analyzer you recommend and why. Very detailed, excellent.

For Activity 2 of this lab, you are required to explore several network management commands, run them, and document your results. To start, you will open Command Prompt by opening the start menu and typing in “command prompt” or “cmd” or push Windows Key + R, type in cmd.exe, and hit enter. In Activity 2A, you will utilize and explore the command “netstat” which displays protocol statistics and current TCP/IP network connections. You are to enter the commands “netstat”, “netstat -e”, “netstat ?”, and “netstat -rn” one at a time and document the results of each. In Activity 2B, you are to utilize and explore the “ipconfig” command. Enter the “ipconfig ?” command to show all its options then document the information. Next, visit <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>, use the “ipconfig” command with all the options listed, then write a short summary regarding lessons learned. For Activity 2C, you will use the “ping” command to test your network connection to a few sites. First you will ping [www.mit.edu](http://www.mit.edu) by typing “ping [www.mit.edu](http://www.mit.edu)” into Command Prompt, then “ping -n 10 [www.mit.edu](http://www.mit.edu)” to test the connection 10 times as opposed to 4. Next, you will ping [www.microsoft.com](http://www.microsoft.com), [www.ucla.edu](http://www.ucla.edu), & [www.purdue.edu](http://www.purdue.edu). Lastly, record the results and do your best to explain them. In Activity 2D, you will enter “arp -a” into the Command Prompt, document the results, and explain them. You are also to read about ARP at <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/arp> and write up a short summary. For Activity 2E, you are to explore the “route” command by entering “route”, “route print”, “route print -4”, and “route print -6” into the Command Prompt, record all results, and explain them. In Activity 2F, you are to run the “tracert” command against [www.mit.edu](http://www.mit.edu), [www.microsoft.com](http://www.microsoft.com), [www.purdue.edu](http://www.purdue.edu), & [www.iu.edu](http://www.iu.edu), document the outcomes, and describe them. Excllent.

## **Data:**

Activity 1

Question 1:

|  |  |
| --- | --- |
| **Software-Based Network Analyzers** | |
| **Software Name** | **Features** |
| Wireshark  https://www.wireshark.org | * Deep inspection of hundreds of protocols, with more being added all the time * Live capture and offline analysis * Standard three-pane packet browser * Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others * Captured network data can be browsed via a gUI, or via the TTY-mode TShark utility * The most powerful display filters in the industry * Rich VoiP analysis * Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult, DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer (compressed and uncompressed), Sniffer Pro, and NetXray, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, Wild Packets EtherPeek/TokenPeek/AiroPeek, and many others * Capture files compressed with gzip can be decompressed on the fly * Live data can be read fro Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others * Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2 * Coloring rules can be applied to the packet list for quick, intuitive analysis * Output can be exported to XML, PostScript, CSV, or plain text |
| Zenmap  https://nmap.org/zenmap | * Multi-platform: Runs on Windows, Linux, Mac OS X, and BSD * Live capture and offline analysis * Host Discovery * Port Scanning * Version Detection * OS Detection * Scriptable Interface * Web Scanning * Full IPv6 Support * Nping Support * Output exported to XML |
| Angry IP Scanner  http://angryip.org/ | * Multi-platform: Runs on Windows, Linux, and Mac OS X * Portable (zero installation on certain platforms) * Ping checks * NetBIOS information * Resolves hostnames * Determines MAC address * Determines currently logged-in user * Plug-in system * Output can be saved as CSV, TXT, XML, or IP-Port list |

Rich in features, support, and years of wisdom, Wireshark is the recommended software-based network analyzer. Wireshark offers compatibility with the most platforms, does everything one could desire out of a network analyzer and in the future might do more, and provides a variety of output methods for offline analysis. Excellent!

Activity 2 Network Management Commands

Activity 2A:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.1.9:49186 it-in-f125:5222 ESTABLISHED

TCP 192.168.1.9:49188 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49189 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49191 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49198 64.4.54.253:https TIME\_WAIT

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -e

Interface Statistics

Received Sent

Bytes 1798840 379564

Unicast packets 2560 2036

Non-unicast packets 260 480

Discards 0 0

Errors 0 0

Unknown protocols 0

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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.

