Homework 3
TCP/IP Network Monitoring and Management

Hw3 Assigned on 2013/9/13, Due 2013/9/24

Hand-In Requirement

- Prepare a activity/laboratory report (name it **Hw3_WebSys.docx**) using the ECET Lab report guideline found at http://www.etcs.ipfw.edu/~lin/InfoForAllCourses/laboratoryreport.htm; make sure that you copy all activity/question and results in the DATA section
- Due September 24, 2013 as an email attachment

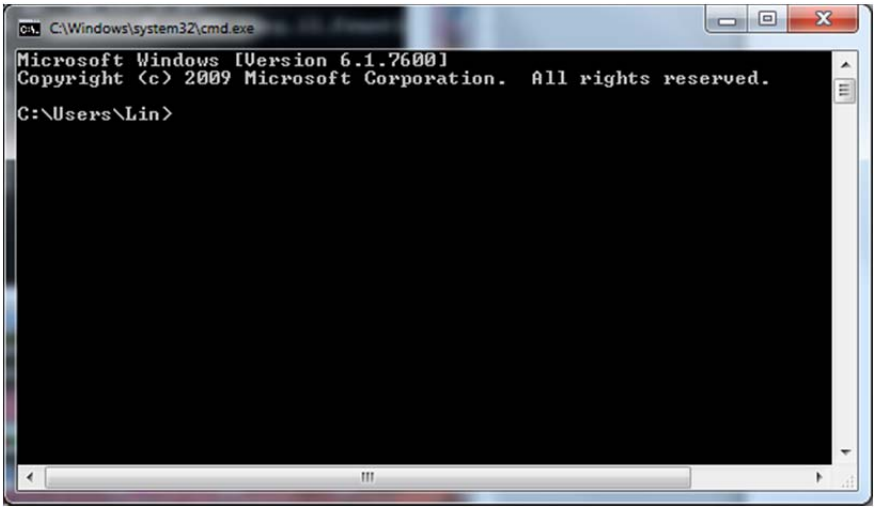
TCP/IP network management tasks include

- Traffic monitoring
- Troubleshooting network access
- Adding new hosts (also known as nodes or stations) to the network
- Mounting remote disks and exporting local disks with Network File System (NFS)

Large networks probably need a commercial network analyzer, or at least a hardware tester such as a time domain refelctometer (TDR). But many smaller networks can get by with publicly available free tools. A list of diagnostic service functions for helping network monitoring, management, and troubleshooting are as shown below.

- Testing the network connection: **ping** command (for both Windows and UNIX)
- Troubleshooting Network Access using: **winipcfg** command (Windows), **ifconfig** (UNIX), **netstat**, and **arp** command
- Configure the network interface: **winipcfg** command (Windows), and **ifconfig** (UNIX)
- Network monitoring: **netstat** command (for both Windows and UNIX)
- Display active network connections: **netstat** command (for both Windows and UNIX)
- Display interface statistics: **netstat** command (for both Windows and UNIX)
- Display active routes of connections: **route** command (for both Windows and UNIX)
- Manipulate static routing tables: **route** command (for both Windows and UNIX)
- Tracing routes: **tracert** command (Windows), **traceroute** command (UNIX)

For a Windows 7 or Windows 8-based PC, these commands are available from the "command prompt" which is available by clicking on the **window icon** (located at the lower left **taskbar** of the Windows Desktop), and enter **command** or **cmd**; and you will see the Windows's Command Window similar to the one below:



Activity 1/Question 1: You are asked by the CIO of a small company of less than 200 employees to find a "network analyzer" with a budget of about $3,000. 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. Network Management Commands

NETSTAT Command

The **netstat** command can be used to check network configuration and monitor a system's TCP/IP network activity. It will provide a variety of information on how much and what kind of network activity is going on.

The **netstat** command syntax can be found by entering the following command under the MS Command Prompt (an example of Windows 7 machine):

