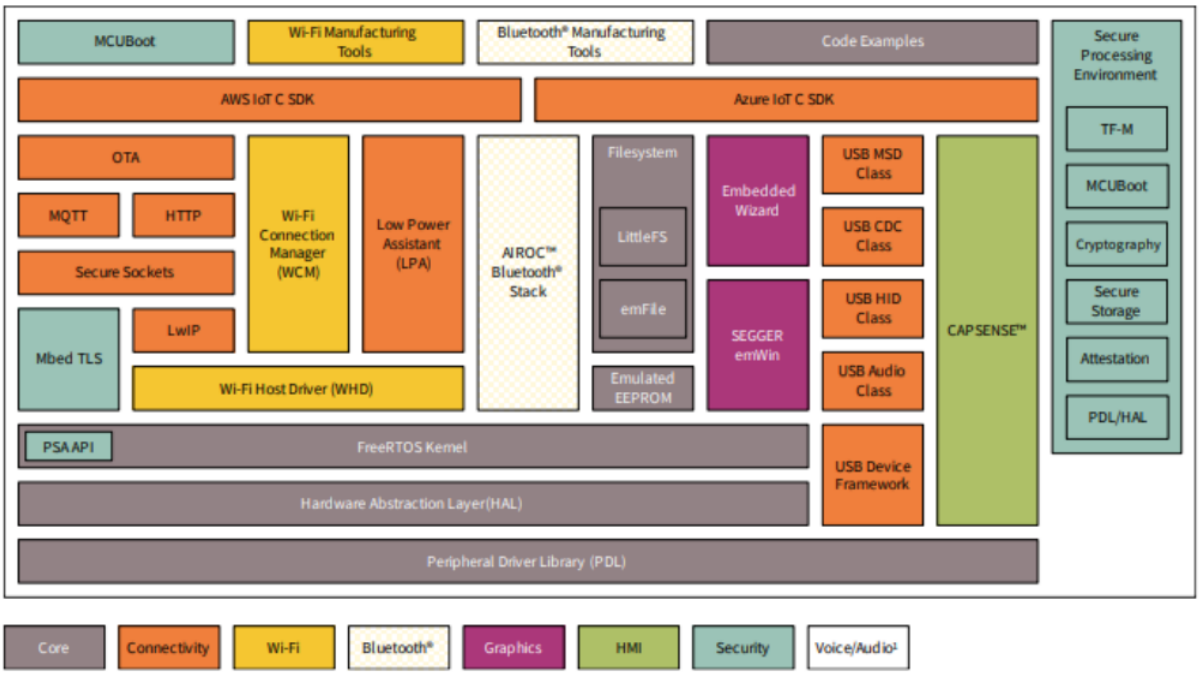
1)

Wifi code example:

- ARP: https://github.com/Infineon/mbed-os-example-wlan-offload-arp
- DHCP: https://github.com/Infineon/mtb-example-wifi-web-server



Wi-Fi Host Driver (WHD) - Embedded Wi-Fi Host Driver that provides a set of APIs to interact with Infineon WLAN chips.

Wi-Fi Connection Manager - Makes Wi-Fi connections easier and more reliable by implementing Wi-Fi Protected Setup (WPS) to simplify the secure connection to a Wi-Fi access point (AP) and by providing a monitoring service to detect problems and keep connections alive.

Connectivity Utilities – A collection of general-purpose middleware utilities including JSON parser, linked list functions, string functions, network helper functions, logging functions, and error code utilities. The network helper functions provides functions to perform tasks like converting strings to IP addresses and vice versa. Header files are provided in the library to include the required set of functions. For example, the network helper functions are included via the header file cy_nw_helper.h while JSON parsing is included via the header file cy_json_parser.h.

lwIP - A Lightweight open-source TCP/IP stack. lwIP stands for "lightweight IP".

lwIP Network Interface Integration - An integration layer that links the lwIP network stack with the underlying Wi-Fi host driver (WHD) and Ethernet driver. This functionality is included via the header file cy_network_mw_core.h.

MbedTLS - An open source, portable, easy to use, readable and flexible SSL library, that has cryptographic capabilities.

MbedTLS Acceleration – Contains MbedTLS hardware accelerated basic cryptography functions.