-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.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -rn

===========================================================================

Interface List

8...48 d2 24 6a 38 81 ......Microsoft Wi-Fi Direct Virtual Adapter #2

7...48 d2 24 6a 38 81 ......Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC

4...48 d2 24 6a 62 57 ......Bluetooth Device (Personal Area Network)

3...00 90 f5 ec 1d 80 ......Realtek PCIe GBE Family Controller

1...........................Software Loopback Interface 1

9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.9 10

127.0.0.0 255.0.0.0 On-link 127.0.0.1 306

127.0.0.1 255.255.255.255 On-link 127.0.0.1 306

127.255.255.255 255.255.255.255 On-link 127.0.0.1 306

192.168.1.0 255.255.255.0 On-link 192.168.1.9 266

192.168.1.9 255.255.255.255 On-link 192.168.1.9 266

192.168.1.255 255.255.255.255 On-link 192.168.1.9 266

224.0.0.0 240.0.0.0 On-link 127.0.0.1 306

224.0.0.0 240.0.0.0 On-link 192.168.1.9 266

255.255.255.255 255.255.255.255 On-link 127.0.0.1 306

255.255.255.255 255.255.255.255 On-link 192.168.1.9 266

===========================================================================

Persistent Routes:

None

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 306 ::1/128 On-link

1 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -a

Active Connections

Proto Local Address Foreign Address State

TCP 0.0.0.0:135 Vehement8:0 LISTENING

TCP 0.0.0.0:445 Vehement8:0 LISTENING

TCP 0.0.0.0:3389 Vehement8:0 LISTENING

TCP 0.0.0.0:5357 Vehement8:0 LISTENING

TCP 0.0.0.0:49152 Vehement8:0 LISTENING

TCP 0.0.0.0:49153 Vehement8:0 LISTENING

TCP 0.0.0.0:49154 Vehement8:0 LISTENING

TCP 0.0.0.0:49155 Vehement8:0 LISTENING

TCP 0.0.0.0:49156 Vehement8:0 LISTENING

TCP 0.0.0.0:49157 Vehement8:0 LISTENING

TCP 192.168.1.9:139 Vehement8:0 LISTENING

TCP 192.168.1.9:49186 it-in-f125:5222 ESTABLISHED

TCP 192.168.1.9:49188 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49189 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49191 ord30s22-in-f106:https CLOSE\_WAIT

TCP [::]:135 Vehement8:0 LISTENING

TCP [::]:445 Vehement8:0 LISTENING

TCP [::]:3389 Vehement8:0 LISTENING

TCP [::]:5357 Vehement8:0 LISTENING

TCP [::]:49152 Vehement8:0 LISTENING

TCP [::]:49153 Vehement8:0 LISTENING

TCP [::]:49154 Vehement8:0 LISTENING

TCP [::]:49155 Vehement8:0 LISTENING

TCP [::]:49156 Vehement8:0 LISTENING

TCP [::]:49157 Vehement8:0 LISTENING

TCP [::1]:49195 Vehement8:0 LISTENING

UDP 0.0.0.0:3389 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:5355 \*:\*

UDP 0.0.0.0:51143 \*:\*

UDP 0.0.0.0:54608 \*:\*

UDP 0.0.0.0:63540 \*:\*

UDP 127.0.0.1:1900 \*:\*

UDP 127.0.0.1:51142 \*:\*

UDP 192.168.1.9:137 \*:\*

UDP 192.168.1.9:138 \*:\*

UDP 192.168.1.9:1900 \*:\*

UDP 192.168.1.9:51141 \*:\*

UDP [::]:3389 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:51144 \*:\*

UDP [::]:54609 \*:\*

UDP [::]:63541 \*:\*

UDP [::1]:1900 \*:\*

UDP [::1]:51140 \*:\*

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -e

Interface Statistics

Received Sent

Bytes 18077532 1109460

Unicast packets 14536 9288

Non-unicast packets 768 492

Discards 0 0

Errors 0 0

Unknown protocols 0

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -n

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.1.9:49186 64.233.183.125:5222 ESTABLISHED

