ECE435: Network Engineering – Homework 10

Wireless / Bridging

Due: Friday, 21 April 2023, 5:00pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 10" and be sure your name is included in the document.

1. **LANs / Switches**

   (a) With a self-learning bridge/switch the switch learns the port/MAC mapping by looking at the SOURCE field in incoming Ethernet frames. How does it ensure the frame gets to the right destination if the DESTINATION MAC address is one it hasn't seen before?

   (b) List one reason why you might separate your LAN into separate networks, rather than having one big LAN.

2. **Wireless**

   (a) You run `iwconfig` on a Raspberry Pi3 and get the following results:

```
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

   It reports the Transmit power as 31 dBm. How much is that in Watts?

   (b) You are using WiFi at one of the 2.4GHz frequencies and you occasionally notice the signal drops out. What might be interfering with your connection? Is it legal for that interference to be happening?

   (c) How is the CSMA/CA (collision avoidance) mechanism used by WiFi different than the CSMA/CD (collision detection) used by wired ethernet? Why didn't WiFi use the wired Ethernet methodology?

3. **Wi-fi Frame**

I managed to put a wi-fi card into "monitor" mode and grabbed a data frame using wireshark. When in monitor mode, the operating system driver tacks a "wiretap" header onto the captured data that provides some extra info about the transmitter/receiver.

```
0x0000  00 00 38 00 2f 40 40 a0 20 08 00 a0 20 08 00 00   ..8./@@. ... ...
0x0010  39 15 fa 00 00 00 00 00 10 6c 94 09 c0 00 bf 00   9........l......
0x0020  00 00 00 00 00 00 00 00 7a 14 fa 00 00 00 00 00   ........z.......
0x0030  16 00 11 03 bc 00 bf 01 08 42 2c 00 b0 be 83 35   .........B,....5
0x0040  19 80 00 1c 10 11 b4 c6 00 1c 10 11 b4 c4 30 e9   ..............0.
0x0050  d2 10 bf 00 81 b7 4e f4 cc 6d 0b ce 80 0d 94 b2   ......N..m......
....
0x0610  8b 20 b3 1b 0c 96 bc b5 1a 2a 66 00 ef 69 24 95   . .......*f..i$.
0x0620  25 3d 4a 73
```

A summary of some of the data gathered:

- Frame 1: 1580 bytes on wire (12640 bits), 1580 bytes captured (12640 bits) on interface wlp2s0
- Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
- Arrival Time: Apr 13, 2023 00:53:45.284591806 EDT
- Data Rate: 54.0 Mb/s, Orthogonal Frequency-Division Multiplexing (OFDM)
- PHY type: 802.11g (ERP) (6)
- Channel: 9 Frequency: 2452MHz
- Signal strength (dBm): -65 dBm

The actual frame starts at offset 0x38.

Say what these fields are, and decode the values if possible.

Wifi HEADER	Name of Field	Decoded Value
`0x0038:` 08 42		
`0x003A:` 2c 00		
`0x003C:` b0 be 83 35 19 80		
`0x0042:` 00 1c 10 11 b4 c6		
`0x0048:` 00 1c 10 11 b4 c4		
`0x004e:` 30 e9		

I can't have you decode the contents of the data part of the frame, as they are encrypted.

At the end are these 8 bytes. The first 4 bytes have to do with the WEP encryption (yes, I have a really old wifi router). What are the last 4 bytes?

Wifi HEADER	Name of Field	Decoded Value
`0x061c:` af e5 0c e2	WEP	—-
`0x0620:` e0 aa 38 16		