





Microcontroladores Aplicados a IoT

Dilson Liukiti Ito



05 – Wi-Fi e ESP32

Microcontroladores Aplicados a IoT

Wi-Fi



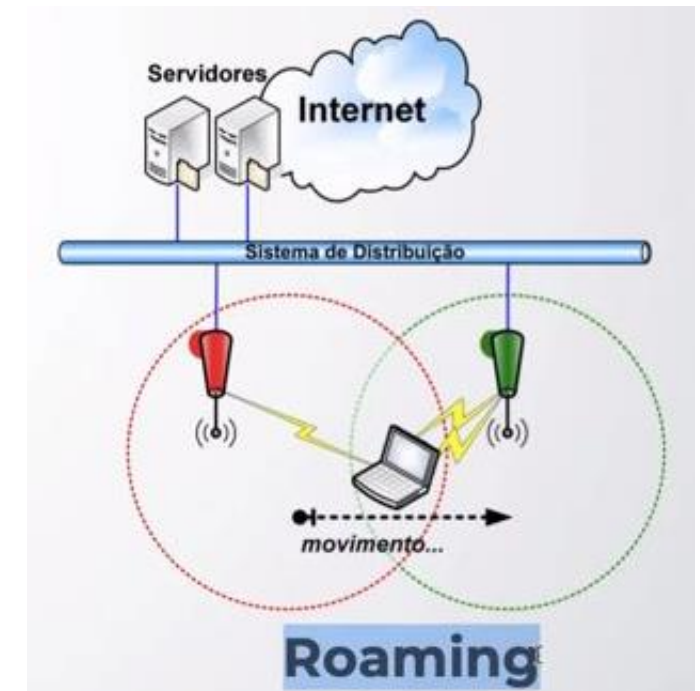
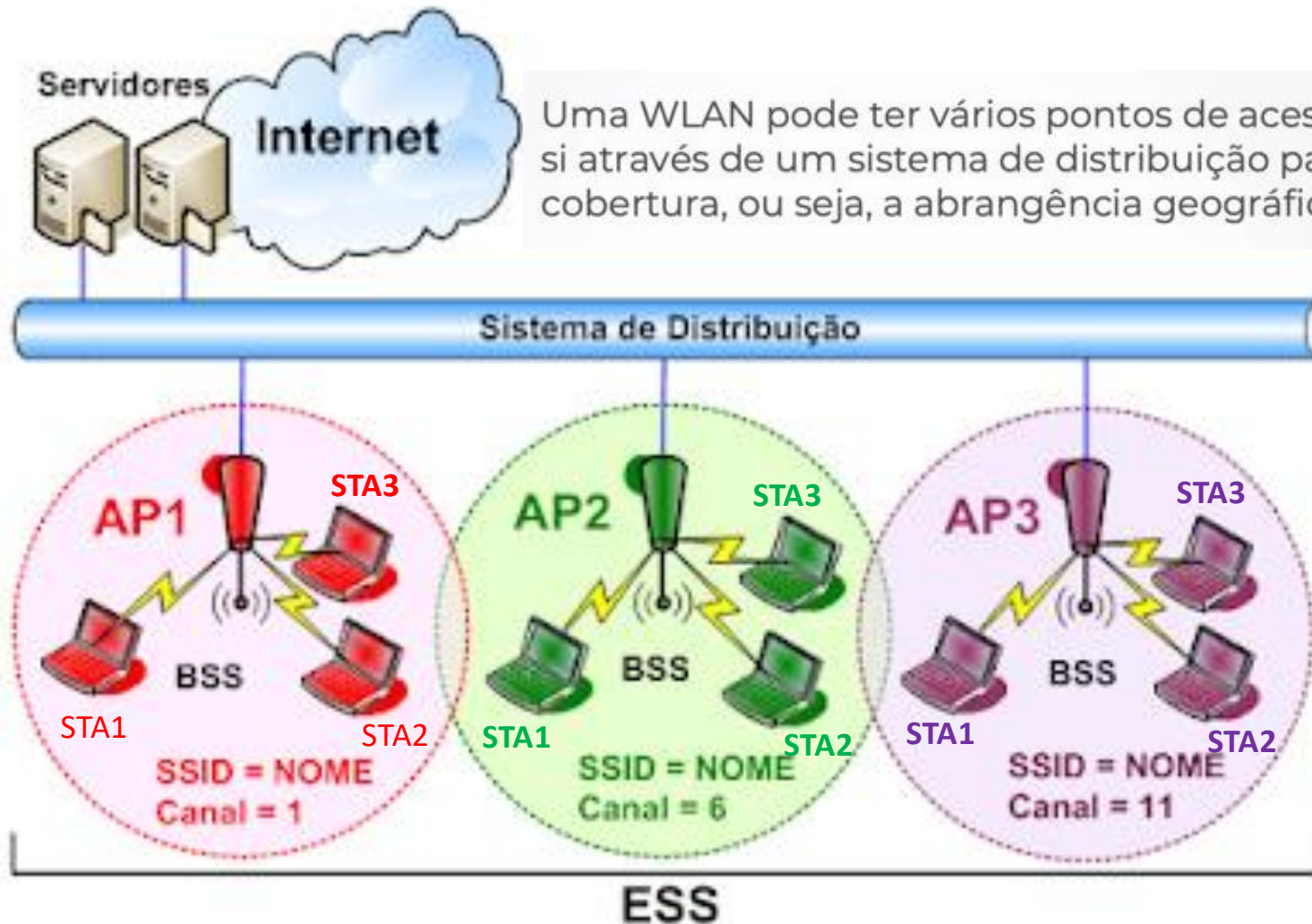
- É um conjunto de especificações técnicas para redes locais sem fio (WLAN — *Wireless Local Area Network*) baseado no padrão [IEEE 802.11](#)
- O padrão 802.11 estabelece normas para a criação e uso de redes sem fio.
- A transmissão nesse tipo de rede é feita por sinais de radiofrequência que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros.