C:\Users\Lin>netstat ?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-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.
  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.
```

Activity 2/Question 2: Enter the following commands

- **netstat**

- **netstat ?**
- **netstat -rn**
- Enter proper commands for the following networking information of your computer, and copy all display results to your activity report:
    - Displays all connections and listening ports of your computer, also find the HTTP connection port.
    - Display your computer's Ethernet statistics
    - Display address and port number of your own computer in numerical format
    - Show connections for the protocol specified by TCP protocol
    - Show routing table that stored in your computer
    - Display fully Qualified Domain Names for foreign addresses
    - Display per-protocol statistics

IPCONFIG Command

To detect bad IP addresses, incorrect subnet masks, and improper broadcast addresses, the **ipconfig** command can be used to obtain a copy of basic configuration of the interface.
The winipcfg command can also be used for changing setup of the network adapter. We note that if the LAN consists of a single Ethernet network, no explicit routing is usually needed.

Activity 3/Question 3:

- Type **ipconfig ?** to show all command options; then copy all display results to your activity report.
- Read "How to use **winipcfg** to view TCP/IP settings? (http://support.microsoft.com/kb/141698)" and View "Using IPCONFIG in Windows 7," http://www.youtube.com/watch?v=ztXB9EjGh70; and write a short summary of lesson learned.

Ping Command

The ping command verifies whether a remote host can be reached. It also shows statistic about packet loss and delivery time. The **ping** command is design for troubleshooting and tracking a single-point hardware or software failure in the Internet. When called, the ping command sends one datagram per second and print one line of output for every ECHO_RESPONSE returned; it sends a message to the designated host and then informs you whether the message was successfully transmitted.

This command is designed for use in network testing, measurement, and management. It was originally used in the UNIX-based networks to see if a remote host is up and responding, and for manual fault isolation. However, it is also found in the Windows based computer systems. The Windows version of ping command is as listed below:

C:\Users\Lin\Documents>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:

```
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Head
```

```
er).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

The LINUX version of ping command can be obtained by typing the command at the command line.
[lin@paullinux lin]$ ping

usage: ping [-LRdfnqrv] [-c count] [-i wait] [-l preload]
[-p pattern] [-s packetsize] [-t ttl] [-I interface address] host
[lin@paullinux lin]$ ping -c 10 www.mit.edu
PING DANDELION-PATCH.MIT.EDU (18.181.0.31): 56 data bytes
64 bytes from 18.181.0.31: icmp_seq=0 ttl=242 time=59.0 ms
64 bytes from 18.181.0.31: icmp_seq=1 ttl=242 time=45.6 ms
64 bytes from 18.181.0.31: icmp_seq=2 ttl=242 time=48.6 ms
64 bytes from 18.181.0.31: icmp_seq=3 ttl=242 time=50.4 ms
64 bytes from 18.181.0.31: icmp_seq=4 ttl=242 time=47.5 ms
64 bytes from 18.181.0.31: icmp_seq=5 ttl=242 time=65.8 ms
64 bytes from 18.181.0.31: icmp_seq=6 ttl=242 time=54.7 ms
64 bytes from 18.181.0.31: icmp_seq=7 ttl=242 time=48.5 ms
64 bytes from 18.181.0.31: icmp_seq=8 ttl=242 time=51.6 ms
64 bytes from 18.181.0.31: icmp_seq=9 ttl=242 time=48.9 ms

--- DANDELION-PATCH.MIT.EDU ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 45.6/52.0/65.8 ms

Activity 4/Question 4: Enter the following commands, copy all the display results to your activity report, and explain what 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

ARP (Address Resolution Protocol) Command

The ARP command provides information about Ethernet/IP address translation. We can use it to detect systems on the local network that are configured with the wrong IP address.

C:\Users\Lin\Documents>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

```
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
```

```
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

Activity 5/Question 5: Enter the following commands, copy all the display results to your activity report, and explain what results are obtained.

- arp –a
- 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

ROUTE Command

Static routing:
It may be used for small to medium-sized networks not characterized by many redundant paths to most destinations. This can be setup by issuing explicit **route** commands. The route command can be found in both UNIX and Window computers. Some versions of the **route** command will also display the current routing tables.

Activity 6/Question 6: Enter the following commands, copy the display results, and explain what results are obtained:

- route
- route print
- route print -4
- route print -6

Tracing Route
The command for telling us which route packets take going from our system to a remote system is **tracert** (Windows) or **traceroute** (UNIX). It prints information about each hop.

C:\Users\Lin\Documents>tracert

```
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
```

```
-h maximum_hops     Maximum number of hops to search for target.
-j host-list        Loose source route along host-list (IPv4-only).
-w timeout          Wait timeout milliseconds for each reply.
-R                  Trace round-trip path (IPv6-only).
-S srcaddr          Source address to use (IPv6-only).
-4                  Force using IPv4.
-6                  Force using IPv6.
```

Activity 7/Question 7: Enter the following commands, copy the display results, and explain what results are obtained:

- tracert www.mit.edu
- tracert www.microsoft.edu
- tracert www.purdue.edu
- tracert www.iu.edu