**CSE 303L: Data Communication and Computer Networks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Demonstration of Concepts** | **Poor (Does not meet expectation (1))**  The student failed to demonstrate a clear understanding of the assignment concepts | **Fair (Meet Expectation (2-3))**  The student demonstrated a clear understanding of some of the assignment concepts | **Good (Exceeds Expectation (4-5)**  The student demonstrated a clear understanding of the assignment concepts | **Score**  **30%** |
| **Accuracy** | The student mis-configured enough network settings that the lab computer couldn't function properly on the network | The student configured enough network settings that the lab computer partially functioned on the network | The student configured the network settings that the lab computer fully functioned on the network | **30%** |
| **Following Directions** | The student clearly failed to follow the verbal and written instructions to successfully complete the lab | The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab | The student followed the verbal and written instructions to successfully complete requirements of the lab | **20%** |
| **Time Utilization** | The student failed to complete even part of the lab in the allotted amount of time | The student failed to complete the entire lab in the allotted amount of time | The student completed the lab in its entirety in the al | **20%** |

**Credit Hours: 1**

# Lab 02

# Investigate the network using “ping” , “tracert” and other Network related Commands

## OBJECTIVES OF THE LAB

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Following topics will be covered in this lab

* Learn to use the TCP/IP Packet Internet Groper (ping) command.
* Learn to use the Trace Route (tracert) command.
* Observe name resolution occurrences using WINS and/or DNS servers.

## ABOUT PING

The original PING command stood for "Packet Internet Groper", and was a package of diagnostic utilities used by DARPA personnel to test the performance of the ARPANET. However, the modern Internet Ping command refers to a program written by Mike Muss in December, 1983, which has since become one of the most versatile and widely used diagnostic tools on the Internet.

Typical Diagnostic Tests Performed By Ping Command

Some of the internet diagnostic tests performed by ping command are:

* **Access –** Ping is used to determine whether the remote host is active or inactive. If a certain site is not pinged, but the other sites can, then it's a pretty good sign that your Internet network is fine and that site is down. On the other hand, if you can't ping any site, then likely your entire network connection is down that needs rebooting.
* **Time & distance –** Another use of Ping command is to determine how long it takes to bounce a packet off of another site. Thereby giving Internet distance in network terms. For example, a web site hosted on your neighbor's computer with a different Internet service provider (ISP) might go through more routers and be farther away in network distance than a site on the other side of the ocean with a direct connection to the Internet backbone. If a site seems slow, then ping distance of that site can be compared with that of other Internet sites to find out whether it is the site, the network, or your system that is slow. You can also compare ping times to get an idea of which sites have the fastest network access and would be most efficient for downloading, chatting, and other applications.
* **Domain IP address –** Typically, Ping command is used to probe either a domain name or an IP address; if a domain name is pinged, and then it displays the corresponding IP address in its response.

**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] target\_name

where target\_name can be either IP Address or host name.

**Option Description**

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

**-t** Ping the specified host until stopped. To see stats &

Continue, type Control-Break; to stop, type

Control-C

**-a (Resolve Addresses)** Resolve address to host names

**-n count (Echo Count)** Sends echo packets specified by count; Default is 4

**-l size (Send buffer Size)** Use to increase or decrease the size of the ICMP packets sent in the ping request;

Min=0, Max=65500

**-f (Set Packet don’t** Select to send a DO NOT FRAGMENT flag in the

**Fragment Flag)** packet. The packet will not be fragmented by Gateways on the route. Use in conjunction with

Send Buffer Size option.

**-i TTL (Time to Live)** set the number of hops (routers) that the ping request can traverse before it is discarded. The TTL field in the packet is decremented by one each time it passes through a router. When the number reaches zero, the router discards the packet and sends a TTL Expired ICMP message back.

**-v TOS (Type of Service)** Sets the TOS value in the ICMP packet for routers that are set up to treat packets with certain types of service differently than others. ToS is not used very often, and most routers ignore it.