Padrões IEEE 802.11



Ano	Geração	Padrão	Banda	Taxa de Dados
1999	1a Geração	IEEE 802.11b	2,4 Ghz	11 Mbps
1999	2a Geração	IEEE 802.11a	5 Ghz	54 Mbps
2003	3a Geração	IEEE 802.11g	2,4 Ghz	54 Mbps
2009	4a Geração	IEEE 802.11n	2,4 Ghz e 5 Ghz	600 Mbps
2014	5a Geração	IEEE 802.11ac	5 GHz	3,6 Gbps
2019	6a Geração	IEEE 802.11ax	2,4 Ghz e 5 Ghz	10 Gbps

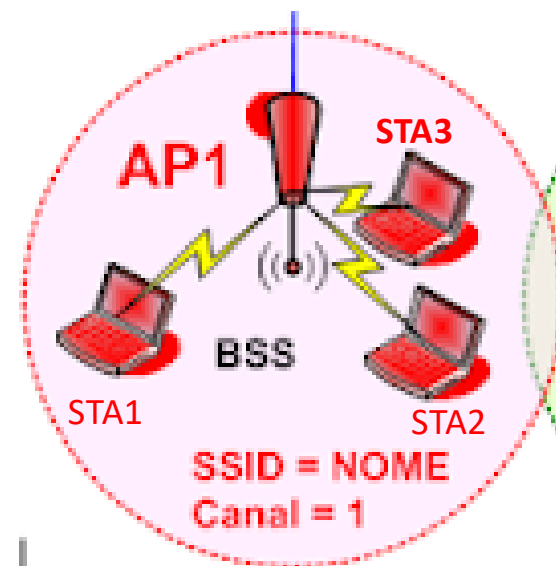
WLAN com múltiplos APs



STA / AP / BSS



- STA (station): estação, dispositivo, que se refere ao dispositivo cliente ([smartphone](#), [notebook](#), tablet);
- Uma das estações será o AP (Access Point). Ele será o ponto de acesso que fará a ponte (bridge) entre duas tecnologias, a Wi-Fi (sem fio) e a infraestrutura cabeada.
- Quando um ou mais STAs se conectam a um AP, tem-se, portanto, uma rede, que é denominada *Basic Service Set* (BSS).



SSID




- O termo SSID significa "service set identifier" ("identificador do conjunto de serviços", em tradução livre).
- Em outras palavras, o **SSID nada mais é do que o nome atribuído a cada rede sem fio.**
- Nomes de rede Wi-Fi podem ter até **32 caracteres** e há distinção entre minúsculas e maiúsculas: "minharede" é diferente de "MinhaRede", por exemplo.
- o ideal seja evitar o uso de caracteres especiais por conta de problemas de compatibilidade com dispositivos mais antigos

BSSID



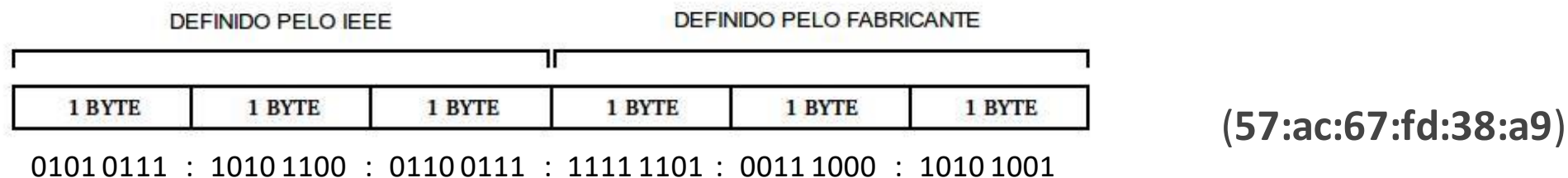
- BSSIDs identificam pontos de acesso e seus clientes
- Por convenção, o endereço MAC de um ponto de acesso é usado como o ID de um BSS (BSSID).
- Portanto, se você conhece o endereço MAC, conhece o BSSID — e, como todos os pacotes contêm o BSSID do originador, você pode rastrear um pacote.

BSSID vs SSID

BSSID	SSID
BSSID is short for basic service set identifier.	SSID is short for service set identifier.
The BSSID is the MAC address of the corresponding WAP.	The SSID is a unique name given to a WLAN.
The BSSID uniquely identifies the access point's radio using a MAC address.	The SSID is the name of the network that acts as a single shared password between access points and clients.
The BSSID is a 48-bit identifier that contains a combination of hexadecimal numbers.	An SSID is a unique alphanumeric string of characters that is limited to 32 characters. 

MAC (Medium Access Control)

- É um número de série de 48 bits / 6 bytes separados por dois pontos (":") ou hífen ("-"), sendo cada byte representado por dois algarismos na forma hexadecimal
- É o endereço base de todos os dispositivos de rede, sendo que existe apenas um para cada placa produzida.



- Apesar de ser único e gravado em hardware, o endereço MAC pode ser alterado através de técnicas específicas.

ESS



- Extended Service Set – ESS (Serviço Estendido)
- A ESS é uma WLAN (Rede Local Sem Fios) com um ou mais pontos de acesso (AP) conectados através de um cabo ethernet (cabo de rede) no sistema de distribuição (roteadores e switches ligados por cabos).
- Ela é utilizada para que seja possível aumentar uma área de cobertura de sinal Wi-Fi.

