Adapted from: https://randomnerdtutorials.com/esp32-access-point-ap-web-server/

Module 12-Networking

For this module you will need:

- Your car constructed from Module 11
- An android phone or laptop/desktop with Chrome

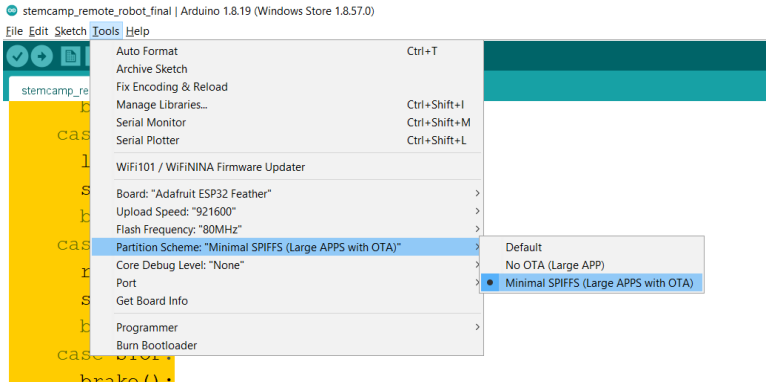
Endure the battery pack switch is OFF.

Ensure the USB cable is plugged into the computer.

Open **stemcamp_controller.ino**

Edit Line 10, and 11 appropriately.

In your Arduino IDE go to Tools->Partition Scheme->Minimal SPIFFS



Upload the sketch to your ESP32.

Once completed, unplug your USB cable.

Jumper wire the power rail from powered from the battery pack to the 5V pin of the ESP32.

Turn the battery pack power switch ON

Adapted from: https://randomnerdtutorials.com/esp32-access-point-ap-web-server/

Connect to your robot car

From a laptop or smart phone, connect to the wi-fi network name you wrote in line 10 and use the password you wrote in line 11.

Open a web-browser and connect to this IP address: **192.168.4.1**

The controller will be displayed.

Begin to drive your device over Wi-Fi!

What is Wi-Fi?

The wireless networking technology known as Wi-Fi (wireless fidelity) uses radio waves to transmit data at high speeds over short distances. Wi-Fi is often used in local area networks (LANs), computer networks that link computers and devices over small geographic areas. Because Wi-Fi allows LANs to operate without cables and wiring, it has become a popular choice for home and business networks.

Wi-Fi can also be used to provide wireless broadband Internet access for devices such as laptops, smartphones, e-readers, and electronic gaming consoles. Wireless-enabled devices are able to connect to the Internet when they are near areas that have Wi-Fi access, called “hot spots.” Hot spots have become common, with many public places such as airports, hotels, bookstores, and coffee shops offering Wi-Fi access. A version of Wi-Fi called Wi-Fi Direct allows connectivity between devices without a LAN.

The origins of Wi-Fi technology can be traced to 1985. In that year the U.S. Federal Communications Commission (FCC) released several bands of the radio spectrum for unlicensed use. Technology firms began building wireless networks and devices to take advantage of the newly available radio spectrum. However, devices from different manufacturers were rarely compatible. To solve this problem, in the 1990s industry leaders came up with a common standard for wireless technology. The Institute of Electrical and Electronics Engineers (IEEE) approved it in 1997. Two years later a group of major companies formed the Wireless Ethernet Compatibility Alliance (WECA, now the Wi-Fi Alliance), a global nonprofit organization created to promote the new standard. WECA named the new technology Wi-Fi.

Adapted from: https://randomnerdtutorials.com/esp32-access-point-ap-web-server/

Under the IEEE Wi-Fi standards, the available frequency bands are split into several separate channels. These channels overlap in frequency, and therefore Wi-Fi uses channels that are far apart. Within each of these channels Wi-Fi uses a “spread spectrum” technique in which a signal is broken into pieces and transmitted over multiple frequencies. Spread spectrum enables the signal to be transmitted at a lower power per frequency. It also allows multiple devices to use the same Wi-Fi transmitter.

Wi-Fi signals are often transmitted over short distances—usually less than 330 feet (100 meters)—in indoor environments. Because of that, the signal would reflect off walls, furniture, and other obstacles. It thus arrived at multiple time intervals and caused a problem called multipath interference. In the 1990s Australian engineer John O’Sullivan and his research team at the Commonwealth Scientific and Industrial Research Organisation (CSIRO) developed a method to reduce the interference. They built a small computer chip that breaks down signals into various tones that make it through the interference. Through several techniques the signals are reassembled when they reach their destination. This improvement makes wireless networks safe and reliable.

What is an IP address?

An **IP address** (short for **Internet Protocol address**) is a label which is used to identify one or more devices on a computer network, such as the internet. It can be compared to a postal address. An IP address is a long number written in binary. Since such numbers are difficult to communicate, IP addresses are usually written as a set of numbers in a given order. Devices using IP addresses use the internet protocol to communicate.
The Internet Assigned Numbers Authority assigns IP addresses to regional internet registries (RIRs). The RIRs assign them to Internet Service Providers. Internet Service Providers then assign IP addresses to their customers. Very often, people have a router or gateway at home, to which they connect computers, printers, and other devices. These routers or gateways are often configured to assign "local" IP addresses to the devices that are connected. Each address has two parts: One that specifies the computer or group of computers, and another which specifies the network. A device can have more than one IP address. Certain types of IP addresses are used to address a group of devices, while others are used to address only one device. Certain types of addresses are unique, others can be re-used. A number of IP addresses are used for special purposes, for example to obtain an IP address automatically. An IP address is converted to physical or Media Access Control Address using the Address Resolution Protocol (ARP). If an IP address is your phone number, then your MAC address is your name. You may change your phone number, but your name will not change.