TCP 192.168.1.9:49188 216.58.216.106:443 CLOSE\_WAIT

TCP 192.168.1.9:49189 216.58.216.106:443 CLOSE\_WAIT

TCP 192.168.1.9:49191 216.58.216.106:443 CLOSE\_WAIT

TCP 192.168.1.9:49226 64.4.54.253:443 ESTABLISHED

TCP 192.168.1.9:49229 64.4.54.254:443 ESTABLISHED

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -p TCP

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.1.9:49186 it-in-f125:5222 ESTABLISHED

TCP 192.168.1.9:49188 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49189 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49191 ord30s22-in-f106:https CLOSE\_WAIT

TCP 192.168.1.9:49226 64.4.54.253:https TIME\_WAIT

TCP 192.168.1.9:49229 64.4.54.254:https TIME\_WAIT

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -r

===========================================================================

Interface List

8...48 d2 24 6a 38 81 ......Microsoft Wi-Fi Direct Virtual Adapter #2

7...48 d2 24 6a 38 81 ......Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC

4...48 d2 24 6a 62 57 ......Bluetooth Device (Personal Area Network)

3...00 90 f5 ec 1d 80 ......Realtek PCIe GBE Family Controller

1...........................Software Loopback Interface 1

9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.9 10

127.0.0.0 255.0.0.0 On-link 127.0.0.1 306

127.0.0.1 255.255.255.255 On-link 127.0.0.1 306

127.255.255.255 255.255.255.255 On-link 127.0.0.1 306

192.168.1.0 255.255.255.0 On-link 192.168.1.9 266

192.168.1.9 255.255.255.255 On-link 192.168.1.9 266

192.168.1.255 255.255.255.255 On-link 192.168.1.9 266

224.0.0.0 240.0.0.0 On-link 127.0.0.1 306

224.0.0.0 240.0.0.0 On-link 192.168.1.9 266

255.255.255.255 255.255.255.255 On-link 127.0.0.1 306

255.255.255.255 255.255.255.255 On-link 192.168.1.9 266

===========================================================================

Persistent Routes:

None

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 306 ::1/128 On-link

1 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -f

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.1.9:49186 it-in-f125.1e100.net:5222 ESTABLISHED