Bandas RF Wi-Fi

DualBand

Bandas de rede Wi-Fi diferentes para necessidades distintas.
Faça mais, conecte com mais performance e menos interferência.

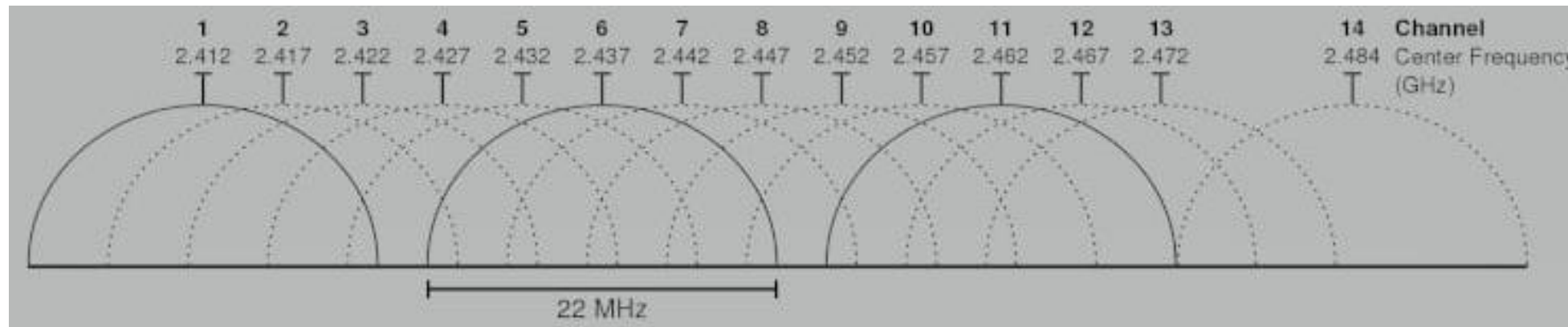


Analogia Canal RF x Canos



- Um canal RF pode ser comparado a um cano. Quanto maior a largura de banda do canal RF, maior é a bitola do cano, maior a taxa de transferência.

Canais WiFi 2,4GHz



Canal	F0 (MHz)	Faixa de frequência (MHz)
1	2412	2401-2423
2	2417	2406-2428
3	2422	2411-2433
4	2427	2416-2438
5	2432	2421-2443
6	2437	2426-2448
7	2442	2431-2453

Canal	F0 (MHz)	Faixa de frequência (MHz)
8	2447	2436-2458
9	2452	2441-2463
10	2457	2446-2468
11	2462	2451-2473
12	2467	2456-2478
13	2472	2461-2483

Canais WiFi 2,4GHz (cont.)



- A transmissão de dados nesta faixa de frequência sofre constantemente de interferências de dispositivos que também operam em 2,4 Ghz como, por exemplo, telefones sem fio, forno micro-ondas, headphones Bluetooth, fones True Wireless ([TWS](#)), entre outros.

Canais WiFi 5GHz



5 GHz Channel Allocations

Frequency (GHz)	5.150				5.250				5.470				5.600				5.640				5.725				5.850	
													TDWR													
802.11 Allocations	UNII-1				UNII-2a				UNII-2c (Extended)												UNII-3					
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720	5745	5765	5785	5805	5825	
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165	
40 MHz	38		46		54		62		102		110		118		126		134		142		151		159			
80 MHz	42				58				106				122		138				155							
160 MHz	50								114																	
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed				120, 124, 128 Devices Now Allowed								1,000 mW EIRP Indoor & Outdoor No DFS needed 165 was ISM, now UNII-3					
DFS Channels					DFS Channels																					

Canais WiFi 5GHz (cont.)



- A grande vantagem desta faixa de frequência é o seu grande número de canais, proporcionando maior largura de banda.
- a ANATEL [permite](#) que se utilize 24 canais que são organizados pela U-NII, que significa Unlicensed National Information Infrastructure.
- A Infraestrutura de informação nacional não licenciada é uma banda de rádio que opera em 4 faixas: UNII-1, UNII-2, UNII-2C (extended) e UNII-3.

Canais WiFi 5GHz (cont.)



- Os canais do grupo UNII-2 e UNII-2C (extended) só são possíveis de serem utilizados se o AP possuir DFS (dynamic frequency selection ou seleção dinâmica de frequência), uma função que permite analisar o meio aéreo antes de permitir sua operação (devido ao fato de radares meteorológicos utilizarem estas frequências).
- Os canais que são ideais para utilização são os das faixas UNII-1 (36, 40, 44 e 48) e UNII-3 (149, 153, 157 e 161)

Canais WiFi 5GHz (cont.)

Canal	F0 (MHz)	Faixa de frequência (MHz)
36	5180	5170-5190
38	5190	5170-5210
40	5200	5190-5210
42	5210	5170-5250
44	5220	5210-5230
46	5230	5210-5250
48	5240	5230-5250
50	5250	5170-5330
52	5260	5250-5270
54	5270	5250-5290
56	5280	5270-5290
58	5290	5250-5330
60	5300	5290-5310
62	5310	5290-5330
64	5320	5310-5330
68	5340	5330-5350

Canal	F0 (MHz)	Faixa de frequência (MHz)
96	5480	5470-5490
100	5500	5490-5510
102	5510	5490-5530
104	5520	5510-5530
106	5530	5490-5570
108	5540	5530-5550
110	5550	5530-5570
112	5560	5550-5570
114	5570	5490-5650
116	5580	5570-5590
118	5590	5570-5610
120	5600	5590-5610
122	5610	5570-5650
124	5620	5610-5630
126	5630	5610-5650

