LAB 1

Understanding Ping, Traceroute and Whois

Source : Wikipedia.org

Ping

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater. With computer operating systems Ping or PING stands for Packet INternet Groper but is ordinarily written as "ping" instead of the proper acronym for which it stands.

Ping operates by sending Internet Control Message Protocol (ICMP) *echo request* packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (*round-trip time*) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

Depending on the implementation, the ping command can be run with various command line switches to enable special operational modes. Example options include: specifying the packet size used as the probe, automatic repeated operation for sending a specified count of probes, and time stamping.

Ping may be abused as a simple form of denial-of-service attack in the form of a ping flood, in which the attacker overwhelms the victim with ICMP echo request packets.

```
# ping -c 5 www.example.com
PING www.example.com (192.0.43.10) 56(84) bytes of data.
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=1 ttl=250 time=80.5 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=2 ttl=250 time=80.4 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=3 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=4 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=5 ttl=250 time=80.4 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
```

```
rtt min/avg/max/mdev = 80.393/80.444/80.521/0.187 ms
```

The utility summarizes its results after completing the ping probes. The shortest round trip time was 80.393 ms, the average was 80.444 ms, and the maximum value was 80.521 ms. The measurement had a standard deviation of 0.187 ms.

Ping Attacks

Ping of death

Largest packet size a computer can handle is normally 65,535 byte. So, sending a 65,536-byte ping packet would violate the Internet Protocol as written in RFC 791, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash. This is called ping of death.

Ping flood

A **ping flood** is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most implementations of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP Echo Replypackets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.

Smurf attack

The **Smurf attack** is a way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a system via spoofed broadcast pingmessages.

This attack relies on a perpetrator sending a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts (for

example via a layer 2 broadcast), most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host. Determining the intermediate routers traversed involves adjusting the time-to-live (TTL), aka **hop limit**, Internet Protocol parameter. Frequently starting with a value like 128 (Windows) or 64 (Linux), routers decrement this and discard a packet when the TTL value has reached zero, returning the ICMP error messageICMP Time Exceeded.

Traceroute works by increasing the TTL value of each successive set of packets sent. The first set of packets sent have a **hop limit** value of 1, expecting that they are not forwarded by the first router. The next set have a **hop limit** value of 2, so that the second router will send the error reply. This continues until the destination host receives the packets and returns an Reply message.

Traceroute uses the returned ICMP messages to produce a list of routers that the packets have traversed. The timestamp values returned for each router along the path are the delay (aka latency) values, typically measured in milliseconds for each packet.

The originating host expects a reply within a specified number of seconds. If a packet is not acknowledged within the expected timeout, an asterisk is displayed. The hosts listed may not be hosts used by other packets. The Internet Protocol does not require that packets between two hosts take the same route. Also note that if the host at hop number N does not reply, the hop will be skipped in the output.

The traceroute utility usually has an option to specify use of ICMP echo request (type 8) instead, as used by the Windows **tracert** utility. If a network has a firewall and operates both MS Windows and Unix-like systems, both protocols must be enabled inbound through the firewall.

There are also traceroute implementations that use TCP packets, such as tcptraceroute or layer four traceroute.

```
$traceroute wikipedia.org
traceroute to wikipedia.org (66.230.200.100), 64 hops max, 44 byte packets
 1  124.ae0.xr1.3d12.xs4all.net (194.109.21.1)  0.305 ms  0.360 ms  0.405 ms
 2  0.so-6-0-0.xr1.tc2.xs4all.net (194.109.5.10)  0.634 ms  0.716 ms  0.673 ms
 3  ams-ix-c00.wvfiber.net (195.69.145.58)  0.638 ms  0.601 ms  0.551 ms
 4  lon-c00-pos-4-0.OC48-ams-pos11-0.wvfiber.net (63.223.28.201)  7.512 ms  7.427 ms  7.494 ms
 5  nyc60-pos-1-0.OC48-lon-c00-pos-3-0.wvfiber.net (63.223.28.145)  84.108 ms  83.804 ms  83.995 ms
 6  66.216.1.181 (66.216.1.181)  83.435 ms  83.278 ms  83.348 ms
 7  ash-c01-tge-3-3.TG-nyc-c01-1-1.wvfiber.net (66.216.1.161)  89.563 ms  89.554 ms  89.551 ms
 8  atl-c01-tge-3-1.TG-ash-c01-3-1.wvfiber.net (66.216.1.157)  103.701 ms  103.606 ms  103.596 ms
 9  cpp-hostway.wvfiber.net (63.223.8.26)  103.678 ms  103.609 ms  103.630 ms
10  e1-12.co2.as30217.net (64.156.25.105)  113.014 ms  113.044 ms  113.084 ms
11  10ge5-1.csw5-pmtpa.wikimedia.org (84.40.25.102)  113.153 ms  113.251 ms  113.180 ms
12  rr.pmtpa.wikimedia.org (66.230.200.100)  113.069 ms  113.172 ms  113.003 ms
```