TCP 192.168.1.9:49188 ord30s22-in-f106.1e100.net:https CLOSE\_WAIT

TCP 192.168.1.9:49189 ord30s22-in-f106.1e100.net:https CLOSE\_WAIT

TCP 192.168.1.9:49191 ord30s22-in-f106.1e100.net:https CLOSE\_WAIT

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved

C:\Windows\system32>netstat -s

IPv4 Statistics

Packets Received = 3990

Received Header Errors = 0

Received Address Errors = 0

Datagrams Forwarded = 0

Unknown Protocols Received = 0

Received Packets Discarded = 42

Received Packets Delivered = 4068

Output Requests = 2573

Routing Discards = 0

Discarded Output Packets = 13

Output Packet No Route = 4

Reassembly Required = 0

Reassembly Successful = 0

Reassembly Failures = 0

Datagrams Successfully Fragmented = 0

Datagrams Failing Fragmentation = 0

Fragments Created = 0

IPv6 Statistics

Packets Received = 0

Received Header Errors = 0

Received Address Errors = 0

Datagrams Forwarded = 0

Unknown Protocols Received = 0

Received Packets Discarded = 0

Received Packets Delivered = 20

Output Requests = 30

Routing Discards = 0

Discarded Output Packets = 0

Output Packet No Route = 2

Reassembly Required = 0

Reassembly Successful = 0

Reassembly Failures = 0

Datagrams Successfully Fragmented = 0

Datagrams Failing Fragmentation = 0

Fragments Created = 0

ICMPv4 Statistics

Received Sent

Messages 6 6

Errors 0 0

Destination Unreachable 6 6

Time Exceeded 0 0

Parameter Problems 0 0

Source Quenches 0 0

Redirects 0 0

Echo Replies 0 0

Echos 0 0

Timestamps 0 0

Timestamp Replies 0 0

Address Masks 0 0

Address Mask Replies 0 0

Router Solicitations 0 0

Router Advertisements 0 0

ICMPv6 Statistics

Received Sent

Messages 0 0

Errors 0 0

Destination Unreachable 0 0

Packet Too Big 0 0

Time Exceeded 0 0

Parameter Problems 0 0

Echos 0 0

Echo Replies 0 0

MLD Queries 0 0

MLD Reports 0 0

MLD Dones 0 0

Router Solicitations 0 0

Router Advertisements 0 0

Neighbor Solicitations 0 0

Neighbor Advertisements 0 0

Redirects 0 0

Router Renumberings 0 0

TCP Statistics for IPv4

Active Opens = 73

Passive Opens = 7

Failed Connection Attempts = 1

Reset Connections = 15

Current Connections = 4

Segments Received = 3565

Segments Sent = 2311

Segments Retransmitted = 12

TCP Statistics for IPv6

Active Opens = 2

Passive Opens = 2

Failed Connection Attempts = 0

Reset Connections = 0

Current Connections = 0

Segments Received = 28

Segments Sent = 28

Segments Retransmitted = 0

UDP Statistics for IPv4

Datagrams Received = 575

No Ports = 43

Receive Errors = 0

Datagrams Sent = 313

UDP Statistics for IPv6

Datagrams Received = 39

No Ports = 0

Receive Errors = 0

Datagrams Sent = 20

Activity 2B:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . . . . . . . : 192.168.1.9

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . . . . . . . . : Vehement8

Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2

Physical Address. . . . . . . . . : 48-D2-24-6A-38-81

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Description . . . . . . . . . . . : Realtek RTL8723AE Wireless LAN 802.11n PC

I-E NIC

Physical Address. . . . . . . . . : 48-D2-24-6A-38-81

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)

Physical Address. . . . . . . . . : 48-D2-24-6A-62-57

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller

Physical Address. . . . . . . . . : 00-90-F5-EC-1D-80

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IPv4 Address. . . . . . . . . . . : 192.168.1.9(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : Thursday, September 7, 2017 2:25:15 PM

Lease Expires . . . . . . . . . . : Friday, September 8, 2017 2:25:14 PM

Default Gateway . . . . . . . . . : 192.168.1.1

DHCP Server . . . . . . . . . . . : 192.168.1.1

DNS Servers . . . . . . . . . . . : 192.168.1.1

NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Microsoft ISATAP Adapter

Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection\* 4 while it has its media

disconnected.

No operation can be performed on Wi-Fi while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its m

edia disconnected.

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . . . . . . . : 192.168.1.9

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

C:\Windows\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection\* 4 while it has its media

disconnected.

No operation can be performed on Wi-Fi while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its m

edia disconnected.

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media unoperational

Connection-specific DNS Suffix . :

C:\Windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection\* 4 while it has its media

disconnected.

No operation can be performed on Wi-Fi while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its m

edia disconnected.

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . . . . . . . : 192.168.1.9

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection\* 4 while it has its media

disconnected.

No operation can be performed on Wi-Fi while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its m

edia disconnected.

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Default Gateway . . . . . . . . . :

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection\* 4 while it has its media

disconnected.

No operation can be performed on Wi-Fi while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its m

edia disconnected.

Wireless LAN adapter Local Area Connection\* 4:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . : ad.ipfw.edu

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . . . . . . . : 192.168.1.9

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{5FA56701-5382-4EA7-90E4-419427221F88}:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

accounts.google.com

----------------------------------------

Record Name . . . . . : accounts.google.com

Record Type . . . . . : 1

Time To Live . . . . : 207

Data Length . . . . . : 4

Section . . . . . . . : Answer

A (Host) Record . . . : 172.217.4.237

talk.google.com

----------------------------------------

Record Name . . . . . : talk.google.com

Record Type . . . . . : 5

Time To Live . . . . : 149

Data Length . . . . . : 8

Section . . . . . . . : Answer

CNAME Record . . . . : talk.l.google.com

Record Name . . . . . : talk.l.google.com

Record Type . . . . . : 1

Time To Live . . . . : 149

Data Length . . . . . : 4

Section . . . . . . . : Answer

A (Host) Record . . . : 64.233.183.125

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has b

een initiated. Any errors will be reported in the Event Viewer in 15 minutes.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /showclassid \*

Windows IP Configuration

Unable to modify the DHCPv4 class id for adapter Local Area Connection\* 4: The s

ystem cannot find the file specified.