Canal	F0 (MHz)	Faixa de frequência (MHz)
128	5640	5630-5650
132	5660	5650-5670
134	5670	5650-5690
136	5680	5670-5690
138	5690	5650-5730
140	5700	5690-5710
142	5710	5690-5730
144	5720	5710-5730
149	5745	5735-5755
151	5755	5735-5775
153	5765	5755-5775
155	5775	5735-5815
157	5785	5775-5795
159	5795	5775-5815
161	5805	5795-5815
165	5825	5815-5835

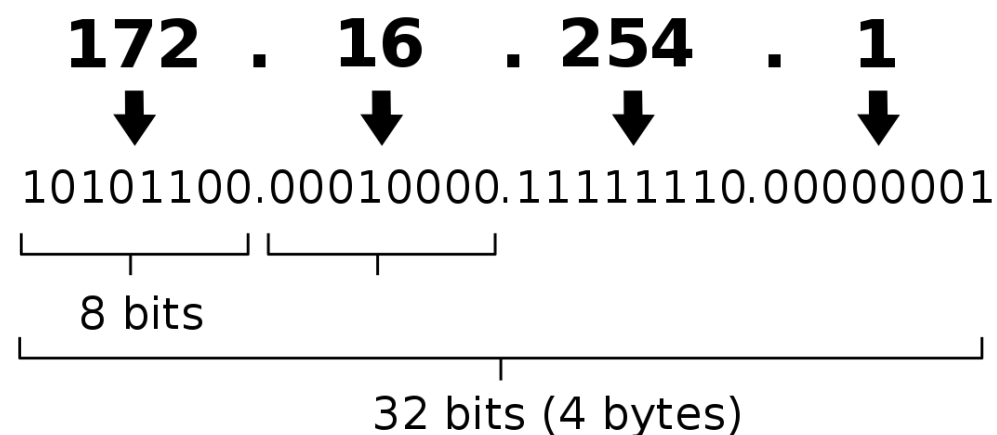
2,4 GHz vs 5 GHz

- Por questões físicas, frequências de rádio mais baixas acabam indo mais longe.
- É por isso que redes de 2,4 GHz são as que alcançam áreas maiores e têm maior penetração diante de obstáculos.
- Já as frequências maiores, como 5 GHz, permitem uma conexão muito mais rápida, mas têm alcance limitado.

IP

- Internet Protocol
- O endereço IP é uma sequência de números composta por 32 bits. Esse valor consiste em um conjunto de quatro sequências de 8 bits.
- Cada sequência é separada por um ponto e recebe o nome de octeto ou simplesmente byte

IPv4 address in dotted-decimal notation



IP (cont.)



- Para que seja encontrado, o seu computador precisa ter um endereço único, o roteador irá atribuir um IP para cada dispositivo conectado a ele. O mesmo vale para qualquer site na internet
- Se duas ou mais máquinas tiverem o mesmo IP, tem-se então um problema chamado "conflito de IP";
- Há conjuntos de endereços que são privados. Isso significa que eles não podem ser usados na internet, pois foram reservados para aplicações locais. São, essencialmente, estes:
 - 10.0.0.0 à 10.255.255.255;
 - 172.16.0.0 à 172.31.255.255;
 - 192.168.0.0 à 192.168.255.255.

Máscara de sub-rede

- Uma máscara de sub-rede é um número de 32-bit que mascara um endereço IP e divide o endereço IP em endereço de rede e endereço de host
- Os bits de rede são representados pela 1 ' s na máscara e os bits de host são representados por 0 ' s. A execução de uma operação lógica no endereço IP com a máscara de sub-rede produz o endereço de rede.

IP	1101 1000 . 0000 0011 . 1000 0000 . 0000 1100	(189.003.128.012)
MASK	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000	(255.255.255.000)
	<hr/>	
	1101 1000 . 0000 0011 . 1000 0000 . 0000 0000	(189.003.128.000)

DHCP



- *Dynamic Host Configuration Protocol*: trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente;
- Quando um computador se conecta a uma rede, envia uma solicitação para que o servidor DHCP "veja" que uma máquina-cliente está querendo fazer parte da rede. O servidor DHCP responde informando os dados cabíveis, principalmente um número IP livre até então;

DHCP (cont.)



- Quando um computador desconecta, seu IP fica livre para uso de outra máquina. Para isso, o servidor geralmente é configurado para fazer uma checagem da rede em intervalos pré-definidos.

DNS



- Quando você digita um endereço qualquer de um site, um servidor de DNS (*Domain Name System*) é consultado. Ele é que informa qual IP está associado a cada site.
- O DNS possui uma hierarquia bem definida. Se, por exemplo, o site www.hausenn.com.br é requisitado, o sistema envia a solicitação a um servidor responsável por terminações ".br". Esse servidor localizará qual o IP correspondente e responderá à solicitação. Se o site solicitado termina com ".com", um servidor responsável por esta terminação é consultado e assim por diante.

```
└─$ ping www.hausenn.com.br  
PING hausenn.com.br (173.254.29.38) 56(84) bytes of data.  
64 bytes from just2057.justhost.com (173.254.29.38): icmp_seq=1 ttl=52 time=191 ms
```

IPv6



- O formato do IPv4 é uma sequência de 32 bits (ou quatro conjuntos de 8 bits) e isso permite, teoricamente, a criação de até 4.294.967.296 endereços.
- O mundo está cada vez mais conectado => Esgotamento de IP
- IPv6 é formado por 128 bits. Com isso, teoricamente, a quantidade de endereços disponíveis pode chegar a 340.282.366.920.938.463.463.374.607.431.768.211.456