Secure Sockets - Network abstraction APIs for underlying lwIP network stack and MbedTLS security library. The secure sockets library eases application development by exposing a socket like interface for both secure and non-secure socket communication.

WPA3 External Supplicant - Supports WPA3 SAE authentication using HnP (Hunting and Pecking Method) and H2E (Hash to Element Method) using RFC.

This is actually two separate libraries – one for HTTP servers and one for HTTP clients. The libraries enable both secure (https) and non-secure (http) modes of connection. They support RESTful HTTP methods: HEAD, GET, PUT, and POST.

The OTA toolkit library is an extensible solution based on MCUBoot that can be modified to work with any third-party or custom IoT device management software. With it you can rapidly create efficient and reliable OTA schemes. It currently supports OTA over MQTT and HTTP.

Low Power Assistant (LPA): With LPA you can achieve the most aggressive power budgets by placing the host device into sleep or deep sleep modes while networks are quiet or when there is traffic that can be handled by the connectivity device.

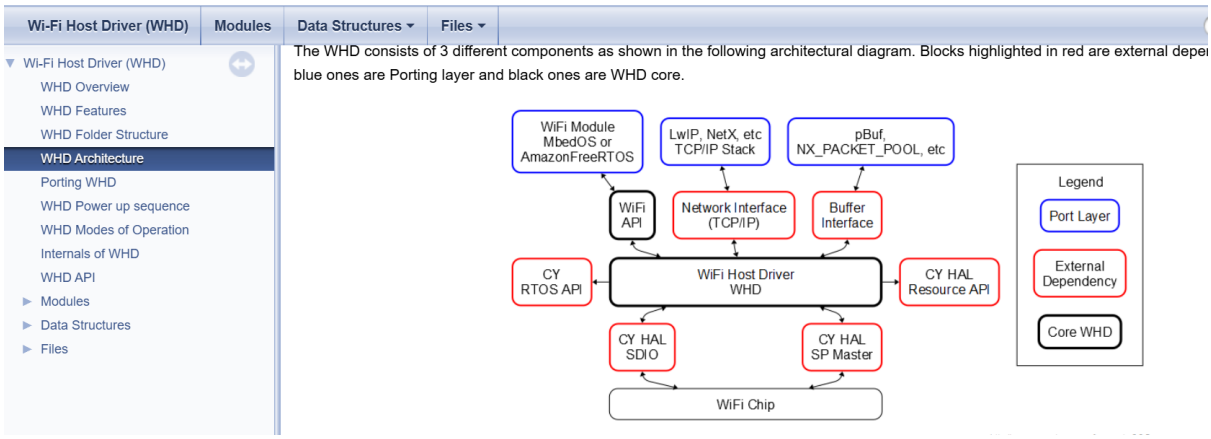
Regardless of which RTOS you use, you must make sure that your tasks/threads are not so high in priority that they interfere with Wi-Fi operation. In the case of FreeRTOS, your tasks should use a priority of 3 or lower to ensure that Wi-Fi works properly. A priority of 3 is equivalent to a priority of CY_THREAD_PRIORITY_NORMAL from the RTOS abstraction library.

Supported bus interface

Interface	4343W	43438	4373	43012	43439	43907
SDIO	O	O	O	O	O	
SPI	O	O			O	
M2M						O

