Introduction to Computer Networking

Dale Callahan, Ph.D., P.E.

MODULE 7: Fun Experiments

7.1 Introduction

This chapter will introduce you to some networking experiments that will help you improve your understanding and concepts of networks. (The experiments assume you are using Windows, but Apple, Unix, and Linux systems will have similar commands.) These experiments can be performed on any computer that has Internet connectivity. The commands can be used from the command line using the command prompt window. The commands that can be used are ping, tracert, netstat, nslookup, ipconfig, route, ARP etc.

7.2 PING

PING is a network tool that is used on TCP/IP based networks. It stands for Packet INternet Groper. The idea is to verify if a network host is reachable from the site where the PING command issued. The ping command uses the ICMP to verify if the network connections are intact. When a PING command is issued, a packet of 64 bytes is sent to the destination computer. The packet is composed of 8 bytes of ICMP header and 56 bytes of data. The computer then waits for a reply from the destination computer. The source computer receives a reply if the connection between the two computers is good. Apart from testing the connection, it also gives the round trip time for a packet to return to the source computer and the amount of packet loss [19].

In order to run the PING command, go to Start → Run and in the box type “cmd”. The command window opens and a cursor is waiting at the prompt. Type the following in the command window.

ping www.targetname.com

The target name should be replaced by Google, Hotmail or some other domain name. An IP address can also be used instead of the domain name. A PING to Google gives the following output.

C:\>ping www.google.com

Pinging www.l.google.com [64.233.161.99] with 32 bytes of data:

Reply from 64.233.161.99: bytes=32 time=58ms TTL=242
Reply from 64.233.161.99: bytes=32 time=70ms TTL=242

Reply from 64.233.161.99: bytes=32 time=60ms TTL=242
Reply from 64.233.161.99: bytes=32 time=60ms TTL=242

Ping statistics for 64.233.161.99:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 58ms, Maximum = 70ms, Average = 62ms

PING command can be specified in various formats. In order to know the arguments that can be specified along with PING, type the following on the command line:

ping /?

In order to set a continuous PING on device or domain name, use the PING command with the '-t' argument

ping –t www.google.com

The continuous ping can be stopped by pressing 'ctrl' and 'c' keys together.

7.3 Tracert

Tracert allows you to trace every router that a packet has traversed during its journey towards the destination. A packet travels through several routers before its reaches its destination. Tracert uses the TTL field in an IP packet and ICMP error messages to determine the route from one host to the other.

In order to run the Tracert command, go to Start → Run and in the box type "cmd." The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

tracert target_name

The target name may be replaced by google, yahoo or some other domain name. An IP address may be used instead of the target name as an alternative. A tracert to google resulted in the following output

C:\>tracert www.google.com

Tracing route to www.l.google.com [64.233.161.104] over a maximum of 30 hops:

1	3 ms	3 ms	3 ms	192.168.0.1
2	10 ms	14 ms	9 ms	10.116.96.1
3	11 ms	22 ms	11 ms	srp0-0.brhmalhe-rtr2.bham.rr.com [66.25.96.2]
4	27 ms	25 ms	25 ms	pos2-0.tampflerl.rtr3.tampabay.rr.com [65.32.8.109]
5	26 ms	26 ms	26 ms	pop1-tby-P0-1.atdn.net [66.185.136.169]

6	36 ms	26 ms	25 ms	bb1-tby-P0-0.atdn.net [66.185.136.160]
7	45 ms	43 ms	42 ms	bb2-atm-P7-0.atdn.net [66.185.152.245]
8	45 ms	43 ms	42 ms	pop2-atm-P1-0.atdn.net [66.185.147.211]
9	42 ms	41 ms	42 ms	Google.atdn.net [66.185.147.218]
10	44 ms	53 ms	53 ms	216.239.46.157
11	44 ms	71 ms	55 ms	66.249.95.124
12	58 ms	58 ms	60 ms	216.239.47.149
13	60 ms	58 ms	58 ms	216.239.47.69
14	63 ms	66 ms	58 ms	216.239.47.156
15	61 ms	61 ms	58 ms	64.233.161.104

Trace complete.

Tracert command can be specified in various formats. In order to know the arguments that can be specified along with tracert, type the following on the command line:

tracert /?

Tracert starts by specifying the destination IP address and setting the TTL field of the packet to one. When the packet travels through a router the TTL field expires as the router decrements the TTL field by one. An ICMP error packet that contains the address of the router is returned back to the source computer. Similarly, the TTL field is increased to two in the next attempt, which expires as the packet goes through the second router. The ICMP error packet provides the source computer with the IP address of the second router. This process is continued till the IP address returned by the router matched the IP address of the specified host. Thus, tracert increments the TTL field by one each time to determine the intermediate hosts.