Unable to modify the DHCPv4 class id for adapter Wi-Fi: The system cannot find t

he file specified.

Unable to modify the DHCPv4 class id for adapter Bluetooth Network Connection: T

he system cannot find the file specified.

There are no DHCPv4 classes defined for Ethernet.

Unable to modify the DHCPv4 class id for adapter Loopback Pseudo-Interface 1: Th

e system cannot find the file specified.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /setclassid \*

Windows IP Configuration

Attempt to set the DHCPv4 class id for adapter Local Area Connection\* 4 failed:

The system cannot find the file specified.

Attempt to set the DHCPv4 class id for adapter Wi-Fi failed: The system cannot f

ind the file specified.

Attempt to set the DHCPv4 class id for adapter Bluetooth Network Connection fail

ed: The system cannot find the file specified.

Successfully set the DHCPv4 class id for adapter Ethernet.

The command “ipconfig” can be used to display all current TCP/IP network configuration information, refresh DHCP and DNS settings, and more. As a result, it is a very important tool to keep in mind when troubleshooting a variety of networking issues. Good

Activity 2C:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping www.mit.edu

Pinging e9566.dscb.akamaiedge.net [23.4.112.131] with 32 bytes of data:

Reply from 23.4.112.131: bytes=32 time=45ms TTL=55

Reply from 23.4.112.131: bytes=32 time=54ms TTL=55

Reply from 23.4.112.131: bytes=32 time=56ms TTL=55

Reply from 23.4.112.131: bytes=32 time=38ms TTL=55

Ping statistics for 23.4.112.131:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 38ms, Maximum = 56ms, Average = 48ms

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping -n 10 www.mit.edu

Pinging e9566.dscb.akamaiedge.net [23.4.112.131] with 32 bytes of data:

Reply from 23.4.112.131: bytes=32 time=34ms TTL=55

Reply from 23.4.112.131: bytes=32 time=44ms TTL=55

Reply from 23.4.112.131: bytes=32 time=55ms TTL=55

Reply from 23.4.112.131: bytes=32 time=86ms TTL=55

Reply from 23.4.112.131: bytes=32 time=78ms TTL=55

Reply from 23.4.112.131: bytes=32 time=36ms TTL=55

Reply from 23.4.112.131: bytes=32 time=44ms TTL=55

Reply from 23.4.112.131: bytes=32 time=33ms TTL=55

Reply from 23.4.112.131: bytes=32 time=36ms TTL=55

Reply from 23.4.112.131: bytes=32 time=44ms TTL=55

Ping statistics for 23.4.112.131:

Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 33ms, Maximum = 86ms, Average = 49ms

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping www.microsoft.com

Pinging e1863.dspb.akamaiedge.net [23.222.72.232] with 32 bytes of data:

Reply from 23.222.72.232: bytes=32 time=33ms TTL=55

Reply from 23.222.72.232: bytes=32 time=30ms TTL=55

Reply from 23.222.72.232: bytes=32 time=35ms TTL=55

Reply from 23.222.72.232: bytes=32 time=38ms TTL=55

Ping statistics for 23.222.72.232:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 30ms, Maximum = 38ms, Average = 34ms

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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=99ms TTL=47

Reply from 164.67.228.152: bytes=32 time=102ms TTL=47

Reply from 164.67.228.152: bytes=32 time=94ms TTL=47

Reply from 164.67.228.152: bytes=32 time=101ms TTL=47

Ping statistics for 164.67.228.152:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 94ms, Maximum = 102ms, Average = 99ms

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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=40ms TTL=244