**-r count (Record Route** Records the route of the outgoing packet and the **for Hops)** returning packet in the record field;

Min=1, Max=9

**-s count (Timestamp for** Specified the timestamp for the number of hops

**Hops)** Min=1, Max=4

**-w timeout** Timeout in milliseconds that ping waits for each reply

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

## EXAMPLES

### Ping a Local host

In this example, a local host is pinged to see if the computer is able to send and receive information.

**Step 1**

Use the Start menu to open the command-prompt:

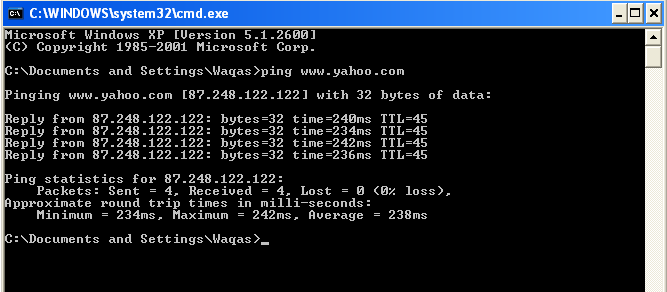
Start>Programs>Accessories>Command Prompt or

Start>Programs>Command Prompt

**Step 2**

Type **ping, space**, and **192.168.2.x**. Press Enter key.

Since Ping uses the **Internet Control Message Protocol** (**ICMP**) echo-request and echo-reply feature to test physical connectivity, it reports on four attempts and gives an indication the reliability of the connection. Look over the result and verify that the ping was successful. Was the ping successful? If not, report to the instructor. A successful host ping is shown in Figure 2.1.



**Figure 2.1: Command Screen for ping** [**www.yahoo.com**](http://www.yahoo.com)

The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP

address.

A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses.

Without this name resolution, the ping would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.

With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.

**--------------------------------------------TASK 01--------------------------------------------**

a) Ping the IP address of the Default Gateway and DNS Servers. Was the result successful?

b) Ping the computer’s loop-back address. Type the following command: **>> ping 127.0.0.1**

c)What is the IP Address of [www.yahoo.com](http://www.yahoo.com): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. How much time did our ping took to reach [www.yahoo.com](http://www.yahoo.com): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

d)Ping the hostname of another computer**.** Try to ping the hostname of the computer that was recorded in the previous lab.

e) Ping the hostname of another computer using –t. Try to ping repetitively, the hostname of the computer

f) How can we stop the ping?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

g) ping the IP address of the default gateway

h) ping the IP address of a DHCP or DNS server

**Use of Ping Option: Resolve Address**

In this example, a website is pinged using its IP Address. By means of ping option: *Resolve Address (-a)*, this IP Address is resolved into its respective host name. Also the ping option: *Echo Count (-n count)* is used to send only 2 echo packets. The details are shown in Figure 2.2.



**Figure 2.2 Use of Address Resolution Ping Option**

## ABOUT TRACERT

The tracert command is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination. Trace route (tracert) is a command-line utility used to trace the path that an Internet Protocol (IP) packet takes to its destination from a source. Tracert will determine the path taken to a destination. It does this by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination. When sending traffic to the destination, it will increment the Time to Live (TTL) field values to aid in finding the path taken to that destination address. The path is outlined from this process.

**Usage**

tracert [-d] [-h maxaimum\_hops] [-j host-list] [-w timeout] target\_name where target\_name can be either IP Address or host name.

**Option Description**

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

**-d (Do Not Resolve** Displays the route using numeric addresses only

**Addresses)** rather than showing both IP address and host

names, for faster display.

