

Redes sem Fio

**Padrão IEEE 802.11
Wi-Fi**

Prof. Carlos Louzada

Wi-Fi

e

**IEEE
802.11**

- Wi-Fi é uma marca registrada da Aliança Wi-Fi (Grupo formado por diversos fabricantes);
- Para ser considerado Wi-Fi o equipamento tem que passar pela certificação;
- Todo equipamento Wi-Fi é **802.11**;
- Nem todo equipamento 802.11 é Wi-Fi.

Sinônimo Wi-Fi

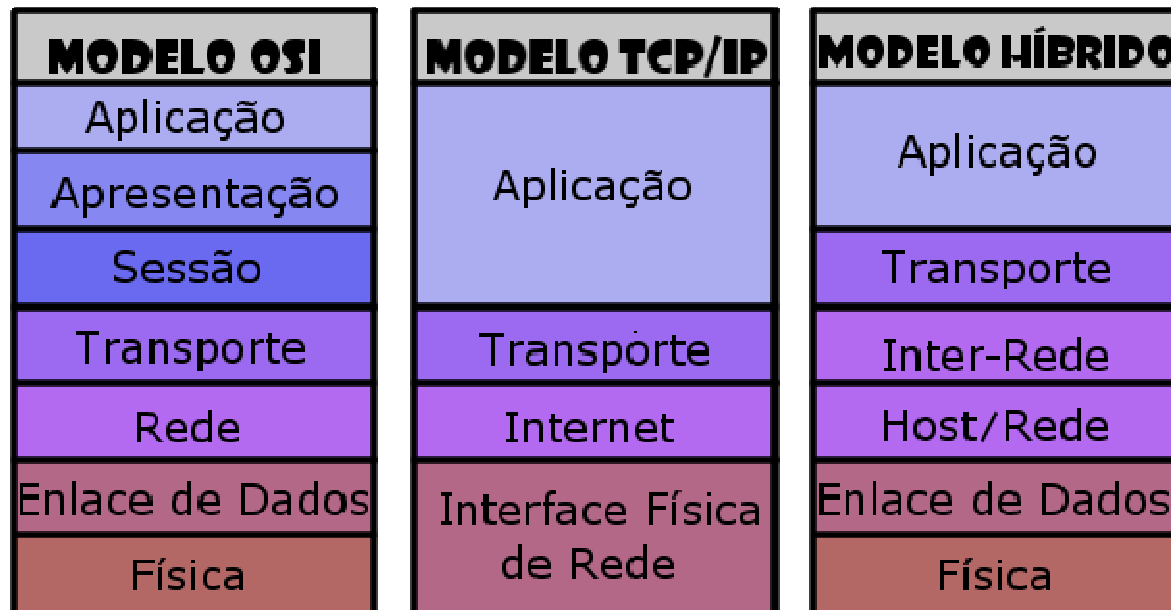
- Wi-Fi;
- IEEE 802.11;
- Sem fio;
- Wireless

IEEE 802.11

- O padrão IEEE 802.11 é usado para montagem de redes locais sem fio;
- Usa a transmissão por ondas de rádio (Radiofrequência - RF);
- A taxa de transferência e o alcance dependem do padrão usado na camada física da rede (IEEE 802.11b, IEEE 802.11g etc).

Wi-Fi no modelo OSI

- Opera nas camadas 1 e 2 do modelo OSI, onde é responsável por pegar os dados passados pelo protocolo de alto nível, dividi-los em quadros e transmiti-los via onda de rádio.



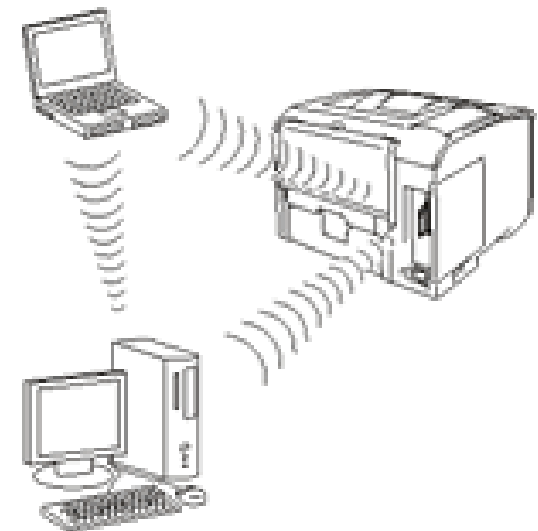
Arquitetura de Redes IEEE 802.11

- Há 3 modos de operação em rede Wi-Fi:
 - *Ad-hoc*;
 - *BSS (Basic Service Set)*; e
 - *ESS (Extended Service Set)*

Ad - hoc

- Usado para conectar um pequeno número de computadores através de transmissão sem fio sem o uso de um periférico chamado **ponto de acesso**.