Reply from 128.210.7.200: bytes=32 time=30ms TTL=244

Reply from 128.210.7.200: bytes=32 time=31ms TTL=244

Reply from 128.210.7.200: bytes=32 time=22ms TTL=244

Ping statistics for 128.210.7.200:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 22ms, Maximum = 40ms, Average = 30ms

The results obtained from running the “ping” command show that I had a sufficient connection to the variety of web servers and that each was online and accessible. There were a few spikes in the latency to some of the servers, but the difference was negligible. The “-n 10” in “ping -n 10 [www.mit.edu](http://www.mit.edu)” tells the “ping” command to run a test 10 times. Any number can be positioned after the “-n” in the command to run that many tests. Very good

Activity 2D:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a

Interface: 192.168.1.9 --- 0x3

Internet Address Physical Address Type

192.168.1.1 2c-30-33-a4-ab-20 dynamic

192.168.1.6 44-8a-5b-b8-a6-7f dynamic

192.168.1.10 4c-cc-6a-8a-66-52 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 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

The “arp” command displays and modified entries in the Address Resolution Protocol (ARP) cache. The Address Resolution Protocol cache contains one or more tables used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. The “arp -a” command displays current ARP cache tables for all interfaces. I had a few known IP addresses at the time because the network interfaces on my laptop were configured for DHCP. Very good!

Activity 2E:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>route print

===========================================================================

Interface List

8...48 d2 24 6a 38 81 ......Microsoft Wi-Fi Direct Virtual Adapter #2

7...48 d2 24 6a 38 81 ......Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC

4...48 d2 24 6a 62 57 ......Bluetooth Device (Personal Area Network)

3...00 90 f5 ec 1d 80 ......Realtek PCIe GBE Family Controller

1...........................Software Loopback Interface 1

9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.9 10

127.0.0.0 255.0.0.0 On-link 127.0.0.1 306

127.0.0.1 255.255.255.255 On-link 127.0.0.1 306

127.255.255.255 255.255.255.255 On-link 127.0.0.1 306

192.168.1.0 255.255.255.0 On-link 192.168.1.9 266

192.168.1.9 255.255.255.255 On-link 192.168.1.9 266

192.168.1.255 255.255.255.255 On-link 192.168.1.9 266

224.0.0.0 240.0.0.0 On-link 127.0.0.1 306

224.0.0.0 240.0.0.0 On-link 192.168.1.9 266

255.255.255.255 255.255.255.255 On-link 127.0.0.1 306

255.255.255.255 255.255.255.255 On-link 192.168.1.9 266

===========================================================================

Persistent Routes:

None

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 306 ::1/128 On-link

1 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>route print -4

===========================================================================

Interface List

8...48 d2 24 6a 38 81 ......Microsoft Wi-Fi Direct Virtual Adapter #2

7...48 d2 24 6a 38 81 ......Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC

4...48 d2 24 6a 62 57 ......Bluetooth Device (Personal Area Network)

3...00 90 f5 ec 1d 80 ......Realtek PCIe GBE Family Controller

1...........................Software Loopback Interface 1

9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.9 10

127.0.0.0 255.0.0.0 On-link 127.0.0.1 306

127.0.0.1 255.255.255.255 On-link 127.0.0.1 306

127.255.255.255 255.255.255.255 On-link 127.0.0.1 306

192.168.1.0 255.255.255.0 On-link 192.168.1.9 266

192.168.1.9 255.255.255.255 On-link 192.168.1.9 266

192.168.1.255 255.255.255.255 On-link 192.168.1.9 266

224.0.0.0 240.0.0.0 On-link 127.0.0.1 306

224.0.0.0 240.0.0.0 On-link 192.168.1.9 266

255.255.255.255 255.255.255.255 On-link 127.0.0.1 306

255.255.255.255 255.255.255.255 On-link 192.168.1.9 266

===========================================================================

Persistent Routes:

None

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>route print -6

===========================================================================

Interface List

8...48 d2 24 6a 38 81 ......Microsoft Wi-Fi Direct Virtual Adapter #2

7...48 d2 24 6a 38 81 ......Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC

4...48 d2 24 6a 62 57 ......Bluetooth Device (Personal Area Network)

