|  |  |  |
| --- | --- | --- |
| Cell | **Visuals** | **Audio** |
| 1 | Shot of Alan  TEXT ON SCREEN:  Download the manual and solution projects at:  [www.cypress.com/training/wicedwifi-101](http://www.cypress.com/training/wicedwifi-101) | Hi, I’m Alan Hawse. I’m Senior Vice President of Technical Staff for Solutions and Software at Cypress Semiconductor. Welcome to Chapter 5 of Cypress Academy WICED WiFi 101. |
| 2 |  | In this chapter, we will talk about the TCP/IP networking stack, fundamentals of IP networks, and how to configure a WICED device to connect to the network. |
| 3 |  | Complex systems are often managed by dividing them up it into layers – using hierarchy. Networking has exactly that problem, it is complicated. And to manage the complexity, the TCP/IP networking stack created as a hierarchical system for reliably communicating over multiple mediums such as Wi-Fi, Ethernet, and so on.  Each later of the stack isolates the user of that layer from the complexity of the layer below it and simplifies communication for the layer above it. |
| 4 |  | Each layer of the stack has a well defined input & output from the layers above and below it.  Moreover, each layer has a well defined Protocol Data Units (PDUs). The PDU is the atomic unit of data for a given layer. |
| 5 | TEXT ON SCREEN:  Show table of layers building up from the bottom one by one. The columns are Layer, Protocol, and PDU.  Alternately, we could show a figure where boxes appear or are highlighted as Alan talks about each one.  The table and an example figure are shown below. | In the case of TCP/IP, the layers are typically defined as:  Layer 1 is the physical layer. In the case of WiFi, the interface at the bottom is radio waves and the interface to the next layer is a stream of bits, i.e. 1’s and 0’s.  Layer 2 is the data-link layer. It takes bits from the physical layer and turns them into frames (or vice versa). Frames are the atomic unit of transmission for the network.  Layer 3 is the IP layer. It takes the frames and turns them into packets which are routable anywhere on the internet. The IP layer deals with addressing and routing of packets.  Layer 4 is the transport layer. It either uses TCP (for reliable, ordered, and error checked streams of bytes), or UDP (for an unreliable connectionless datagram flow. Think of TCP as a pipe between computers or as a phone call while UDP is like dropping letters in the mail – they may not get there in the same order you sent them or in some cases may not arrive at all.  Layer 5 is the application layer. It will take segments or datagrams and turn them into the appropriate data depending on the application.  If this is your first time looking at this picture, the whole thing looks a bit complicated. But don’t despair as the networking stack is built into WICED and it manages most of the complexity for you. |
| 6 | TEXT ON SCREEN:  Station = STA = Client  Access Point = AP | A Wi-Fi connection has two ends: the station, such as an IoT device, and the access point such as a wireless router.  For a station to connect to an access point, it needs to know the SSID, the Band which is either 2.4 or 5 GHz, the Encryption Scheme, and the network key … meaning password. |
| 7 | TEXT ON SCREEN:  SSID = Service Set Identifier | The SSID is the name of the network and is composed of 0-32 bytes. The name does not need to be ASCII but it typically is. Since the SSID can use any byte values, the name is inherently case sensitive.  There are also different 802.11 modulation schemes such as a, b, g, n, ac, or ax, and channel numbers which are region specific. However, if you are connecting to an access point from a station using WICED, none of that matters since the WICED SDK takes care of all of that for you.  Actually this is one of the most important values of WICED. All of these radio standards are actually insanely complicated… and have tons of not well specified behaviours. The Cypress WICED chips benefit from years of learning in wifi and are your best chance to make devices that will “always work”. |
| 8 | TEXT ON SCREEN:  Open (no encryption)  WEP  WPA  WPA2 | Wi-Fi networks commonly use encryption. The network can either be Open, WEP, WPA, now WPA2. WPA2 is by far the most commonly used scheme today and is the most secure. |
|  | TEXT ON SCREEN:  Personal or Pre-Shared Key (PSK)  Enterprise | There are two versions of WPA2 – Personal or Pre-Shared Key (PSK) and Enterprise. PSK uses a password to encrypt the data. This is secure, but since everyone uses the same password, it can be difficult to manage for large groups of users. For that reason, corporate networks typically use, wpa2 Enterprise. This involves using a RADIUS server to authenticate every station individually. |
| 9 | TEXT ON SCREEN:  MAC Address:  xx:xx:xx:xx:xx:xx  First 3 bytes are the OUI  Last 3 bytes are the station ID | The Wi-Fi Media Access Control (mac) address is a 48-bit unique number comprised of an Organizationally Unique ID (OUI) assigned by the IEEE per manufacturer, and a station ID. Every wifi device on the planet has a different mac address. These MAC addresses are only used locally in the wifi network, and as the information is passed onto other parts of the network.  The data-link layer addresses each frame with a source and destination MAC address. Devices on the network pass frames to higher levels of the stack that are addressed to them. |
| 10 | TEXT ON SCREEN:  Address Resolution Protocol = ARP | In order for packets to go to other IP devices in the network, the data-link layer needs to figure out the MAC address of a particular IP address.  Address Resolution Protocol (ARP) is used to do this.  Each device on the network maintains a table that maps MAC address to IP address.  Whenever a device has a frame to send to an IP address that it doesn’t know the MAC address for, it send out an broadcast ARP request. If the device at the unknown address is on the local network, it will respond with its MAC address.  If not, the router for your local network will respond with its own MAC address which will handle the task of getting the packets to the right place.  I always thought that this scheme was super clever. |
| 11 |  | The internet, or the cloud, is a mesh of interconnected IP networks. All devices have a legal IP address and belong to a local network. Routers connect the local networks to remote networks by forwarding IP packets from the local network to the correct next network. The exact details of this are beyond the scope of this class, but the good news is you don’t need to know the details because it is handled for you automatically.  There are two ip address schemes in the world. IPV4 and IPV6.  IP.v4 address are a 32 bit number usually expressed as 4 bytes, such as 192.168.15.7. The first n-bits are the network address while the last 32-n bits are the client address. A netmask defines how many bits are the network address and how many are the client address.  For IoT devices, the IP address is usually assigned by a Dynamic Host Control Protocol (DHCP) server. DHCP is integrated into WICED and handles the exchange of IP addresses automatically for both servers and clients. |
| 12 |  | That’s the basics of Wi-Fi networking. In the next video we’ll talk about how to use the WICED SDK to configure your IoT device to connect to the network. |
| 13 | TEXT ON SCREEN:  Cypress Developers Community  community.cypress.com  Show video of email and twitter windows. | As always, you can post your comments and questions in our Wifi developer community or you are welcome to email me at alan\_hawse@cypress.com or tweet me at @askioexpert with your comments, suggestions, criticisms and questions. |

Table for Cell 5:

|  |  |  |
| --- | --- | --- |
| **Layer** | **Protocol** | **PDU (Protocol Data Unit)** |
| 5: Application | MQTT, HTTP, DNS, etc. | Data |
| 4: Transport | TCP  UDP | Segment (TCP)  Datagram (UDP) |
| 3: Network | IP | Packet |
| 2: Data-Link | 802.11 MAC | Frame |
| 1: Physical | 802.11 (a, b, g, n, ac) | Bits |

Figure:

