Hands On Activities: TCP/IP Network Monitoring and Management

1. TCP/IP Network Management Tasks

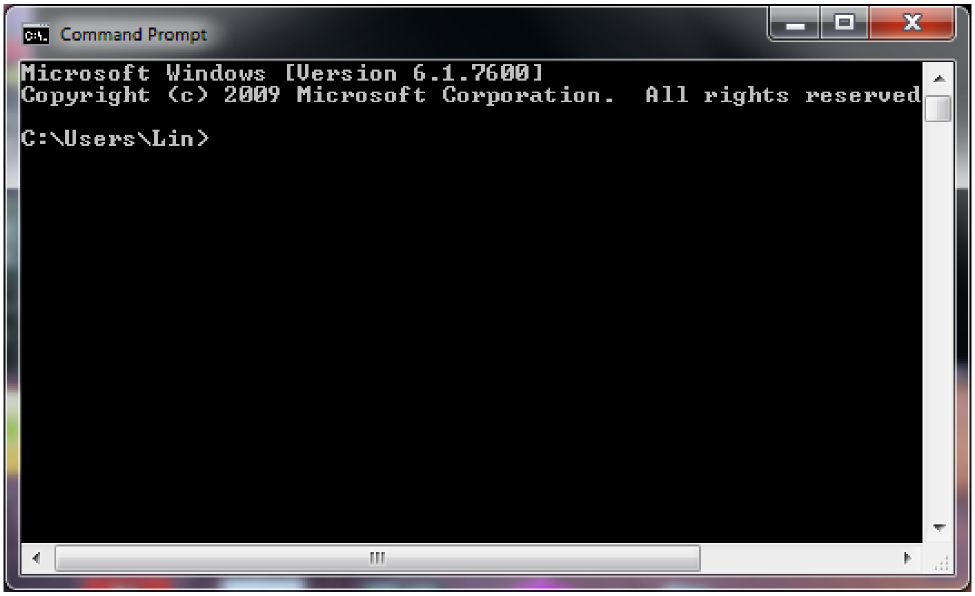
TCP/IP network management tasks include
- Examine your physical and IP network address
- Traffic monitoring
- Troubleshooting network access
- Adding new hosts (also known as nodes or stations) to the network

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 (Windows): **ipconfig**, **netstat**, and **arp** commands
- 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)
- Tracing routes: **tracert** command (Windows), **traceroute** command (UNIX)

For Windows XP/Vista/7-based PC, these commands are located in the C:\Windows subdirectory and they are designed as MS-DOS programs so that we can only run them under the MSDOS prompt.

Click **Start** (located at the left bottom of your PC), Enter **com** or **command** to start Command Prompt window similar to the one below (from Windows 7):



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved

C:\Users\Lin>
```

2. Window XP/Vista/7 Command-Line Utilities for Network Management

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 **ipconfig** 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.

```
C:\Users\Lin>ipconfig /?

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. "Local Area Connection 1" or
                                             "Local Area Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                         compartments
```

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 systems. The Windows version of ping command is as listed below:

```
C:\Users\YourName>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] destination-list

Options:
    -t             Ping the specified host until interrupted.
    -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.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each
reply.
```

ARP 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.

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```
C:\Users\YourName>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.
```

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. Under Windows, the **netstat** command syntax can be found by entering the following command under the MS-DOS prompt

```
C:\Users\YourName>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.
```

TRACERT 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 95/98/2000 and Windows NT systems. Some versions of the **route** command will also display the current routing tables.

```
C:\Users\YourName>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.
```

ROUTE Command

```
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. This
               option is not supported in Windows 95.

  -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
Dynamic routing:
The optimal paths to destination are determines at packet transmission time.
```

3. Monitoring Activities

A. Testing the network connection - PING

Try the following commands under the MS-DOS Window, and interpret the results:

```
C:\Users\YourName\>ping www.ipfw.edu
C:\Users\YourName\>ping www.google.com
C:\Users\YourName\>ping www.yahoo.com
C:\Users\YourName\>ping www.bing.com
C:\ Users\YourName\> ping cs.purdue.edu
```

B. Tracing Route - TRACERT

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

Enter the hollowing commands and obtain tracing route results:

```
C:\Users\YourName\>tracert www.ipfw.edu
C:\ Users\YourName\>tracert www.google.com
C:\ Users\YourName\>tracert www.yahoo.com
C:\ Users\YourName\>tracert www.bing.com
C:\ Users\YourName\>tracert cs.purdue.edu
```

C. Configure the Network Interface with ipconfig (Windows)

Use **ipconfig** command to obtain a copy of network interface address information: Host name, MAC address, IP address, default gateway, other network connection info etc.

Enter the following command, to see one screen at a time of your computer, then hit SPACE bar until all info are displayed:

```
C:\ Users\YourName\>ipconfig /all | more
```

D. Display Active Network Connections

D-1. Enter the **netstat** command, without arguments, to list all active network connections with your computer (the local host).

```
C:\ Users\YourName\>netstat
```

We then launch a new connection Internet site, then check the network activities by issuing the **netstat** command again see what happen.

```
C:\ Users\YourName\>netstat
```

D-2. If you provide the -a flag in addition, sockets that are waiting for a connection (i.e. listening) are displayed as well. This will give you a list of all servers that are currently running on your system. This shows most servers simply waiting for an incoming connection.

- Enter the command

```
C:\ Users\YourName\>netstat -a
```

D-3. Displaying Interface Statistics

When invoked with the -e flag, netstat will display statistics for the network interfaces currently configured.

- Enter the command:

```
C:\ Users\YourName \>netstat -e
```

D-4. Display Routing Tables

- Enter the following command to obtain a copy of routing tables setup for your networked PC:

```
C:\Users\YourName\>netstat -rn
```