**-h maximum\_hops (Max.** Specifies the maximum number of hops to use for

**Hops)** tracing; Default is 30

**-w timeout** Specifies how long to wait for a reply to each

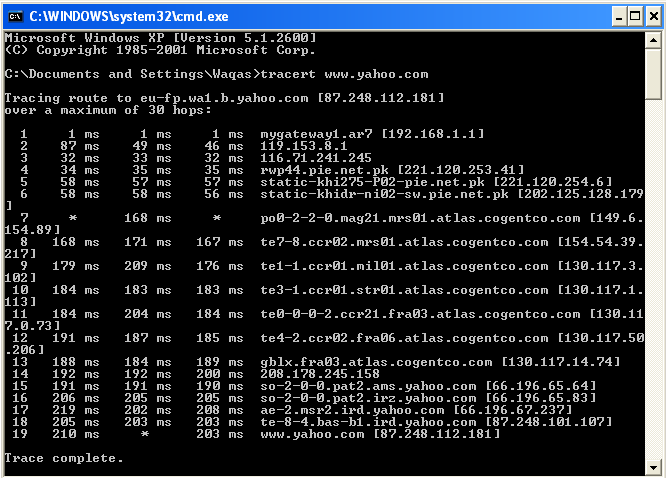
Request in milliseconds; Default is 4000 [for 4 sec]

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

**Step 1**

Trace the route to the Yahoo web site

Type tracert www.yaho.com and press Enter.



**Figure 2.3 Command Screen for tracert www.yahoo.com**

Tracert is TCP/IP abbreviation for trace route. The preceding figure shows the successful result when running tracert from Bavaria in Germany. The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the tracert requests had to pass through to get to the destination. tracert uses the same echo requests and replies as the ping command but in a slightly different way. Observe that tracert actually contacted each router three times. Compare the results to determine the consistency of the route. Notice in the above example that there were relatively long delays after router 11 and 13, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity. Each router represents a point where one network connects to another network and the packet was forwarded through.

**--------------------------------------------TASK 03--------------------------------------------**

1. Trace the route to the GOOGLE PAKISTAN website by typing:

**>> tracert www.google.com.pk**

The result shows the complete route to the site, along with the number of hops in the path.

b) Trace the route to the UET website using options listed in option description table.

c) What is the difference between the following commands?

Tracert [www.yahoo.com](http://www.yahoo.com)

Tracert –h 20 [www.yahoo.com](http://www.yahoo.com)

Task 04 (Life Long Learning)

Practice the following network commands and understand/report their usage

1. **netstat**  
   Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the [IP](http://whirlpool.net.au/wiki/IP) routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

**Try the following**

* 1. \_ **netstat -a**: Shows the state of all sockets, routing table entries, and interfaces.
  2. \_ **netstat -r**: Displays the routing table.
  3. \_ **netstat -i**: Displays the interface information.
  4. \_ **netstat -n**: Displays numbers instead of names.
  5. \_ **netstat -s**: Displays per-protocol statistics.

1. **pathping**  
   Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router.
2. **telnet**  
   Telnet is software that allows users to remotely access another computer such as a server, network device, or other computer. With telnet users can connect to a device or computer, manage a network device, setup a device, transfer files, etc.
3. **nslookup**  
   Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.
4. **getmac**

Command used to show both local and remote MAC addresses. When run with no parameters (ie. getmac) it displays MAC addresses for the local system. When run with the /s parameter (eg. getmac /s \\foo) it displays MAC addresses for the remote computer. When the /v parameter is used, it also displays the associated connection name and network adapter name.

* **getmac /s 192.168.1.1** – Get MAC Address by IP Address
* **getmac /s localhost** – Get local MAC Address

1. **ARP Command**.

Using the arp command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache is a simple mapping of IP addresses to MAC addresses

Use **arp -a** to see the entire ARP table.

1. **Tracert Command:**

Traces the route packets take to reach a destination, showing each "hop" along the way (e.g., tracert google.com).

1. **nbtstat Command:**

Displays NetBIOS over TCP/IP statistics and connections.

Other Useful Commands

1. **net command:**

A powerful command for managing various network aspects, including shares, users, and services.

1. **route command:**

Displays and modifies the IP routing table.

1. **Systeminfo command**:

Provides detailed information about your system configuration, including network adapters.

1. **Hostname command:**

Shows your computer's name.