FEDC:2D9D:DC28:7654:3210:FC57:D4C8:1FFF

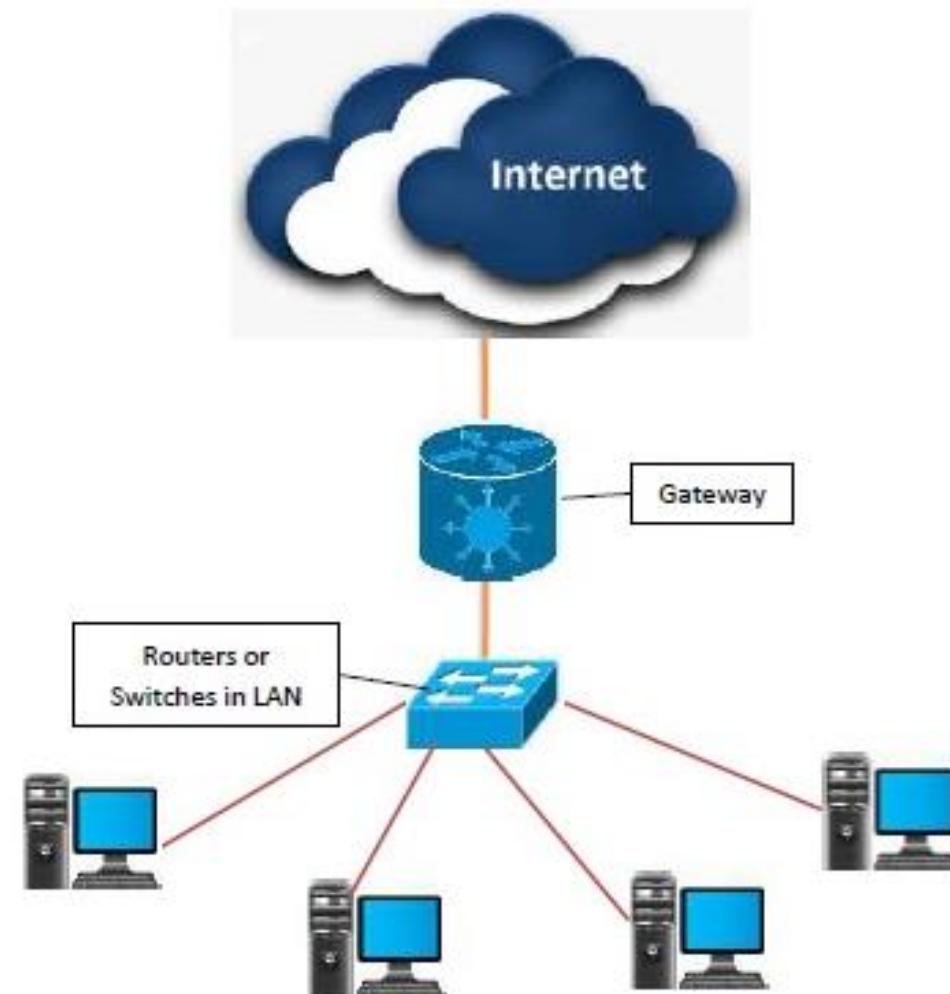
IPv6 (cont.)



- roteadores, servidores, sistemas operacionais, entre outros precisam estar plenamente compatíveis com o IPv6, mas a internet ainda está baseada no IPv4. Isso significa que ambos os padrões vão coexistir por algum tempo.

Gateway

- Um gateway é um nó de rede que forma uma passagem entre duas redes operando com diferentes protocolos de transmissão.
- Ele atua como o ponto de saída de entrada para uma rede, pois todo o tráfego que flui pelas redes deve passar pelo gateway. Somente o tráfego interno entre os nós de uma LAN não passa pelo gateway.



Gateway (cont.)

- Um gateway conecta redes, enquanto um roteador normalmente entrega dados dentro de uma rede.
- Os roteadores Wi-Fi fornecidos geralmente para o serviço de Internet para casas e para pequenas empresas são um roteador (entregando dados) e um gateway (traduzindo-o para que os dispositivos de destino possam usá-lo).

Protocolos Segurança Wi-Fi



- A criptografia Wi-Fi é um método que usa algoritmos para embaralhar o sinal de dados entre dispositivos. O embaralhamento impede que pessoas não autorizadas interceptem ou leiam qualquer informação transmitida pela conexão Wi-Fi.
- Proteção de seus dados

Encriptação Wi-Fi



WEP. Wired Equivalent Privacy

Padrão 1999 - 2004. Fácil de quebrar e difícil de configurar.
Abandonado.



Segurança • Fraca



Configuração • Difícil



WPA. Wi-Fi Protected Access

Foi usado como um aprimoramento temporário para o WEP. Fácil de quebrar. Configuração: moderada



Segurança • Fraca



Configuração • Mais ou menos



WPA2. Versão 2 do Wi-Fi Protected Access

Desde 2004. Criptografia AES.



Segurança • Boa



Configuração • Normal



WPA3. Versão 3 do Wi-Fi Protected Access

Em breve. Proteção de senha. WiFi Easy Connect.