Ex.: impressora sem fio.

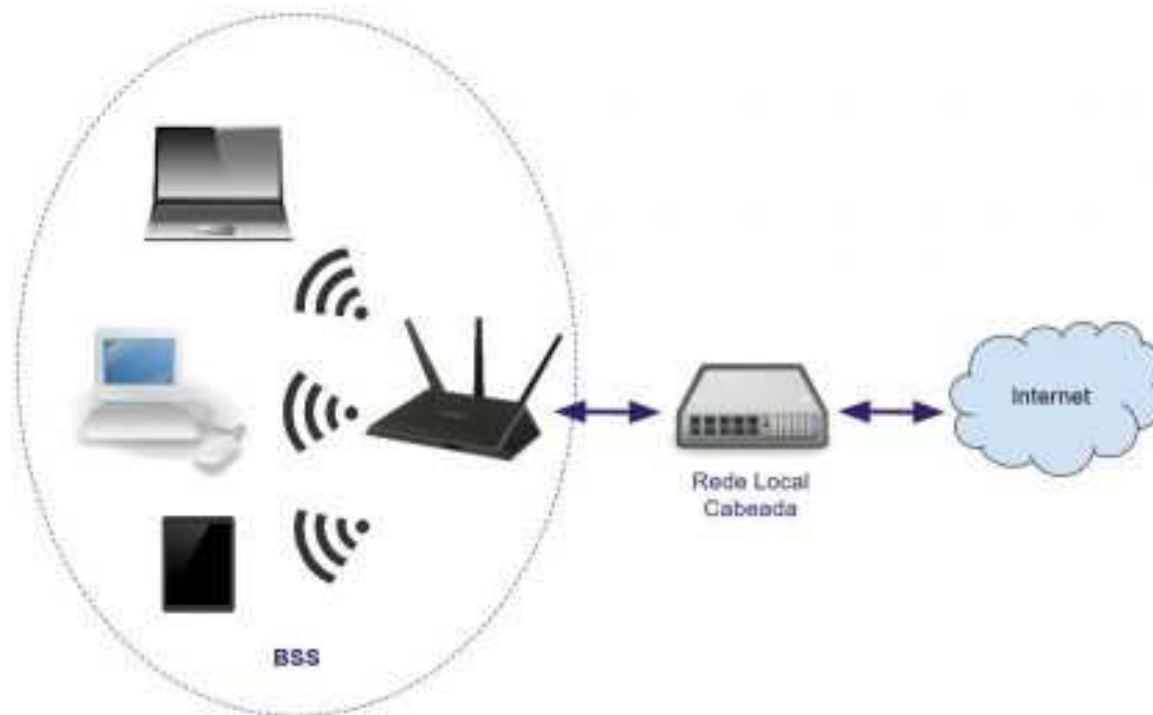


BSS (Basic Service Set)

- Nesse modo de operação a rede sem fio é comandada por um periférico chamado **ponto de acesso** (*Acess Point* - AP);
Ex.: roteadores de banda larga.
- Existem também IBSS (*Infrastructure Basic Service Set*) onde é usado para interligar computadores a uma rede maior ou internet.

BSS (Basic Service Set)

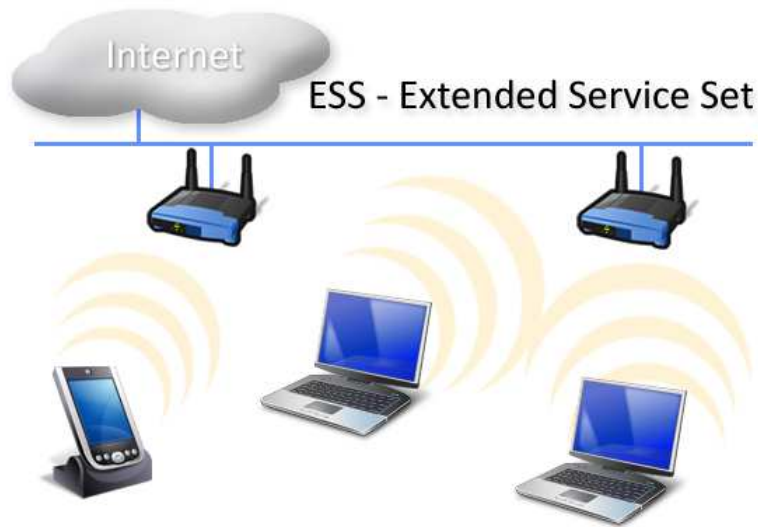
- A rede recebe um nome, chamado de **SSID** (Service Set ID).



