ECE358: Computer Networks

Winter 2018

Project 2: Data Link Layers and ARQ Protocols

Date of submission:2018-03-13

Submitted by: YuCheng Liu

Student ID: y698liu

Student name: Liu, YuCheng

Waterloo Email address: y698liu@uwaterloo.ca

Marks received:

Marked by:

Table of Contents

[Question 1: Protocol Header Analysis 2](#_Toc510276468)

# Question 1: Protocol Header Analysis

## Frame 4:

0017 a486 2900 74d0 2b26 ff76 0800 4500

003c 366d 4000 4006 6a19 8161 380f 8368

5d5d b06e 0050 2244 81dc 0000 0000 a002

16d0 1d0b 0000 0204 05b4 0402 080a 6d5e

b7b1 0000 0000 0103 0307

Ethernet header:

00 17 a4 86 29 00: Ethernet destination address is 00 17 a4 86 29 00(unicast)

74 d0 2b 26 ff 76: Ethernet source address: 74 d0 2b 26 ff 76(unicast)

08 00: The payload type is IP(0x0800)

IP header:

45: This is an IP version 4 datagram,

45: The header length is 5\*4 = 20 bytes.

00

(0 0 0 0 0 0 0 0 in binary): This datagram has routine precedence (the lowest). The IP Precedence filed is used by some routers to determine which datagram to drop, therefore datagram with the lowest precedence will be dropped first.

(0 0 0 0 0 0 0 0 in binary): the 3 type of service (ToS) bits

0 0 0 *Normal delay*

0 0 0 *Normal throughput*

0 0 0 *Normal Reliability*

(0 0 0 0 0 0 0 0 in binary): The last two bits must be zero (for future use).

00 3c: Total length of the IP datagram is 3\*16+12 = 60 (0x003c) bytes.

36 6d: The identification of this datagram is 0x366d (for fragmentation purpose).

40 00: (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0):

1 Don’t Fragment flag set

0 More Fragment flag unset

The fragment offset is 0.

This means that the datagram cannot be fragmented, and there are no fragments after this datagram. With a fragment offset equals to zero, we know that this is the only fragment of a datagram.

40: Time to live 64 = (0x40), meaning the datagram may exist for at most 64 more hops.

06: The protocol on top is TCP (0x06).

6a 19: This is the checksum of the datagram.

81 61 38 0f: Source IP address is 129.97.56.15

83 68 5d 5d: Destination IP address is 131.104.93.93

TCP header:

b0 6e: The Source port is 45166, which is an arbitrarily port number assigned by the operating system.

00 50: The Destination port is 80, which is the well-known port for HTTP

22 44 81 dc: The Seq. no .is 574915036

00 00 00 00: The Ack no. is 0

a0: Data offset is 40 (a\*4) bytes. (The number of 32 bit words in the TCP Header. This indicates where the data begins.)

There are 6 bits reserved for future uses. Must be zero.

02 (0 0 0 0 0 0 1 0): Control Bits: 6 bits

URG 0, ACK 0, PSH 0, RST 0, SYN 1, FIN 0

Only synchronize sequence numbers are set to 1.

16 d0: the receiver window size is 5840 (0x16d0) bytes

1d 0b: Checksum of the whole TCP segment.

00 00: Urgent pointer

0204 05b4 0402 080a 6d5e

b7b1 0000 0000 0103 0307: data

## Frame 14:

0017 a486 2900 14da e974 0821 0800 4500

0054 0000 4000 4001 209f 8161 380b 8e96

d207 0800 a34e db36 0001 0a77 8b52 0000

0000 23dd 0100 0000 0000 1011 1213 1415

1617 1819 1a1b 1c1d 1e1f 2021 2223 2425

2627 2829 2a2b 2c2d 2e2f 3031 3233 3435

Ethernet header:

00 17 a4 86 29 00: Ethernet destination address is 00 17 a4 86 29 00(unicast)

14 da e9 74 08 21: Ethernet source address: 14 da e9 74 08 21(unicast)

08 00: The payload type is IP(0x0800)

IP header:

45: This is an IP version 4 datagram,

45: The header length is 5\*4 = 20 bytes.

00

(0 0 0 0 0 0 0 0 in binary): This datagram has routine precedence (the lowest). The IP Precedence filed is used by some routers to determine which datagram to drop, therefore datagram with the lowest precedence will be dropped first.

(0 0 0 0 0 0 0 0 in binary): the 3 type of service (ToS) bits

0 0 0 *Normal delay*

0 0 0 *Normal throughput*

0 0 0 *Normal Reliability*

(0 0 0 0 0 0 0 0 in binary): The last two bits must be zero (for future use).

00 54: Total length of the IP datagram is 5\*16+4 = 84 (0x0054) bytes.

00 00: The identification of this datagram is 0x0000 (for fragmentation purpose).

40 00: (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0):

1 Don’t Fragment flag set

0 More Fragment flag unset

The fragment offset is 0.

This means that the datagram cannot be fragmented, and there are no fragments after this datagram. With a fragment offset equals to zero, we know that this is the only fragment of a datagram.

40: Time to live 64 = (0x40), meaning the datagram may exist for at most 64 more hops.

01: The protocol on top is ICMP (0x01).

20 9f: This is the checksum of the datagram.

81 61 38 0b: Source IP address is 129.97.56.11

8e 96 d2 07: Destination IP address is 142.150.210.7

TCP header:

08 00: The Source port is 2048, which is an arbitrarily port number assigned by the operating system.

a3 4e: The Destination port is 41806.

db 36 00 01: The Seq. no .is 3677749249

0a 77 8b 52: The Ack no. is 175606610

00: Data offset is 0 (0\*4) bytes. (The number of 32 bit words in the TCP Header. This indicates where the data begins.)

There are 6 bits reserved for future uses. Must be zero.

00 (0 0 0 0 0 0 0 0): Control Bits: 6 bits

URG 0, ACK 0, PSH 0, RST 0, SYN 0, FIN 0

00 00: the receiver window size is 0 (0x0000) bytes

23 dd: Checksum of the whole TCP segment.

01 00: Urgent pointer

0000 0000 1011 1213 1415

1617 1819 1a1b 1c1d 1e1f 2021 2223 2425

2627 2829 2a2b 2c2d 2e2f 3031 3233 3435: data

# Network Utilities

## Q2 ARP:

a) The arp utility helps diagnose problems associated with the Address Resolution Protocol (ARP). TCP/IP hosts use arp to determine the physical (MAC) address that corresponds with a specific IP address.

b)

## Q3 ipconfig

a) The IPConfig command line utility will show detailed information about the network you are connected to. It also helps with reconfiguration of your IP address through release and renew.

## Q4 netstat

a) Netstat, Network statistics, displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is an important part of the Network + exam process, and it is a helpful tool in finding problems and determining the amount of traffic on network as a performance measurement.

## Q5 NSLookup

NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.

## Q6 Ping

The PING utility tests connectivity between two hosts. PING uses a special protocol called Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply. It also can be used to verify whether you have TCP/IP installed and your network card is working.

## Q7 traceroute

Traceroute is very similar to Ping, except that Traceroute identifies pathways taken along each hop, rather than the time it takes for each packet to return.