Segurança • Excelente



Configuração • Excelente

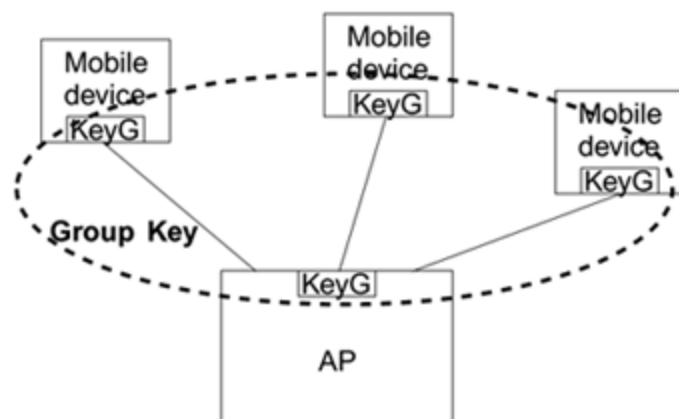
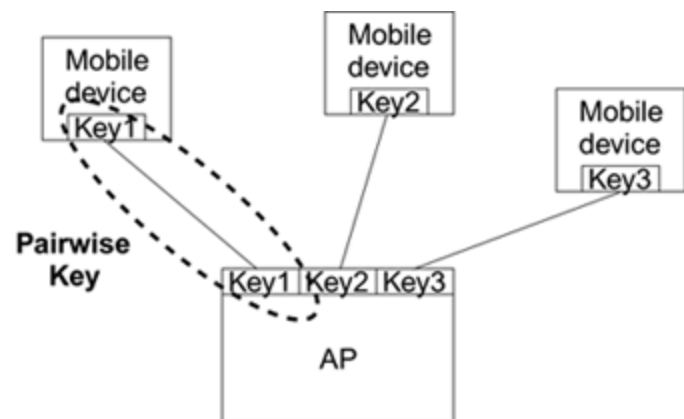
WPA / WPA2

- 802.1X (Enterprise): utiliza o EAP (Extensible Authentication Protocol);
- PSK (Shared Key) utiliza uma chave compartilhada entre o AP e o STA;

TKIP / AES

- WPA utiliza o TKIP (Temporal Key Integrity Protocol) ou o CCMP (Counter Mode CBC-MAC Protocol) como meio de encriptação;
- WPA2 utiliza CCMP tendo o TKIP como opcional.
- TKIP e CCMP são protocolos de encriptação. AES e RC4 são cifras. As duplas são CCMP/AES e TKIP/RC4.

Pairwise / Group Keys



- pairwise key: Cada cliente negocia uma chave de encriptação exclusiva com o Access Point;
- Group Cipher Identifica os tipos de encriptação utilizados na comunicação de grupo da rede (multicast / broadcast).

Encriptação Wi-Fi overview



- Enquanto o WPA2 oferece mais proteção do que o WPA e, portanto, oferece ainda mais proteção do que o WEP, a segurança do seu roteador ainda dependerá muito da senha que você definir. **O WPA e o WPA2 permitem usar senhas de até 63 caracteres.**
- O WPA2 é a versão melhorada do WPA;
- WPA e WPA2 suportam criptografia TKIP e CCMP;
- O WPA2 precisa de mais poder de processamento do que o WPA;

Encriptação Wi-Fi overview (cont.)



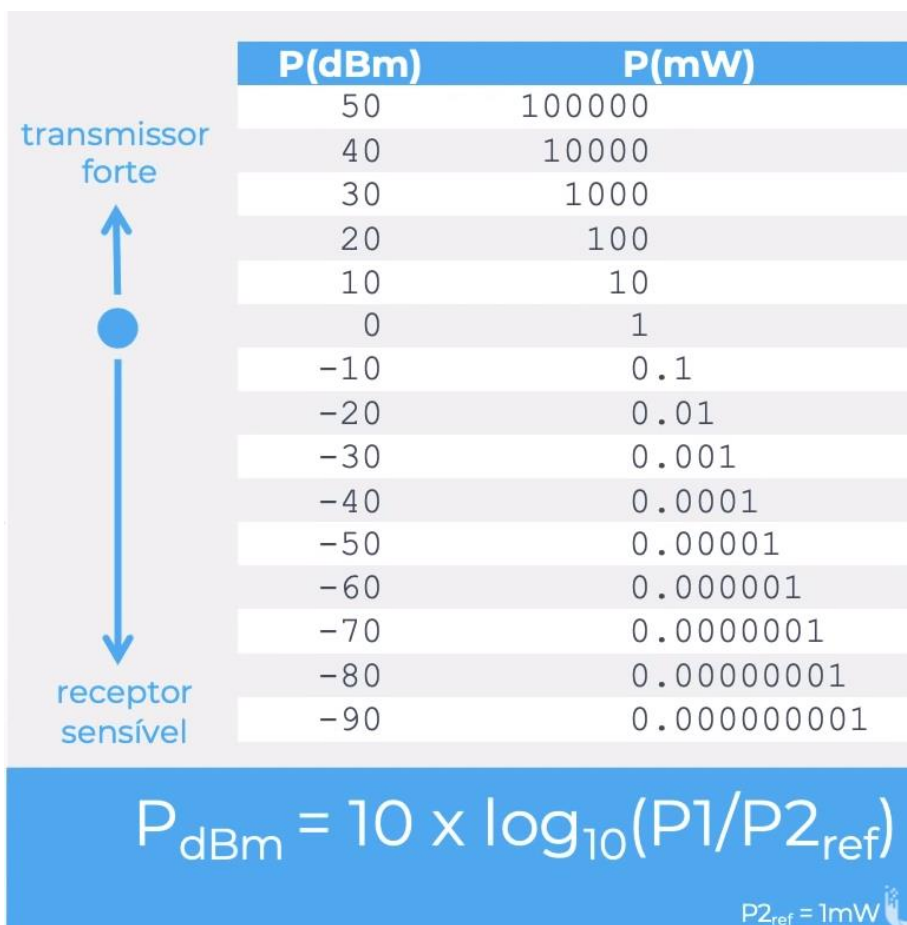
- Aqui está a classificação básica (do melhor ao pior) dos métodos de segurança Wi-Fi disponíveis para os roteadores:
 - **WPA2 CCMP**
 - **WPA CCMP**
 - **WPA TKIP/CCMP (TKIP existe um método de fallback)**
 - **WPA TKIP**
 - **WEP**
 - **Rede Aberta (sem qualquer segurança)**