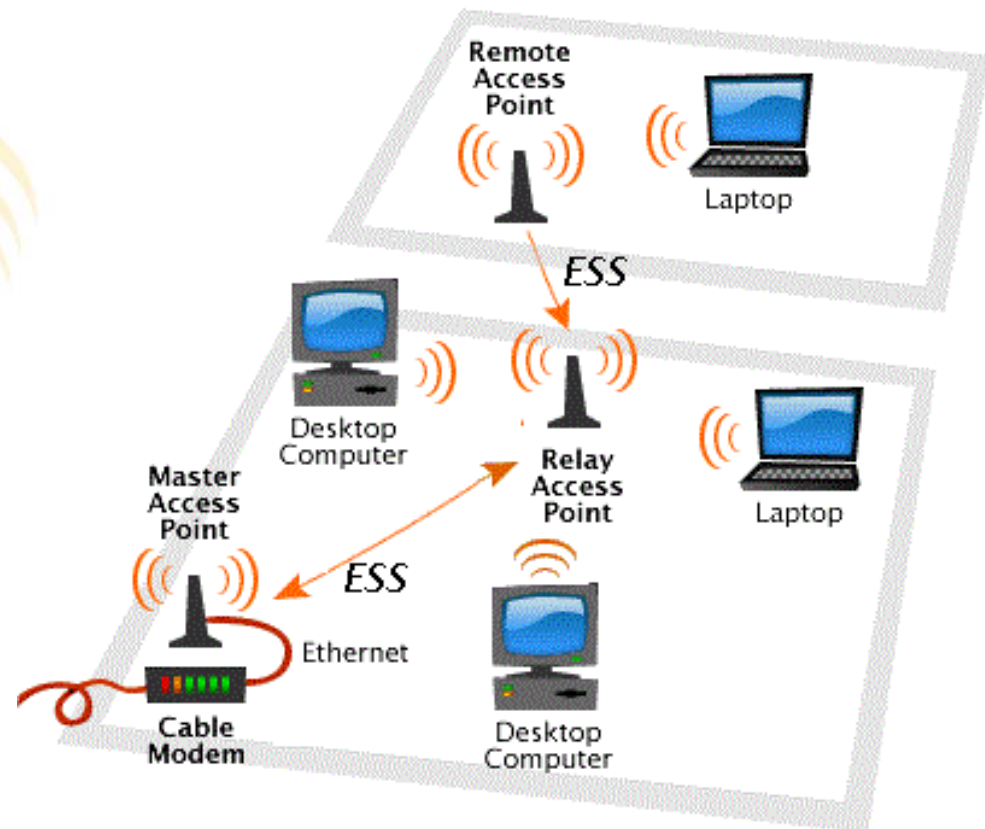
ESS – *Extended Service Set*

- São usados vários pontos de acesso formando uma rede maior com o mesmo SSID;
- Permite que o usuário mantenha a sua conectividade com a rede quando está em trânsito e sai do alcance de um ponto de acesso e entra no alcance de outro.

ESS – *Extended Service Set*



Qualquer periférico contendo uma placa de rede sem fio é chamado de *estação*.



ESS – *Extended Service Set*

Serviço da Estação:

- Autenticação;
- Desautenticação;
- Privacidade;
- Entrega de dados;
- Associação;
- Desassociação;
- Reassociação;
- Distribuição;
- Integração.

Criptografia

- WEP (Wired Equivalent Privacy);
- WPA (Wi-Fi Protected Access);
- WPA2 (Wi-Fi Protected Access 2);
- WPA3.

WEP (*Wired Equivalent Privacy*)

- **O WEP** foi desenvolvido para redes sem fio e aprovado como padrão de segurança Wi-Fi em setembro de 1999.
- Era destinado a oferecer o mesmo nível de segurança das redes cabeadas, no entanto, existem diversos problemas de segurança conhecidos no WEP e, além disso, ele é **fácil** de ser quebrado e difícil de ser configurado.
- Foi oficialmente abandonado pela Wi-Fi Alliance em 2004.