3...00 90 f5 ec 1d 80 ......Realtek PCIe GBE Family Controller

1...........................Software Loopback Interface 1

9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

===========================================================================

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 306 ::1/128 On-link

1 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

The “route” command displays and modifies entries in the local IP routing table. Adding the “print” parameter to the command prints a route or routes. Adding “-4” to the “route print” command will print the IPv4 Route Table and adding “-6” to the “route print” command will print out the IPv6 Route Table. Very good

Activity 2F:

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert www.mit.edu

Tracing route to e9566.dscb.akamaiedge.net [23.4.112.131]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.1.1

2 94 ms 27 ms 17 ms 198.18.4.24

3 15 ms 11 ms 11 ms 72-42-196-137.rev.omnicity.net [72.42.196.137]

4 14 ms 17 ms 16 ms 72-42-196-145.rev.omnicity.net [72.42.196.145]

5 28 ms 20 ms 38 ms 72-42-196-101.rev.omnicity.net [72.42.196.101]

6 27 ms 24 ms 240 ms 98-158-72-61.rev.omnicity.net [98.158.72.61]

7 44 ms 33 ms 50 ms 98-158-72-1.rev.omnicity.net [98.158.72.1]

8 54 ms 42 ms 44 ms 216.176.4.186

9 49 ms 50 ms 46 ms akamai.indatelservices.com [216.176.4.62]

10 46 ms 87 ms 34 ms a23-4-112-131.deploy.static.akamaitechnologies.c

om [23.4.112.131]

Trace complete.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert www.microsoft.com

Tracing route to e1863.dspb.akamaiedge.net [23.222.72.232]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.1.1

2 36 ms 19 ms 5 ms 198.18.4.24

3 37 ms 12 ms 15 ms 72-42-196-137.rev.omnicity.net [72.42.196.137]

4 14 ms 21 ms 13 ms 72-42-196-145.rev.omnicity.net [72.42.196.145]

5 16 ms 23 ms 13 ms 72-42-196-101.rev.omnicity.net [72.42.196.101]

6 30 ms 26 ms 33 ms 98-158-72-61.rev.omnicity.net [98.158.72.61]

7 23 ms 38 ms 40 ms 98-158-72-1.rev.omnicity.net [98.158.72.1]

8 64 ms 36 ms 53 ms 216.176.4.186

9 47 ms 61 ms 52 ms akamai.indatelservices.com [216.176.4.62]

10 39 ms 50 ms 58 ms a23-222-72-232.deploy.static.akamaitechnologies.

com [23.222.72.232]

Trace complete.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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 192.168.1.1

2 10 ms 11 ms 11 ms 198.18.4.24

3 38 ms 10 ms 11 ms 72-42-196-137.rev.omnicity.net [72.42.196.137]

4 18 ms 23 ms 40 ms 72-42-196-145.rev.omnicity.net [72.42.196.145]

5 21 ms 27 ms 23 ms 72-42-196-101.rev.omnicity.net [72.42.196.101]

6 51 ms 21 ms 31 ms 98-158-72-61.rev.omnicity.net [98.158.72.61]

7 42 ms 39 ms 40 ms 98-158-72-1.rev.omnicity.net [98.158.72.1]

8 43 ms 44 ms 40 ms 206.53.139.33

9 58 ms 19 ms 19 ms indiana-university-co-indiana-gigapop.10gigabite

thernet12-5.core1.ind1.he.net [184.105.35.194]

10 23 ms 50 ms 55 ms tel-210-c9006-01-te0-0-0-0-151.tcom.purdue.edu [

192.5.40.81]

11 29 ms 27 ms 30 ms itap-dc-core-vss-01-te2-3-1.tcom.purdue.edu [192

.5.40.90]

12 29 ms 27 ms 25 ms 128.210.7.200

Trace complete.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>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 192.168.1.1

2 15 ms 5 ms 10 ms 198.18.4.24

3 15 ms 12 ms 147 ms 72-42-196-137.rev.omnicity.net [72.42.196.137]

4 39 ms 27 ms 12 ms 72-42-196-145.rev.omnicity.net [72.42.196.145]