WPA3 AP mode support

Security	4343W	43438	4373	43012	43439	43907
WPA3			O		O	

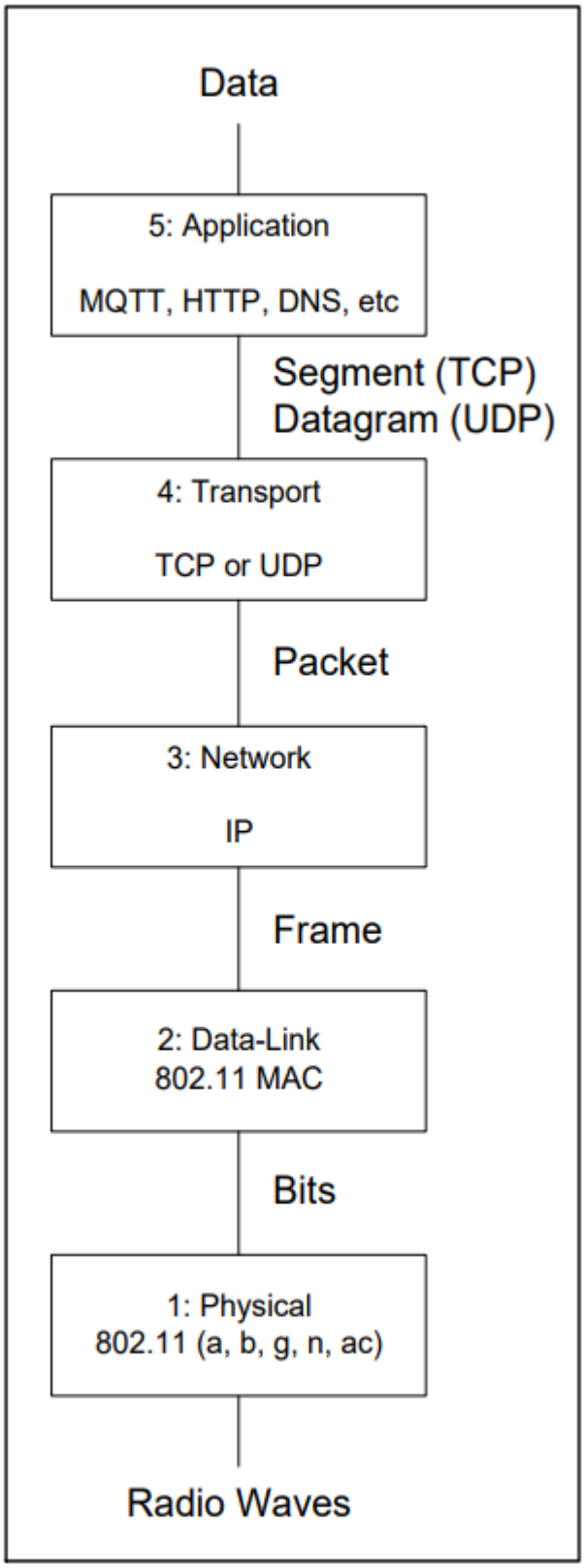


2)

TCP/IP stands for Transmission Control Protocol/Internet Protocol. The "Network Stack" or more accurately, the "TCP/IP Network Stack" is exactly that: a hierarchical system for reliably communicating over multiple networking mediums (Wi-Fi, Ethernet, etc.). Protocol Data Units (PDUs) of that layer. A PDU is the atomic unit of data for a given layer: e.g. the Datalink Layer takes an IP packet and divides it up into 1 or more Wi-Fi Data Link Layer Frames. The physical layer takes Datalink Layer Frames and divides them up into bits.

The layers of the stack are:

Layer	Protocol	Protocol Data Unit	Comment
Layer 5 Application	DNS, DHCP, MQTT, HTTP, etc.	Data	The application layer is the protocol used to do something useful in the device e.g. HTTP (get or put data), DNS (find an IP address from a name), MQTT (publish or subscribe), etc.
Layer 4 Transport	TCP UDP	(TCP) Segments (UDP) Datagram	Reliable, ordered, error checked stream of bytes – think of it as a pipe between computers or as a phone call. An unreliable connectionless datagram flow– think of it like dropping an envelope in the mail to the post office, you don't know it is received until the other side confirms and delivery order is not guaranteed.
Layer 3 Network	IP	Packets	An IP network can send and receive IP packets with source and destination IP addresses to anywhere on the Internet. The IP layer deals with addressing and routing of packets.
Layer 2 Data-Link	802.11 MAC	Frame	A frame is the atomic unit of transmission in the network. Each frame is no more than one Maximum Transmission Unit (MTU) of data which is specific to each data-link layer. All the data from the layers above are broken into frames by the data link layer. Converts bits into unencrypted frames. This layer only communicates on the Local Area Network. A frame contains the MAC address for the source and destination which are mapped to/from the IP addresses.
Layer 1 Physical	802.11(a,b,g,n,ac)	Bits	Sends and receives streams of bits over the Wi-Fi Radio; handles carrier access and arbitration for the network medium.



There are two ends of a Wi-Fi network: The Station (i.e. the IoT device) and the Access Point (i.e. the wireless router). In order for a Station to connect to a Wi-Fi Access Point, it must know the following information: SSID, Encryption Scheme, and Password (if required). The Wi-Fi chip will take care of selecting the proper band and channel. All Datalink Frames are labeled with the source and destination MAC Addresses.