RSSI



- **received signal strength indicator (RSSI)** é é uma indicação do nível de potência que está sendo recebido pelo rádio receptor, em unidades arbitrárias;
- Portanto, quanto maior o valor RSSI, mais forte o sinal. Assim, quando um valor RSSI é representado de forma negativa (por exemplo, -100), quanto mais próximo o valor estiver de 0, mais forte foi o sinal recebido.

dBm



- É a unidade de medida utilizada principalmente em telecomunicações para expressar a potência absoluta.
- O dBm é o nível de potência em dB em relação ao nível de referência de 1mW (miliWatts).

dBm (cont.)

- uma variação de - 3 dBm é equivalente à metade da potência, e de + 3 dBm é equivalente ao dobro da potência
- A potência cai de 50 dBm para 47 dBm, significa uma queda de 100 W para 50 W.
- A potência subiu de 50 dBm para 53 dBm, significa um aumento de 100 W para 200 W.

dBm (cont.)



Potência Sinal	Qualidade esperada
-30dBm	Força máxima do sinal, você provavelmente está ao lado do ponto de acesso.
-55dBm	Qualquer coisa até esse nível pode ser considerada excelente força de sinal.
-67dBm	Força de sinal confiável - a borda do que a Cisco considera adequado para apoiar a voz sobre a WLAN
-80dBm	Força de sinal não confiável
-90dBm	As chances de conectar são muito baixas neste nível

Update ESP-IDF

```
$ cd ESP32/esp-idf/
```

```
$ git fetch  
$ git switch release/v4.3
```

```
$ git submodule update --init --recursive
```

```
$ git status  
On branch release/v4.3  
Your branch is up to date with 'origin/release/v4.3'.
```

```
$ git describe  
v4.3.2-600-gb137ae4259
```

```
$ ./install.sh esp32
```

```
I (27) boot: ESP-IDF v4.3.2-600-gb137ae4259-dirty 2nd stage bootloader
```

EventGroup()

```
#define WIFI_CONNECTED_BIT BIT0  
#define WIFI_FAIL_BIT BIT1
```

```
EventGroupHandle_t wifi_events;
```

```
wifi_events = xEventGroupCreate();
```

```
EventBits_t bits = xEventGroupWaitBits(wifi_events, WIFI_CONNECTED_BIT  
|                                     WIFI_FAIL_BIT, pdFALSE, pdFALSE,  
portMAX_DELAY);
```

```
if (bits & WIFI_CONNECTED_BIT)
```


esp_err_t e ESP_ERROR_CHECK()



```
typedef int esp_err_t;
```

```
#define ESP_OK 0 /*!< esp_err_t value indicating success (no error) */  
#define ESP_FAIL -1 /*!< Generic esp_err_t code indicating failure */
```

```
ESP_ERROR_CHECK();
```

```
esp_err_to_name(esp_err_t)
```