WPA (*Wi-Fi Protected Access*)

- No momento em que o padrão 802.11i de segurança sem fio estava sendo desenvolvido, o WPA foi usado como uma melhoria temporária de segurança para o WEP.
- Um ano antes do WEP ser abandonado oficialmente, o WPA foi formalmente adotado.

- A maioria dos aplicativos WPA modernos usa uma chave pré-compartilhada (PSK), mais conhecida como WPA Persona e o protocolo *Temporal Key Integrity Protocol* ou TKIP para criptografia.
- O WPA *Enterprise* usa um servidor de autenticação para gerar chaves e certificados.
- Os ataques que representavam a maior ameaça para o protocolo, não eram feitos diretamente, mas sim através do sistema *Wi-Fi Protected Setup* (WPS) - sistema auxiliar desenvolvido para simplificar a conexão dos dispositivos aos pontos de acesso modernos.

WPA2 (Wi-Fi Protected Access 2)

- O protocolo de segurança baseado no padrão sem-fio 802.11i foi introduzido em 2004.
- A melhoria mais importante adicionada ao WPA2 em relação ao WPA foi o uso do *Advanced Encryption Standard* (AES).
- O AES foi aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como **secretas**, portanto, deve ser bom o suficiente para proteger redes domésticas.

- Neste momento, a principal vulnerabilidade de um sistema WPA2 é quando o atacante já tem acesso a rede Wi-Fi segura e consegue obter acesso a certas chaves para executar um ataque a outros dispositivos na rede.
- Dito isto, as sugestões de segurança para as vulnerabilidades conhecidas do WPA2 são, em sua maioria, significativas apenas para as redes de nível empresarial e não são realmente relevantes para as pequenas redes domésticas.
- Infelizmente, a possibilidade de ataques através do *Wi-Fi Protected Setup* (WPS), ainda é elevada nos pontos de acesso WPA2, algo que também é um problema com o WPA.

Qual o método de segurança irá funcionar em sua rede?

Classificação básica (do melhor ao pior) dos métodos de segurança WiFi disponíveis para os modernos (depois de 2006) roteadores:

- WPA2 + AES
- WPA + AES
- WPA + TKIP/AES (TKIP existe um método de fallback)
- WPA + TKIP
- WEP
- Rede Aberta (sem qualquer segurança)

Proteja sua rede Wi-Fi

- O WPA e o WPA2 permitem usar senhas de até 63 caracteres.
- Use o máximo possível de caracteres variados na sua senha da rede WiFi. (*letras maiúsculas e minúsculas, números, caracteres especiais e acima de 8 dígitos*).
- Os hackers estão interessados em alvos mais fáceis, se eles não podem quebrar a sua senha em vários minutos, eles provavelmente irão procurar redes mais vulneráveis.

WPA3

- Proteger a rede Wi-Fi de hackers é uma das tarefas mais importantes da segurança cibernética.
- É por isso que a chegada do WPA3, o protocolo de segurança sem fio da próxima geração, merece atenção.
- Ele não apenas manterá as conexões Wi-Fi mais seguras, mas também ajudará a salvar você de suas próprias falhas de segurança.