SSID (https://en.wikipedia.org/wiki/Service_set_(802.11_network) stands for Service Set Identifier. The SSID is the network name and is composed of 1-32 bytes (a.k.a. octets - which is the same as an 8-bit byte - but for some reason which is lost in the mists of history, networking guys always call them octets). The name does not have to be human readable (e.g. ASCII) but because it is unencoded bytes, it is effectively case sensitive (be careful).

Band (either 2.4, 5 or 6 GHz)

Wi-Fi radios encode 1's and 0's with one of a number of different modulation schemes depending on the type of Wi-Fi network (a,b,g,n,ac,ax) and operating mode. The types of encoding are transparent to your IoT application since the chip, radio, and firmware will virtualize this for you. The data is then transmitted into the 2.4, 5 or 6 GHz band. The 5 GHz and 6 GHz bands have higher throughput and less latency, but less range, while the opposite is true for 2.4 GHz band.

Channel number

The available channels (https://en.wikipedia.org/wiki/List_of_WLAN_channels) are band (2.4, 5 or 6 GHz) and geographically (location) specific. Additionally, the FCC regulates which channels and bands may be used for different operating regions of the world. At the Wi-Fi layer, this is configured via a country-code setting which maps to a set of available channels for that region.

Encryption (Open, WEP, WPA, WPA2, WPA3)

In order to provide security for Wi-Fi networks it is common to use data link layer encryption (https://en.wikipedia.org/wiki/Wireless_security). The types of network encryption are Open (i.e. no security), Wired Equivalent Privacy (WEP) which is not completely secure (but may be OK for some type of limited legacy applications), Wi-Fi Protected Access (WPA), WPA2 and WPA3. From here on we will just call it WPA, but we generally mean WPA2 or WPA3.

WEP and WPA PSK both use a password—called a key—to encrypt the data. The WEP encryption scheme is not recommended as it is very easy to compromise (e.g. using tools like Wireshark and AirSnort). The PSK key scheme of WPA is very secure as it uses AES (Advanced Encryption Standard). However, sharing keys is a painful, unsecure process because it means that everyone has the same key. To solve the key distribution problem, most enterprise networking solutions use WPA Enterprise which requires use of a RADIUS server to handle authentication of each station individually.

Media Access Control (MAC) address The Wi-Fi MAC address
(https://en.wikipedia.org/wiki/MAC_address) is a 48-bit unique number comprised of an OUI (Organizationally Unique ID) and a station ID. The first three bytes of the MAC address are the OUI field which is assigned by IEEE to be unique per manufacturer (e.g. Infineon). For the datalink layer to send a frame it must address the frame with a source and destination MAC address. Other devices on the network will only pass frames into the higher levels of the stack that are addressed to them. Remember that the Datalink Layer does not know anything about the higher layers (e.g. IP). Finally, the most significant bit of the most significant byte (e.g. bit 47) specifies a multicast (Group) address and the special address of all 1's (e.g. ff:ff:ff:ff:ff:ff) is a broadcast address (send to everyone).

Address Resolution Protocol (ARP)

An IP address can either be IPV4 or IPV6. We will focus on IPV4 addresses which are a 32-bit number that is generally expressed as four hex-bytes separated by periods. For example, 192.168.15.7 is a valid IPV4 address. Inside of every device there is an ARP (https://en.wikipedia.org/wiki/Address_Resolution_Protocol) table that has a map of MAC addresses

to IP addresses. To discover the MAC address of an IP address, an "ARP request" is broadcast to the network. All devices attached to a network listen for ARP requests. If you hear an ARP request with your IP address in it, you respond with your MAC address. From that point forward both sides add that information to their ARP table (and in fact if you hear others ARPing you can update your table as well). The brilliant part of this scheme is that if you ARP for an IP address that is not on your local network, the router will respond with its MAC address. This indicates that any IP address meant for the wide area network (WAN), instead of the local area network (LAN) will be sent to your router. The router then handles returning it to the ultimate destination, often by going through multiple routers along the way. Similarly, on the way back, the router ensures any packet sent arrives to the correct device on its LAN.

IP Networking and Network Address Translation