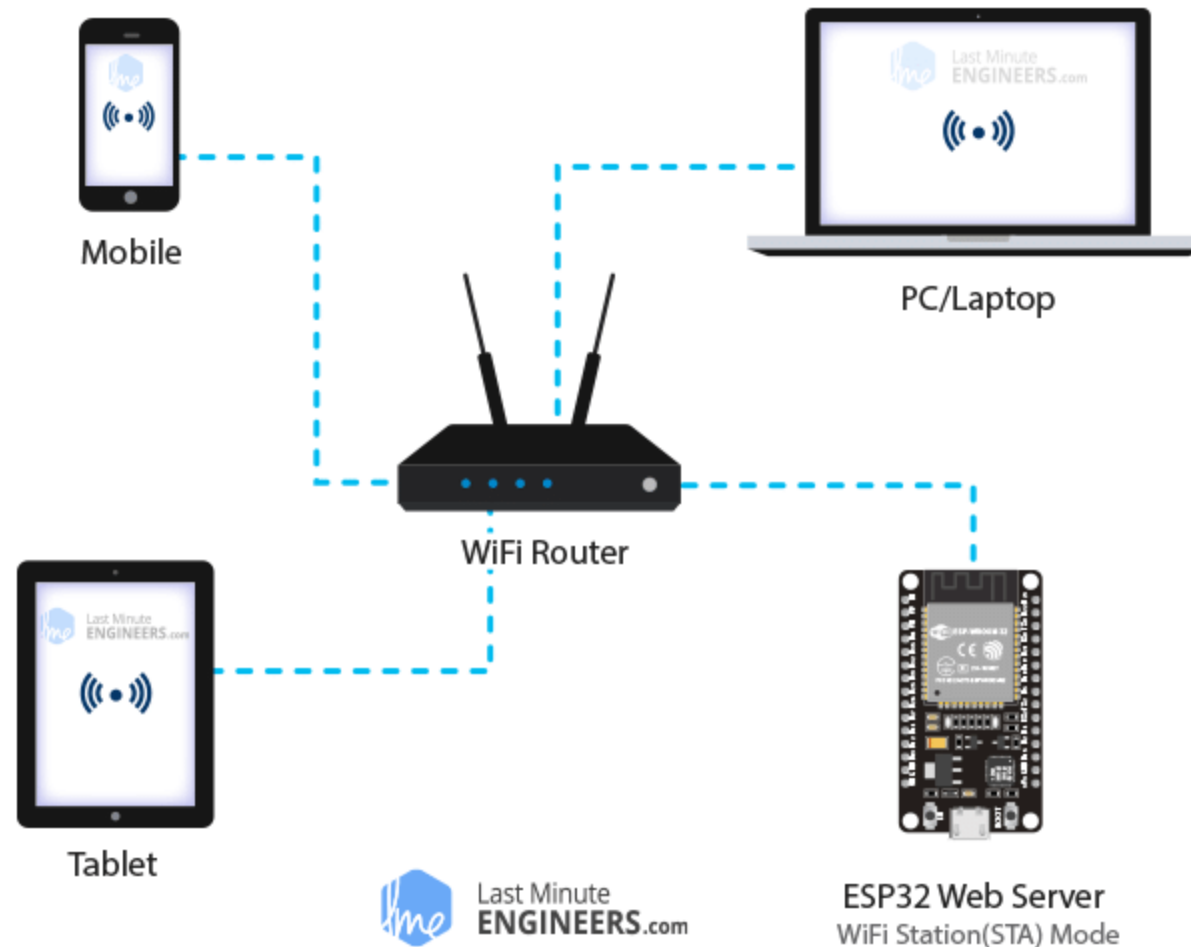
Exemplos

- Scan
- STA
- AP

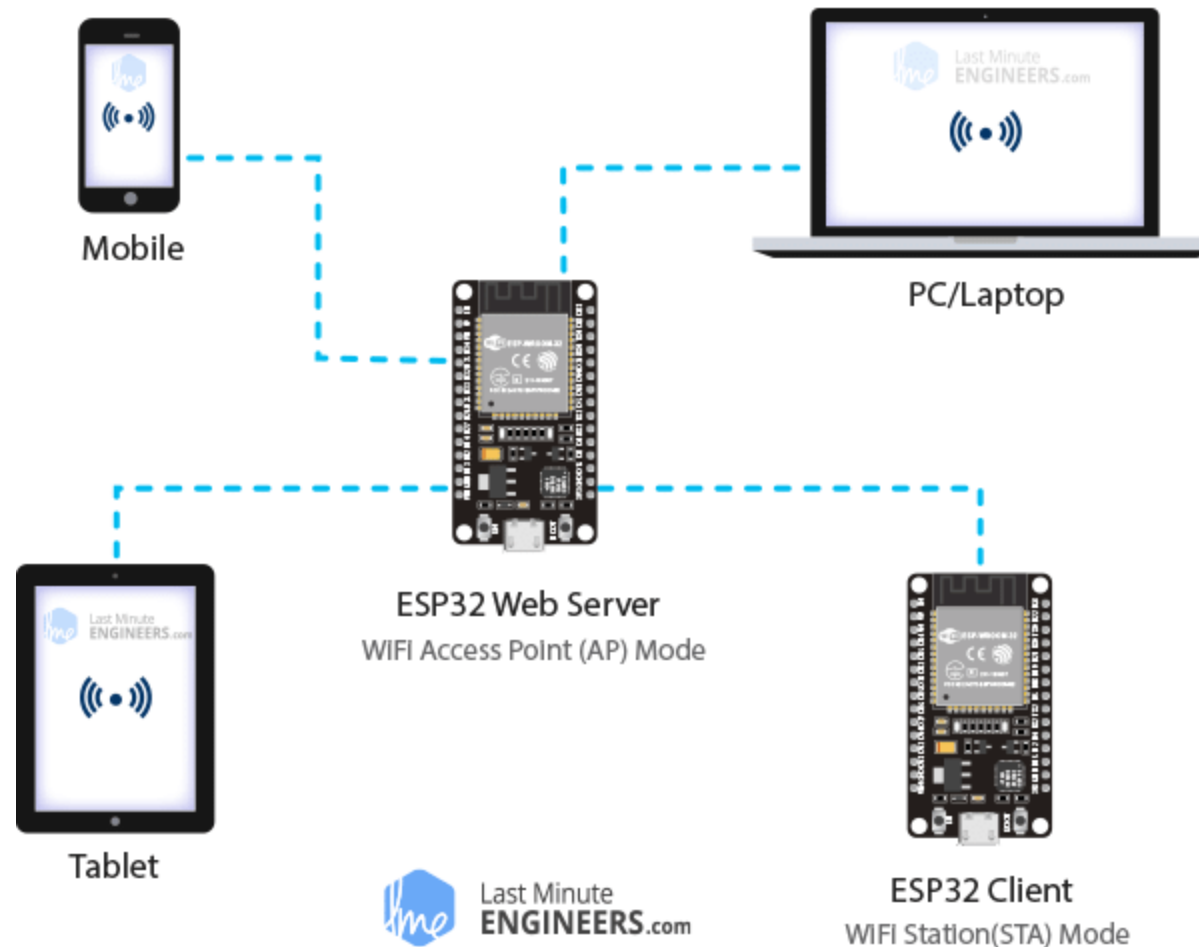
[Download Aula05.zip](#)



ESP32 como estação (STA)



ESP32 como AP



Exercício

- Faça um programa que mantenha o ESP32 em modo AP até que receba as credenciais válidas de uma rede WiFi (get / post), quando então deverá conectar à essa rede em modo station.
- Faça o correto manejo das credenciais e da tentativa de conexão com o AP. Relatando o "disconnect reason" ou o status quando for conveniente;
- Desafio: Mostre as redes que o módulo "enxerga" na página onde serão repassadas as credenciais.

Recomendados



- https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodri_go_paim/intro.html
- <https://onlinepngtools.com/convert-png-to-base64>