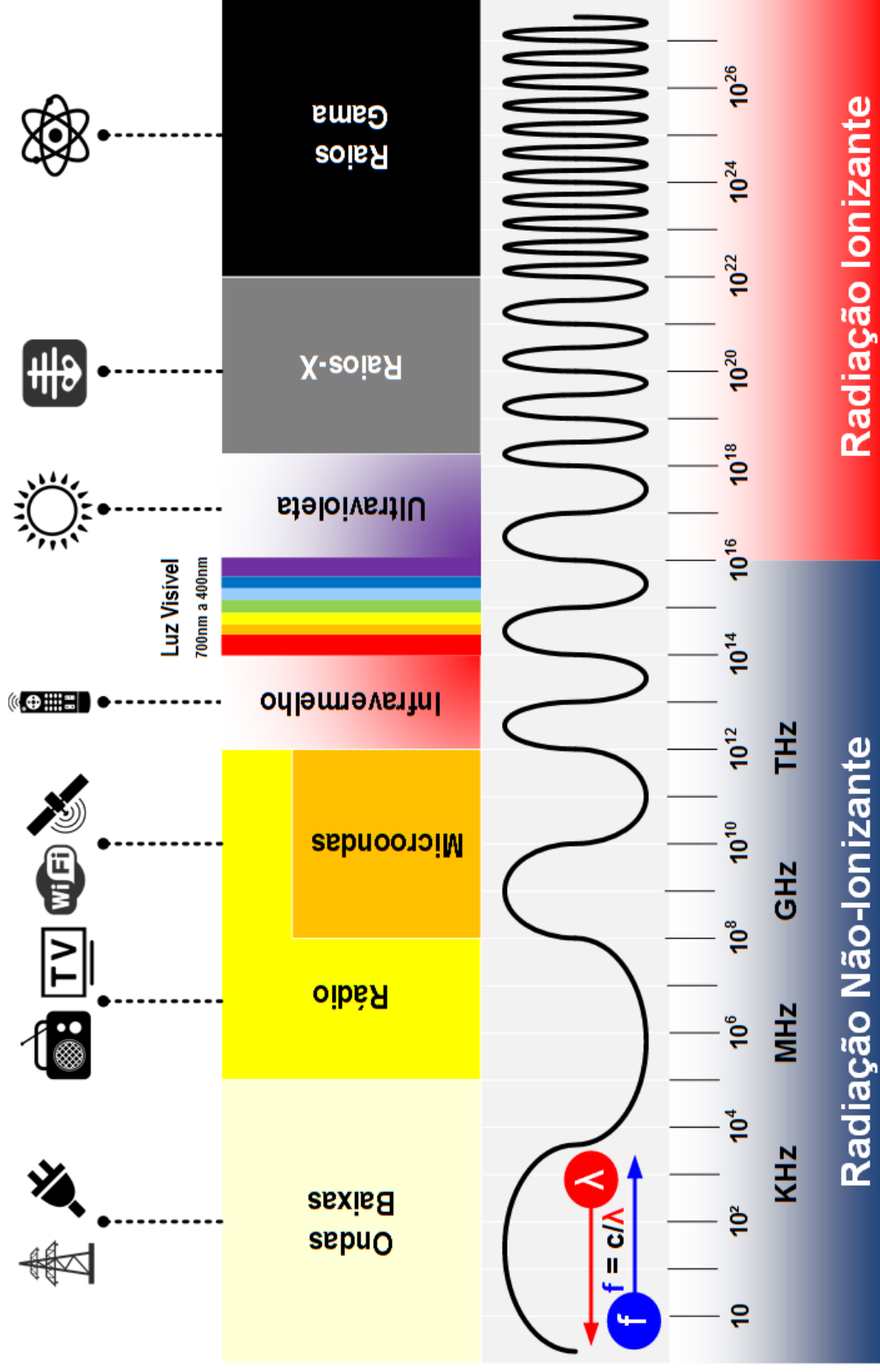
WPA3

Ele oferece:

- Proteção de Senha;
- Conexão mais seguras;
- Mais proteção em locais públicos;
- Mais amigável para IoT;
- Criptografia mais robusta.

Uso do Espectro

- Redes Wi-Fi operam transmitindo ondas de rádio;
- Duas faixas de frequências não regulamentadas:
 - 2,4 GHz;
 - 5GHz.



Uso da faixa de 2,4GHz

- EUA → 2.401MHz até 2.473MHz;
- Brasil → 2.401MHz até 2.483,5MHz;
- **Dividida em 14 canais:**
 - EUA → 11 canais;
 - Brasil → 13 canais.

