**ECEN 192**

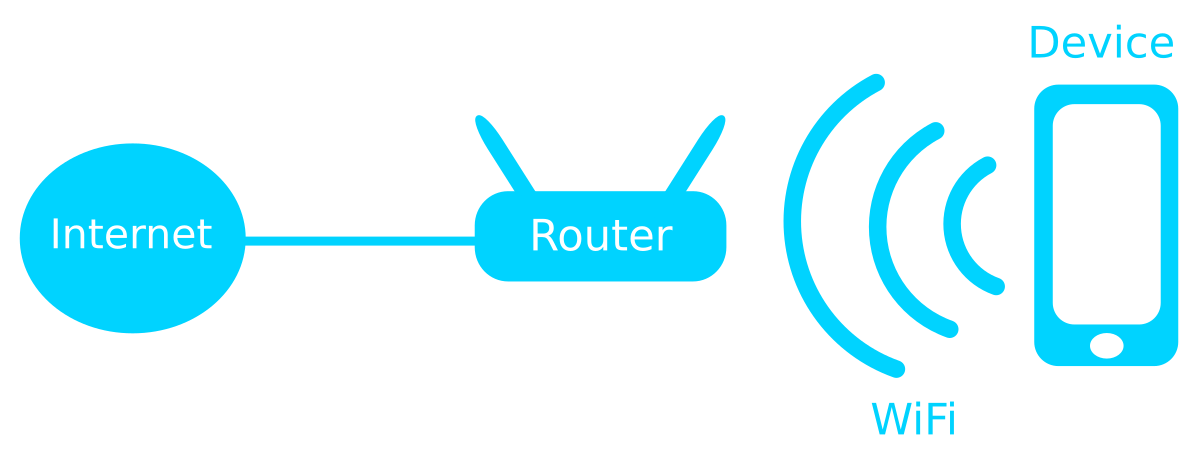
**Lab 10 – Networking**

**Overview:**

In this lab, you will learn the basics of computer networking and the structure of Wi-Fi packets. You will then use this to turn your y-board into a Wi-Fi sniffer, that will be able to identify the unique signature of any device communicating a Wi-Fi network. Lastly, you will connect your y-board to the BYU Wi-Fi network and control it from the internet. This lab will transition into next week’s lab where you will explore vulnerabilities in this code and hack each other’s boards.

**Introduction:**

You’ve probably heard the terms Wi-Fi and the internet and likely use them daily. However, these terms are not synonymous and are often confused. **Wi-Fi** is a protocol for transmitting data over electromagnetic waves from a user device (i.e. your phone or laptop) to an access point, typically a router in your home. Your router then connects via a modem to the **internet**, a global network of connected computers and servers. In short, Wi-Fi is the way you send data wirelessly and can access the internet, and the internet is a massive web of computers connected all around the world. While you might be most familiar with accessing the internet through a browser, there are many other ways to do so, one of which we will explore today using your y-board.



A Wi-Fi transmission consists of packets, which are bundles of data that contains the message being sent as well as supplemental information for the receiver. Each packet is composed of a header, payload, and footer. The header contains information about the transmission's source and destination, as well as details about the actual data (payload). The footer includes checksums, which ensure the data was sent correctly without errors.

**Lab Procedure:**

1. Wi-Fi Sniffer

Download the zip file for the code here <add hyperlink to github repo> and upload it to your y-board. If you need help, check out the documentation for the previous labs on how to do this.

This code will turn your y-board into a Wi-Fi sniffer, which is a device that can listen to any Wi-Fi packets being sent, no matter the Wi-Fi network it is being sent on. A lot of the data in a Wi-Fi packet is encrypted, so that an attacker cannot intercept your information. However, there are some things we can tell from a sniffed packet. Every Wi-Fi packet contains a unique signature called a MAC address, which identifies the device that sent it. Every device in the world has a unique MAC address that no one shares so we can tell when the same device has sent multiple packets. Additionally, the first six digits of the MAC address uniquely identify the device manufacturer and by reading this, we can identify what company or organization made the device.

Make sure switch 2 is in the down position before turning the y-board on to enable sniffing mode. Also make sure your SD card is inserted. If it is not, press the reset button after inserting it. If your screen says “OUI Lookup not available,” ask a TA and they can help. Once on, you will see a bunch of blinking lights ranging from red (for a strong intercepted signal) to blue (a weak one). The knob controls the LED brightness. Your board is keeping a list of the most recent senders and assigns an LED to each one of them. Thus, when the same light blinks several times, it is the same device sending multiple packets. Two of the most recent ones are listed by their manufacturer name on the screen.

On campus, especially in the EB, you may notice Hewlett Packard Enterprises frequently because they are the manufacturer of the Wi-Fi access points in the building.

Walk around for a bit, see what different devices you can pick up and at what strength. Can you get it to see your phone? What about another y-badge? It will appear as Espressif Inc.

1. Explore Channels

Just as there are different radio stations, associated with different radio frequencies, there are different Wi-Fi channels depending on the frequency of the electromagnetic wave they are sent on. Up until now, we were only listening on channel 1, which ranges from 2.401 to 2.423 GHz.

Move switch 1 to the up position. This will bring up a menu to set the Wi-Fi channel that you are listening on by pressing the buttons. Flip the switch back to return to regular sniffing mode. Below is an image of the different Wi-Fi channels on the electromagnetic spectrum. While there are 14 channels, in the US, we only use the first 11. You will see that there is a lot of overlap between the channels. This is actually ok and will still work but can cause problems if too many devices are transmitting on adjacent channels. Because of this, the commonly used channels by most devices are spaced out. Can you find the channels with the most traffic? There should be 3.

A diagram of a channel

Description automatically generated with medium confidence

1. Connect to Server

Being able to listen to other people’s Wi-Fi traffic is great, but let’s get your board on the network. Do this by flipping switch 2. Now you will see that BYU servers assigned your device an IP address and a password.

Your IP address is how every device on the BYU network or any network for that matter knows who you are and how to talk to you. We are now going to control your device remotely. Navigate to ecen192.byu.edu. From there you will see a link on the top right of the page called send command. Here you will be able to login with your username and password as seen on your display and then control the color of the lights on your board.

Try changing the color of your board remotely from the computer. We will pick up from here next week!

**Further Exploration:**

Try using the Wi-Fi sniffer in different locations, such as a public place off-campus or your apartment. What kind of devices can you detect there? Can you locate a device by its signal strength? This might be challenging, but in areas with fewer Wi-Fi devices, it is possible.