WHOIS

WHOIS (pronounced as the phrase *who is*) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912

The WHOIS system originated as a method for system administrators to obtain contact information for IP address assignments or domain name administrators. The use of the data in the WHOIS system has evolved into a variety of uses, including

- Supporting the security and stability of the Internet by providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams;
- Determining the registration status of domain names.

```
whois -h com.whois-servers.net example.com
```

```
[Querying com.whois-servers.net]
[com.whois-servers.net]

Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
   Domain Name: EXAMPLE.COM
   Registrar: RESERVED-INTERNET ASSIGNED NUMBERS AUTHORITY
   Whois Server: whois.iana.org
   Referral URL: http://res-dom.iana.org
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   Status: clientDeleteProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 26-mar-2004
   Creation Date: 14-aug-1995
   Expiration Date: 13-aug-2011
>>> Last update of whois database: Tue, 17 Aug 2010 02:23:52 UTC <<<
```

Pathping

PathPing is a network utility supplied in Windows NT and beyond that combines the functionality of ping with that of tracert.

It provides details of the path between two hosts *and* Ping-like statistics for each node in the path based on samples taken over a time period, depending on how many nodes are between the start and end host.

The advantages of *PathPing* over **ping** and **traceroute** are that each node is pinged as the result of a single command, and that the behavior of nodes is studied over an extended time period, rather than the default *ping* sample of four messages or default *traceroute* single route trace.

```
Tracing route to wikipedia.com [207.142.131.235]
over a maximum of 30 hops:
  0  simonslaptop [192.168.0.11]
  1  192.168.0.1
  2  thus1-hg2.ilford.broadband.bt.net [217.32.64.73]
  3  217.32.64.34
  4  217.32.64.110
  5  anchor-border-1-4-0-2-191.router.demon.net [212.240.162.126]
  6  anchor-core-2-g0-0-1.router.demon.net [194.70.98.29]
  7  ny1-border-1-a1-0-s2.router.demon.net [194.70.97.66]
  8  ge-8-0-153.ipcolo1.NewYork1.Level3.net [209.246.123.177]
  9  ae-0-51.bbr1.NewYork1.Level3.net [64.159.17.1]
 10  so-2-0-0.mp1.Tampa1.Level3.net [209.247.11.201]
 11  ge-6-0.hsa2.Tampa1.Level3.net [64.159.1.10]
 12  unknown.Level3.net [63.208.24.2]
 13

Computing statistics for 325 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          simonslaptop [192.168.0.11]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                 0/ 100 =  0%   |

Trace complete.
```

LAB Exercise

1. Traceroute to the following destinations/countries choosing a specific site of your own choice hosted in each of the mentioned countries and write down the main route from your site/country to the destination. You are required to mention the main nodes along with country/city name. You have to use the whois database to find out the required information. (You may use

http://www.ip-adress.com/whois, or

http://www.apnic.net/apnic-info/whois_search2, or

www.whois.net)

Asia

Singapore
China
India

Middle East

Saudi Arabia
Dubai

Europe

Germany
Italy

United States

Mexico

Brazil

Canada

Australia

Newzealand

South Africa

2. Write down at least three different observations about behavior of traceroute including an observation mentioning an “abnormal” output or something you are not expecting.
3. You can use traceroute to approximately find out earth diameter, can you explain how?