

ECE 5480 - Assignment4

1.

Both IP4 and IP6 comes from finite pool of numbers. For IP4 the pool is 32 bits meaning a total number of 2^{32} that is 4,294,967,296 number of available address.

For IP6, the addresses are 128 bits resulting in total number of 2^{128} that is equal to 340,282,366,920,938,463,463,374,607,431,768,211,456 number of total available addresses.

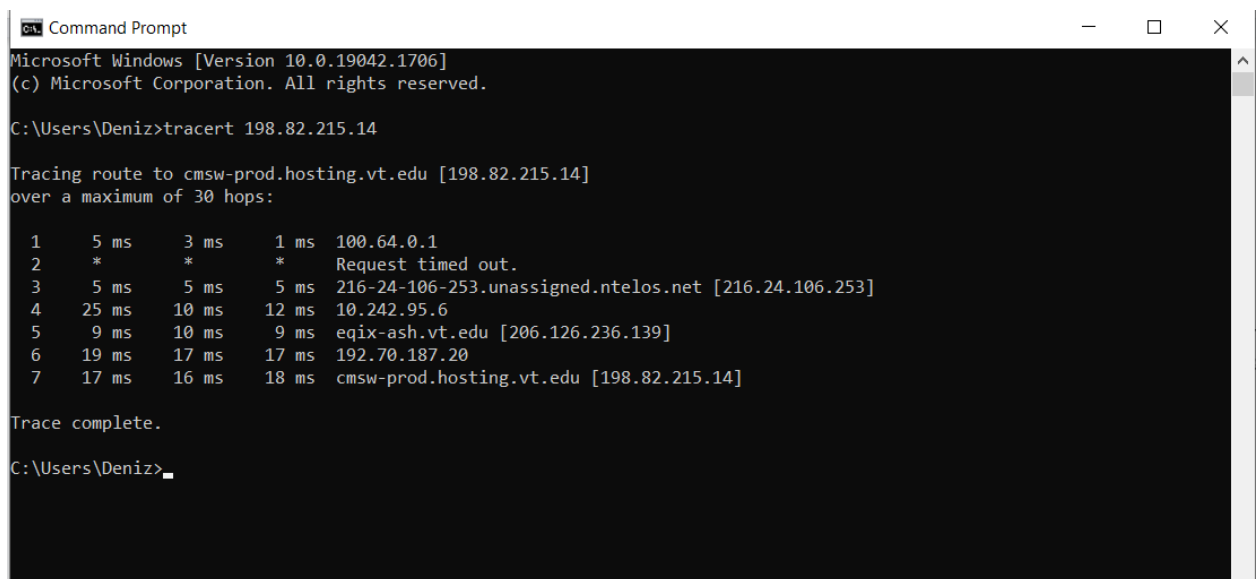
2.

Mac addresses are is the physical address that identifies a computer to another within the same local network. The IP address is the global address of a computer within Internet. MAC address is a local identifier, consists of 12 digits, is a data link layer address, can be reused and is unique to the network card installed on the device. It is hardcoded in the manufacturing of the device hence it cannot be changed. Whereas IP addresses identify a device in globla internet, is a network layer address, if IPv4 then 32 bits, and is assigned the device through software configurations and hence can be changed at any time.

3.

NAT router can be modified such that, for a packet to leave the local area network and go to another device on Internet, the packets source IP address should be existing in that LAN and if it is not the packet's sending should be blocked.

4.



```
Command Prompt
Microsoft Windows [Version 10.0.19042.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Deniz>tracert 198.82.215.14

Tracing route to cmsw-prod.hosting.vt.edu [198.82.215.14]
over a maximum of 30 hops:

  0  5 ms   3 ms   1 ms  100.64.0.1
  1  *      *      *      Request timed out.
  2  5 ms   5 ms   5 ms  216-24-106-253.unassigned.ntelos.net [216.24.106.253]
  3  25 ms  10 ms  12 ms  10.242.95.6
  4  9 ms   10 ms  9 ms  eqix-ash.vt.edu [206.126.236.139]
  5  19 ms  17 ms  17 ms  192.70.187.20
  6  17 ms  16 ms  18 ms  cmsw-prod.hosting.vt.edu [198.82.215.14]

Trace complete.

C:\Users\Deniz>
```

The traceroute displays the path package takes as it is send to destination domain/ IP address which is 198.82.215.14 for this example.

Each row represents a hop or stop along the path. First column indicates which hop. Second, third and fourth columns are RTT times for distinct packages which indicates the total time it took for each package to go to the hop and go back to the client. The last row indicates the IP address or domains of the hop/router. The `***` indicates a time out meaning RTT times were over a certain threshold. In this example it took 7 hops for the package to be send to destination.

5.

A single hexadecimal character represents 4 bits.

Starting with analyzing the IP header,

Field name: version

Purpose: version indicates the IP protocol version which is IPv4 in this case since it is 4.

contents(hex): 4

Length: 4 bits

Field name: helen

Purpose: indicates how many 32 bits words are present in the header.

contents(hex): 5

Length: 4 bits

Field name: service type

Purpose: provided for features related to the quality of data streaming or VoIP calls.

contents(hex): 00

Length: 8 bits

Field name: total length

Purpose: indicates the total length of IP datagram. Together with helen the dimension of the payload can be calculated.

contents(hex): 00 42

Length: 16 bits

Field name: identification

Purpose: used to identify fragments of IP datagram uniquely.

contents(hex): 91 a9

Length: 16 bits

Field name: flags and fragmentation offset

Purpose: first 3 bits(flags) helps to control and identify fragments and be configured accordingly. Rest is offset and is representing the number of bytes ahead of a particular fragment in the datagram.

contents(hex): 00 00

Length: 16 bits

Field name: time to live

Purpose: max time packet will be valid within the internet. After the deadline is passed, datagram is discarded automatically.

contents(hex): ff

Length: 8 bits

Field name: protocol

Purpose: indicates the network protocol used. 11 stands for UDP protocol.

contents(hex): 11

Length: 8 bits

Field name: header checksum

Purpose: 55 43

contents(hex): IP header is checked by being compared to its checksum. If they match package is valid.

Length: 16 bits

Field name: source ip address

Purpose: the IP address of the device sending the package

contents(hex): c0 a8 04 06

Length: 32 bits

Field name: destination ip address

Purpose: the IP address of the device receiving the package

contents(hex): 08 08 08 08

Length: 32 bits

The rest of the ip packet is IP data which encapsulates the protocol packet from the transport layer. Within the IP data there is the transport protocol.

What follows the IP header in this question is the UDP header since the protocol's hex value was 11.

The UDP header is 8 bytes in total and the rest is data.

The UDP header sections can be listed as follows;

Field name: source port number

Purpose: indicates the port which package is being sent from.

contents(hex): e4 b6

Length: 16 bits

Field name: destination port number

Purpose: indicates the port which package is sent to.

contents(hex): 00 35

Length: 16 bits

Field name: total length

Purpose: indicates the total length of the UDP package.

contents(hex): 00 2e

Length: 16 bits

Field name: checksum

Purpose: again checksum is for error correction. The package header is being compared to its checksum to estimate whether there has been an error during transmission or not.

contents(hex): 79 c0
Length: 16 bits