LAB # 2

DIAGNOSTIC UTILITIES

# Objective

To learn how to use some Diagnostic Utilities for Computer Networks

# Theory

Following table gives the descriptions of different diagnostic Utilities

|  |  |
| --- | --- |
| Diagnostics Utility | **Functions** |
| IPCONFIG | Verifies a TCP/IP configuration, including DHCP, DNS, and WINS server addresses. |
| FINGER | Retrieves system information from a remote computer that supports the TCP/IP Finger service. |
| NSLOOKUP | Examines entries in the DNS database that pertain to a particular host or domain. |
| HOSTNAME | Returns the local computer’s hostname for authentication. |
| NETSTAT | Displays protocol statistics and the current state of TCP/IP connections. |
| NBTSTAT | Check the state of current NetBIOS over TCP/IP connections, updates the LMHOSTS cache, or determines your registered name &scope ID. |
| Route | Views or modifies the local routing table |
| Tracert | Verifies the route used from the local host to a remote host. |

## Ping: Verify connections to a remote computer or computers

### Theory

The ping command verifies connections to remote computer or computers, by sending ICMP echo packets to the computer and listening for echo reply packets. Ping waits for up to 1 second for each packet sent and prints the number of packets transmitted and received. Each received packet is validated against the transmitted message. By default, four echo packets containing 64 bytes of data (a periodic uppercase sequence of alphabetic characters) are transmitted.

You can use the ping utility to test both the computer name and the IP address of the computer. If the IP address is verified but the computer name is not, you may have a name resolution problem. In this case, be sure that the computer name you are querying is in either the local HOSTS file or in the DNS database.

### Parameters

-t Pings the specified computer until interrupted

-a resolve addresses to computer names.

-n count Sends the number of ECHO packets specified by count. The default is 4.

-l length Sends ECHO packets containing the amount of data specified by length. The default is 64 bytes; the maximum is 8192.

-f Sends a Do not Fragment flag in the packet. The packet will not be fragmented by gateways on the route.

-i ttl Sets the Time To Live field to the value specified by ttl.

-v tos sets the Type Of Service field to the value specified by tos.

-r count Records the route of the outgoing packet and the returning packet in the Record Route field. A minimum of 1 and a maximum of 9 computers may be specified by count.

-s count specifies the timestamp for the number of hops specified by count.

-j computer-list Routes packets via the list of computers specified by computer-list. Consecutive computers may be separated by intermediate gateways (loose source routed). The maximum number allowed by IP is 9.

-k computer-list Routes packets via the list of computers specified by computer-list. Consecutive computers may not be separated by intermediate gateways (strict source routed). The maximum number allowed by IP is 9.

-w timeout Specifies a timeout interval in milliseconds destination-listSpecifies the remote computers to ping

## Example:

Y:\>ping yahoo.com

Output:

Pinging sirsyed [192.168.1.1] with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

## Example:

Y:\>ping google.com

Output:

Pinging aurangzeb [192.168.1.5] with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<10ms TTL=128

Reply from 192.168.1.5: bytes=32 time<10ms TTL=128

Reply from 192.168.1.5: bytes=32 time<10ms TTL=128

Reply from 192.168.1.5: bytes=32 time<10ms TTL=128

## Exercise:

On command prompt, type

ping 192.168.2.145

Attach the output

## Exercise:

On command prompt, type

ping 192.168.1.3

Attach the output

## Ipconfig

### Theory

This diagnostic command displays all current TCP/IP network configuration values. This command is of particular use on systems running DHCP, allowing users to determine which TCP/IP configuration values have been configured by DHCP.

ipconfig [/all | /renew [adapter] | /release [adapter]]

Parameters

all Produces a full display. Without this switch, ipconfig displays only the IP address, subnet mask, and default gateway values for each network card.

renew [adapter] Renews DHCP configuration parameters. This option is available only on systems running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

release [adapter] Releases the current DHCP configuration. This option disables TCP/IP on the local system and is available only on DHCP clients. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

With no parameters, the ipconfig utility presents all of the current TCP/IP configuration values to the user, including IP address and subnet mask. This utility is especially useful on systems running DHCP, allowing users to determine which values have been configured by DHCP.

## Example:

Y:\> ipconfig

Output:

Windows NT IP Configuration

Ethernet adapter Elnk31:

IP Address. . . . . . . . . : 192.168.2.13

Subnet Mask . . . . . . . : 255.255.0.0

Default Gateway . . . . : 192.168.1.8

## Example 5.4

Y:\> ipconfig /?

Output:

Windows NT IP Configuration

usage: ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

/? Display this help message.

/all Display full configuration information.

/release Release the IP address for the specified adapter.

/renew Renew the IP address for the specified adapter.

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.

## Exercise:

On command prompt, type

Y:\> ipconfig /all

Attach the output

## Exercise:

In this procedure, you use the Ipconfig utility to view an IP configuration and the PING utility to test your workstation and connections to another TCP/IP host.