7.4 Netstat

PING and Tracert are the common tools used to detect any problems over a TCP/IP network. Netstat is another utility that can be used to troubleshoot a TCP/IP connection. In some networking scenarios, there may be a need to run several server software applications on the same machine, which may use the same default port for connection. The netstat command allows a user to identify if a particular port is free on in use and avoid software crashes due to unavailability of the port.

Netstat is a command line utility that can be run from the command prompt. Netstat stands for Network Statistics. In order to run the Netstat command, go to Start → Run and in the box type "cmd." The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

netstat

The following is displayed on the command prompt:

C:\>netstat

Active Connections

Proto	Local Address	Foreign Address	State
TCP	ams:1053	baym-cs6.msgr.hotmail.com:1863	ESTABLISHED
TCP	ams:1056	cs34.msg.dcn.yahoo.com:5050	ESTABLISHED
TCP	ams:1070	sip25.voice.re2.yahoo.com:5061	ESTABLISHED
TCP	ams:1115	192.168.0.12:5101	ESTABLISHED

This command will display a list of all the current TCP/IP connections. The protocol, the local address, the foreign address and the connection state are displayed. In order to see the other formats in which the command can be used, type the following in the command window:

netstat /?

Using netstat with the '-e' argument, the status of Ethernet can be determined. The statistics can be viewed based on protocol by using netstat with '-es' argument as follows:

netstat –es

7.5 nslookup

Nslookup is used to query the Internet Domain Name Servers. Nslookup command operates in two modes. They are called as the interactive mode and the non-interactive mode. In order to use nslookup command, go to Start → Run and in the box type "cmd". The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

nslookup

The prompt changes from 'c:\' to '>'. Type in www.hotmail.com. The following appears on the command prompt:

C:\>nslookup
Default Server: ns1.mindspring.com
Address: 207.69.188.185

> hotmail.com
Server: ns1.mindspring.com
Address: 207.69.188.185

Non-authoritative answer:
Name: hotmail.com
Addresses: 64.4.32.7, 64.4.33.7

The above command uses the name server of your Internet Service Provider (ISP) to resolve the IP address for the domain name specified. The nslookup command can be exited by pressing 'ctrl' and 'c' keys together.

In order to use some other name server type nslookup in the following format:

nslookup domain_name name_server

So, in order to query 'www.google.com' using the name server 'hunterftp.hunter.com', type the following:

nslookup www.google.com hunterftp.hunter.com

The following is displayed:

C:\>nslookup www.google.com hunterftp.hunter.com
Server: hunterftp.hunter.com
Address: 128.242.141.2

Non-authoritative answer:
Name: www.l.google.com
Addresses: 64.233.167.99, 64.233.167.104, 64.233.167.147
Aliases: www.google.com

7.6 Ipconfig

Ipconfig is used to show information on TCP/IP, DNS server addresses, your network interface cards etc. Ipconfig can be used from the command line. In order to use Ipconfig, go to Start → Run and in the box type "cmd". The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

ipconfig

The information regarding your IP address, gateway and the subnet mask is displayed. More information can be obtained by using the following command:

ipconfig/all

Ipconfig can be used to renew or release a DHCP configuration for all interface cards or adapters. In order to see the formats in which Ipconfig can be used, type the following:

ipconfig /?

7.7 Route

The routing tables in your computer can be viewed using the route command. In order to use the route command, go to Start → Run and in the box type "cmd". The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

route Print

This displays all the active routes on your computer. One can add a route to a particular host or a network using the route command. Similarly, a route can be deleted using the route command. The format to add or delete a route can be found by typing the following in the command line:

route /?

These commands should be changed carefully as they may make you unreachable to the Internet.

7.8 ARP

The ARP command maps the IP addresses of a station to the MAC hardware addresses. As discusses in module 5, the ARP request contains the IP address of the requestor and IP address of the computer whose MAC address is desired. The ARP packet is broadcasted and the destination computer accepts the packet by looking at its IP address. The destination computer then sends an ARP reply packet that contains its IP address and MAC address to the requestor.

In order to look at the arp cache maintained in your computer, go to Start → Run and in the box type "cmd". The command window opens and a cursor is waiting at the prompt. Type the following in the command window:

arp –a

The following arp cache table is displayed:

C:\>arp -a

Interface: 192.168.0.8 --- 0x20002
Internet Address Physical Address Type
192.168.0.1 00-09-5b-36-b4-06 dynamic

Windows deletes an entry that has not been used every 10 minutes. Windows also deletes the oldest entry even if the lifetime is not expired in order to make room for new entries in the ARP cache table. The following command can be used to list, add, and remove an ARP cache entry.

ARP command	Result
arp -a or arp –q	Lists the ARP cache
arp -s ipaddress macaddress	Adds an arp entry
arp -d ipaddress	Removes an arp entry

In a local area network, a ping to another computer adds an entry in the arp cache. If the computer is left idle for some time and the arp cache is checked again, then the entry is not visible as it is deleted after 10 minutes [20].