5 25 ms 21 ms 25 ms 72-42-196-101.rev.omnicity.net [72.42.196.101]

6 32 ms 90 ms 58 ms 98-158-72-61.rev.omnicity.net [98.158.72.61]

7 33 ms 38 ms 25 ms 98-158-72-1.rev.omnicity.net [98.158.72.1]

8 48 ms 28 ms 32 ms 206.53.139.33

9 21 ms 31 ms 42 ms indiana-university-co-indiana-gigapop.10gigabite

thernet12-5.core1.ind1.he.net [184.105.35.194]

10 36 ms 32 ms 31 ms ae-4.12.rtr.ll.indiana.gigapop.net [149.165.183.

13]

11 25 ms 37 ms 61 ms tge-1-2.12.br.hper.net.uits.iu.edu [149.165.183.

14]

12 27 ms 32 ms 42 ms ae-33.932.dcr3.bldc.net.uits.iu.edu [134.68.3.12

9]

13 23 ms 66 ms 30 ms zeus1-iu.gateway.indiana.edu [129.79.78.189]

Trace complete.

The “tracert” command determines the path taken to a destination by sending ICMP echo request messages to the destination with incrementally TTL field values and displays the information in the Command Prompt. Like the “ping” command, “tracert” can be used to troubleshoot various networking issues, such as high latency to a World of Warcraft server. Very good

## **Conclusion:**

The TCP/IP Network Monitoring and Management lab is a good way to introduce individuals to the Command Prompt. It does an excellent job of demonstrating the importance of the simple yet powerful “netstat”, “ipconfig”, “ping”, “arp”, “route”, and “tracert” commands in networking. It also encourages the investigation and use of network analyzer tools to be used for a variety of reasons.

**Excellent!**

## **Questions:**

1. Activity 1
   1. You are asked by the CIO of a small company of less than 200 employees to find a “network analyzer”. Search the Internet for at least three products (can be software-based or hardware-based), create a table to show a feature comparison of at least three products, and prepare your recommendation for the order.
2. Activity 2
   1. Activity 2A
      1. Enter the following commands:
         1. netstat
         2. netstat -e
         3. netstat ?
         4. netstat -rn
         5. Enter proper commands for the following networking of your computer and copy all display results to your report:
            1. Displays all connections and listening ports of your computer, also find the HTTP connection port
            2. Display your computer’s Ethernet statistics
            3. Display address and port number of your own computer in numerical format
            4. Show connections for the protocol specified by TCP protocol
            5. Show routing table that stored in your computer
            6. Display fully Qualified Domain Names for foreign addresses
            7. Display per-protocol statistics
   2. Activity 2B
      1. Type ipconfig ? to show all command options; then copy all display results to your activity report
      2. Use ipconfig command with all the provided options, <https://technet.microsoft.com/en-us/library/bb490921.aspx>
      3. Write a short summary of lesson learned.
   3. Activity 2C
      1. Enter the following commands, copy all the display results to your activity report, and explain what results are obtained.
         1. ping [www.mit.edu](http://www.mit.edu)
         2. ping -n 10 [www.mit.edu](http://www.mit.edu)
         3. ping [www.microsoft.com](http://www.microsoft.com)
         4. ping [www.ucla.edu](http://www.ucla.edu)
         5. ping [www.purdue.edu](http://www.purdue.edu)
   4. Activity 2D
      1. Enter the following commands, copy all the display results to your activity report, and explain what results are obtained.
         1. arp -a
         2. Read ARP found at Microsoft Web site and prepare a short summary: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/arp.mspx?mfr=true>
   5. Activity 2E
      1. Enter the following commands, copy the display results, and explain what results are obtained.
         1. route
         2. route print
         3. route print -4
         4. route print -6
   6. Activity 2F
      1. Enter the following commands, copy the display results, and explain what results are obtained:
         1. tracert [www.mit.edu](http://www.mit.edu)
         2. tracert [www.microsoft.edu](http://www.microsoft.edu)
         3. tracert [www.purdue.edu](http://www.purdue.edu)
         4. tracert [www.iu.edu](http://www.iu.edu)

Grade 100/100