## Procedure:

* Use the Ipconfig utility to verify that your TCP/IP configuration has initialized.
* At command prompt, type: Ipconfig
* If the configuration is correctly initialized the IP address, subnet mask, and default gateway (if configured values display).
* Ping the loopback address to verify that TCP/IP is installed and loaded correctly. At a command prompt, type: ping 127.0.0.1
* Ping the IP address of your computer to verify that you added it correctly. Type: ping 172.168.5.1
* Ping the IP address of your second computer to verify that you can communicate with a host on the local network. Type: ping 172.168.5.2
* If a remote host is available on your configuration, ping the IP address of the remote host to verify that you can communicate through a router. Type: **ping IP address of remote host**
* Write the output of each

## Nslookup

* This diagnostic tool displays information from Domain Name System (DNS) name servers. Before using this tool, you should be familiar with how DNS works. Nslookup is available only if the TCP/IP protocol has been installed.
* nslookup [-option ...] [
* computer-to-find | - [server]]
* Modes
* Nslookup has two modes: interactive and non-interactive.
* If you only need to look up a single piece of data, use non-interactive mode. For the first argument, type the name or IP address of the computer to be looked up. For the second argument, type the name or IP address of a DNS name server. If you omit the second argument, the default DNS name server will be used.
* If you need to look up more than one piece of data, you can use interactive mode. Type a hyphen (-) for the first argument and the name or IP address of a DNS name server for the second argument. Or, omit both arguments (the default DNS name server will be used).
* Nslookup Commands
* Nslookup: finger
* Connects with the finger server on the current computer. The current computer is defined when a previous lookup for a computer was successful and returned address information (see the set querytype=A command).
* finger [username] [> filename] | [>> filename]
* Nslookup: ls
* Lists information for a DNS domain. The default output contains computer names and their IP addresses. (When output is directed to a file, hash marks are printed for every 50 records received from the server.)
* ls [option] dnsdomain [> filename] | [>> filename]

### NSLOOKUP Syntax

* Nslookup [-option …] [computer-to-find | - [server]]

### Object:

### To use NSLOOKUP in command mode

* At a command prompt, modify the properties so that it has a screen buffer size of 50
* Use the Layout property page to do this
* If the command prompt is not full-screen, press ALT+ENTER
* Type the following command

### Nslookup hostx

* where hostx is a host in your domain
* NSLOOPKP will return the IP address of the computer hostx because the information is stored in the DNS database.
* Exit the command prompt
* **Hostname:-** It returns the local computer host name .

## Exercise:

* On command prompt, type
* Y:\username>nslookup hostname
* Attach the output

**Netstat**:- Displays protocol statistics and the current state of TCP/IP connections

## Exercise:

On command prompt, type

Y:\username>netstat

Attach the output

**NBTSTAT** :- Check the state of current NetBIOS over TCP/IP connections, updates the LMHOSTS cache, or determines your registered name & scope ID

## Exercise:

On command prompt, type

Y:\username>nbtstat

### Read the different options of nbtstat command.

## Exercise:

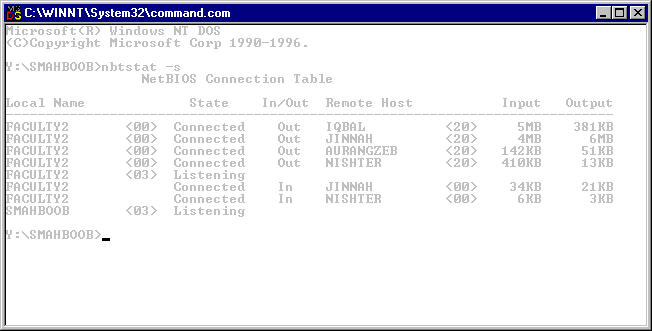
On command prompt, type

Y:\username>nbtstat -n

Attach the output

**Exercise:**

On command prompt, type

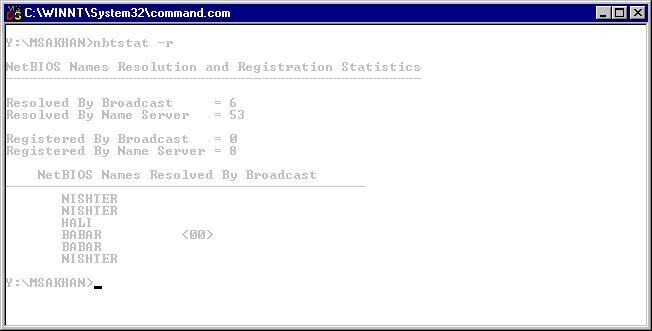
Y:\username>nbtstat –s

Attach the output

## Exercise :

On command prompt, type

Y:\username>nbtstat –r



The screen looks like this

Attach the output

**Tracert :-** Verifies the route used from the local host to a remote host.

**Exercise:**

On command prompt, type

Y:\username>tracert ssuet.edu.pk

-h option maximum number of hops for a search to a target

Attach the output

## Exercise:

On command prompt, type

Y:\username>tracert –h 10 iqra.edu.pk

Attach the output

**HOME ASSIGNMENT:**

Prepare presentation on any three(3) diagnostic utilities of TCP/IP and also Submit hard copy