Lab 3

1. Install wireshark

2. Capture packets using wireshark

3. Draw an IP header.

4. Explain the fields for a particular IP packet captured. Try to explain the purpose of each field.

5. Here you find a network trace with fragment bit set in the IP packets. What’s the major difference from the packet you described for answering previous questions.

https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=ipv4frags.pcap

6. List three games you like and list their technical/design highlights.

7. List the names of applications/services you like (up to 20 names).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version  4 | IHL  20 bytes | TOS  0x0800 | Total Length  512 | |
| Identification  0x3b5b (15195) | | | Flags  0x40 | Fragment offset  0 |
| TTL  128 | | Protocol  TCP (6) | Header checksum  0x0000 [ validation disabled] | |
| Source address  129.153.106.142 | | | | |
| Destination address  34.104.35.123 | | | | |
| Options | | | | |
| Data | | | | |

Version:

This shows the first few values of the bits depending on which version it is, the amount of addresses ipv6 have is 1028 times more than ipv4

IHL:

Also known as Internet Header Length, this IP component is used to show how many 32-bit words are present in the header

TOS:

Also known as Type of service. This field is provided features related to the quality of service for data streaming or VoIP calls. VOIP is a technology that allows you to make voice calls using WIFI or data. The first 3 bits are the priority bits.

Total Length:

The total length is measured in bytes. This is used to show the dimension of the payload.

Identification:

Used to identify fragments of an IP datagram. Can be use to add information for packet tracing.

IP Flags:

Is a 3-bit field that helps you control and identify fragments.

Fragment offset:

Represents the number of data bytes ahead of the particular fragment

Time to live:

It shows the maximum time the datagram will be in the internet system in 8-bit field.

Once the time runs out, the datagram will be erased it. Every time a datagram is

processed, the TTL value is reduce by 1

Protocol:

Is reserved to denote the internet protocol

Source Address:

Is address of the source used for the packet

Destination address:

Stores the address of the receiver

IP Options:

Optional field, used when the IHL is longer than 5

Data:

Stores the data from the protocol layer, which has handed over the data to the IP layer