University of Victoria

CENG 460

Computer Communication Networks

Lab 2 - Ethernet and IEEE 802.11

Instructor:
Dr. Lin Cai

Teaching Assistant:
Amir Andaliby

Tyler Stephen V00812021
A01 - B04

4 March, 2016

1 Introduction

This lab will examine link layer traffic over Ethernet and IEEE 802.11 (wi-fi). Source and destination MAC addresses will be examined for Ethernet. The composition of frame subtypes in IEEE 802.11 will be identified and compared. The reliability of a IEEE 802.11 signal will be determined by examining a series of Data frames.

2 Procedure and Discussion

2.1 Ethernet

Wireshark was used to examine the trace `ethernet-trace-1.pcap` which was obtained from the course lab website. Refering to packet 10, the HTTP GET request from a browser to `gaia.cs.umass.edu`:

1. What is the 48-bit MAC address of the client computer?

The client MAC address is 00:d0:59:a9:3d:68.

2. What is the 48-bit destination MAC address in the Ethernet frame? Is this the MAC address of gaia.cs.umass.edu? Which device has this MAC address?

The destination MAC address is 00:06:25:da:af:73. This is not the MAC address of the host for gaia.cs.umass.edu. It is the MAC address of the router that will make the connection to the internet. Wireshark tells us that 00:06:25 corresponds to "LinksysG", indicating that the router is probably manufactured by Linksys.

3. Give the hexadecimal value for the two-byte Frame type field.

Frame type: IP (0x0800).

4. What is the value of the source MAC address? Is this the address of your computer, or of gaia.cs.umass.edu? Which device has this MAC address?

The source MAC address is 00:d0:59:a9:3d:68. This is the MAC address for the network card on my computer.

The HTTP response frame tells us:

5. What is the destination MAC address in the Ethernet frame? Is this supposed to be the Ethernet address of the computer you are using?

The desination MAC address is 00:d0:59:a9:3d:68, which is my computer. It is reasonable that the response message is addressed *from* the router *to* my computer.

6. Find the hexadecimal value for the two-byte Frame type field.

Frame type: IP (0x0800).

2.2 IEEE 802.11

This section used the trace `wlan-trace-1.pcap`, also available from the course lab website. The trace contains captured wi-fi network traffic. The trace tells us:

7. Which AP is the most active one (i.e., the one sends most Beacon messages)? What is its BSS ID?

BSS ID: Cisco-Li_e3:e3:8f (00:16:b6:e3:e9:8f) sends all beacon messages. There are 458 messages.

8. How many Data frames are in the trace, how many subtypes they have, and what is the most common subtype of these Data frames?

The filter `wlan.fc.type == 2` tells us that there are a total of 1783 Data frames. The breakdown of subtypes is

Table 1: WLAN Data subtypes

Subtype	Name	Count
0x20	Data	1743
0x24	Null function	39
0x22	Data + CF-Poll	1
	Total	1783

9. How many Control frames are in the trace, how many subtypes they have, and what is the most common subtype of these Control frames?

The filter `wlan.fc.type == 1` tells us that there are a total of 1391 Control frames. The breakdown of subtypes is

Table 2: WLAN Control subtypes

Subtype	Name	Count
0x1d	Acknowledgment	1385
0x1c	Clear-to-send	5
0x1a	Power-Save poll	1
	Total	1391

10. How many Management frames are in the trace, how many subtypes they have, and what is the most common subtype of these Management frames?

The filter `wlan.fc.type == 0` tells us that there are a total of 557 Management frames. The breakdown of subtypes is

Table 3: WLAN Management subtypes

Subtype	Name	Count
0x08	Beacon frame	458
0x04	Probe request	81
0x05	Probe response	14
0x0b	Authentication	2
0x00	Authentication request	1
0x01	Authentication response	1
	Total	557

11. Estimate the retransmission times, i.e., the number of retransmissions (i.e., the total number of transmissions - number of original frames) over the number of original transmissions. Show your calculation.

The total number of data frames without retry is 1430, which is found by applying filter `wlan.fc.type == 2 && wlan.fc.retry == 0`. The number of data frames with retry is 353 and is given by the filter `wlan.fc.type == 2 && wlan.fc.retry == 1`. The total of these two values is 1783, which is the total number of Data frames from Table 1. The retransmission ratio, is:

$$\frac{\text{no. retransmissions}}{\text{no. tansmissions without retry}} = \frac{353}{1430} = 0.24685.$$

12. What are the Type and Subtype values for the Association Request / Association Response frames, Probe Request / Probe Response frames, respectively?

These frame types are Management frame subtypes and are listed in Table 3. Wireshark associates 0x00 and 0x01 to *Authentication* request / response. Cisco support documents[1] indicate that subtypes 0x00 and 0x01 may refer to the *Association* request / response.

3 Conclusion

Examining the source and desination addresses of the traffic in the ethernet trace makes it clear that MAC addresses are only known for the "next hop" in the network. The client in the trace only knows about its own MAC address and the address of its router. This is because the final destination address is located in the next layer up, the network layer, and is obscured from the link layer.

The IEEE 802.11 wifi trace contains frames from each of the three possible types: Data, Control and Management. Nearly all of the Data frames have the Data subtype; Nearly all of the Control frames have the Acknowledgement subtype, and; Nearly all of the Management frames are Beacon frames. The trace had a retransmission rate of 0.24685, indicating that almost one quarter of the frames needed to be retransmitted.

4 Feedback

1. Compare ethernet source and destination addresses for local peer to peer traffic and traffic through a router.
2. Compare data from encrypted and unencrypted wi-fi traffic. Try to extract values from the unencrypted traffic.

[1] https://supportforums.cisco.com/document/52391/80211-frames-starter-guide-learn-wireless-sniffer-traces