CST4550 lab3

**Task1: Probing the target and knowing your network**

1. Find the IP address of www.google.com. Make a note below

IP:-216.58.223.78

You got statistics about the ping such as the packets sent and received, etc. Now find out the maximum frame size on the network**.** Send a packet of size 1500 to www.google.com. Write your answers below:

**Ping www.google.com –f –l 1500**

2. Now try to reduce the size of the packet a little bit, say 1300. Write your answer down

Ping statistics for 216.58.223.68:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 40ms, Maximum = 74ms, Average = 49ms

3. Reduce the size of the packet till you find out the maximum packet size allowed in the network. What is the packet size in your case?

Max packet size: 1464 packets

Check with your friend on other machine, is it the same size?

4. Take the IP address of your friend and repeat the steps above. Do you still have the same Max size?

**Task2: Locating the target**

1. Type the following **ping www.google.com –I 3.** Write the response below:

Pinging google.com [216.58.223.78] with 32 bytes of data:

Reply from 196.20.225.41: TTL expired in transit.

Reply from 196.20.225.41: TTL expired in transit.

Reply from 196.20.225.41: TTL expired in transit.

Reply from 196.20.225.41: TTL expired in transit.

Ping statistics for 216.58.223.78:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

1. By manipulating the number of hobs, try to emulate the traceroute command. Draw a diagram that shows all nodes between you and google.com

Tracing route to google.com [216.58.223.78]

over a maximum of 30 hops:

1 3 ms 2 ms 3 ms 192.168.100.1

2 5 ms 4 ms 5 ms 192.168.227.1

3 8 ms 5 ms 5 ms 196.20.225.41

4 7 ms 5 ms 7 ms 197.226.230.10

5 7 ms 5 ms 5 ms 197.226.230.8

6 133 ms 42 ms 41 ms 72.14.221.88

7 45 ms 40 ms 41 ms 172.253.53.1

8 43 ms 40 ms 40 ms 108.170.234.95

9 43 ms 43 ms 40 ms mba01s07-in-f14.1e100.net [216.58.223.78]

Trace complete.

**Task 3: DNS information gathering**

1. In the command line use the interactive mode of **nslookup**

2. Recall the types of DNS records in the lecture. Set the dns record type to “a”, what does this mean? Set type=a it links the domain to the physical ip address of a computer hosting that domain’s services.

3. Type www.google.com and press enter. Write your results down

> www.google.com

Server: UnKnown

Address: 192.168.100.1

Non-authoritative answer:

Name: www.google.com

Address: 216.58.223.68

4.Did you get an authoritative or non- authoritative answer?

Non-Authoritative Answer

5. Now change the type to cname and press enter

> www.google.com

Server: UnKnown

Address: 192.168.100.1

google.com

primary name server = ns1.google.com

responsible mail addr = dns-admin.google.com

serial = 405847288

refresh = 900 (15 mins)

retry = 900 (15 mins)

expire = 1800 (30 mins)

default TTL = 60 (1 min)