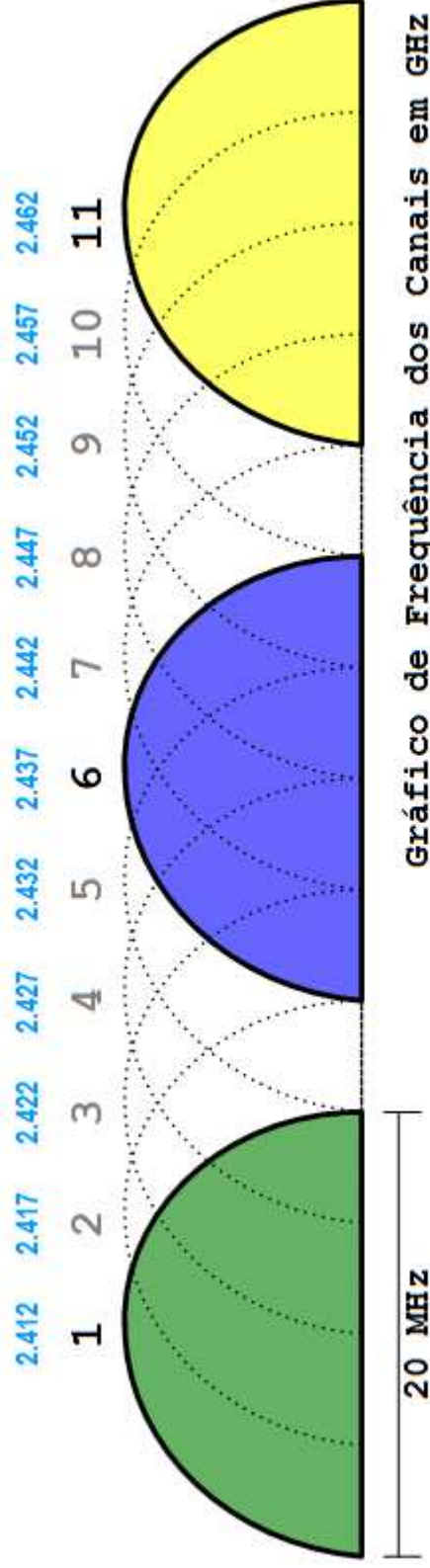


Gráfico de Frequência dos Canais em GHz

medium.com/ubntbr

Uso da faixa de 5 GHz

- Menos utilizada;
- Menos interferência;
- Maior taxa de transferência (*throughput*);
- Menor alcance;
- Vai de 5.150 MHz até 5.350 MHz, depois de 5.725 MHz até 5.835MHz.
- Dividida em 13 canais.

Tabela 6.9: Canais da banda de 5 GHz.

Canal	Frequência inferior	Frequência central	Frequência superior	Banda
Canal 36	5.170 MHz	5.180 MHz	5.190 MHz	Inferior
Canal 40	5.190 MHz	5.200 MHz	5.210 MHz	Inferior
Canal 44	5.210 MHz	5.220 MHz	5.230 MHz	Inferior
Canal 48	5.230 MHz	5.240 MHz	5.250 MHz	Inferior
Canal 52	5.250 MHz	5.260 MHz	5.270 MHz	Central
Canal 56	5.270 MHz	5.280 MHz	5.290 MHz	Central
Canal 60	5.290 MHz	5.300 MHz	5.310 MHz	Central
Canal 64	5.310 MHz	5.320 MHz	5.330 MHz	Central
Canal 149	5.735 MHz	5.745 MHz	5.755 MHz	Superior
Canal 153	5.755 MHz	5.765 MHz	5.775 MHz	Superior
Canal 157	5.775 MHz	5.785 MHz	5.795 MHz	Superior
Canal 161	5.795 MHz	5.805 MHz	5.815 MHz	Superior
Canal 165	5.815 MHz	5.825 MHz	5.835 MHz	Superior

Principais padrões

- Os principais padrões na família IEEE 802.11 são:
 - **IEEE 802.11:** para frequência 2.4 GHz com capacidade teórica de 2 Mbps.
 - **IEEE 802.11a:** para frequência 5 GHz com capacidade teórica de 54 Mbps.
 - **IEEE 802.11b:** para frequência 2,4 GHz com capacidade teórica de 11 Mbps. Este padrão utiliza DSSS (*Direct Sequency Spread Spectrum* – Sequência Direta de Espalhamento de Espectro) para diminuição de interferência.
 - **IEEE 802.11g:** para frequência 2,4 GHz com capacidade teórica de 54 Mbps.
 - **IEEE 802.11n:** para frequência 2,4 GHz e/ou 5 GHz com capacidade de 150 a 600 Mbps. Esse padrão utiliza como método de transmissão MIMO-OFDM.

Tabela 6.11: Comparação entre protocolos da camada física.

Protocolo	Taxa de transferência máxima	Frequência	Modo	Modulação
802.11-1997	2 Mbps	2,4 GHz	FHSS ou DSSS	Barker + PSK (DSSS) ou Barker + GFSK (FHSS)
802.11b	11 Mbps	2,4 GHz	DSSS	CCK + DQPSK
802.11a	54 Mbps	5 GHz	OFDM	Ver Tabela 6.12
802.11g	54 Mbps	2,4 GHz	OFDM	Ver Tabela 6.12
802.11n	600 Mbps ¹	2,4 GHz ou 5 GHz	MIMO-OFDM	Ver Tabela 6.13
802.11ac	7 Gbps ²	5 GHz	MIMO-OFDM	Ver Tabelas 6.15 e 6.16
802.11ad	7 Gbps	60 GHz	MIMO-OFDM	Não disponível

802.11g	11 Mbps	2,4 GHz	DSSS	CCK + DQPSK
802.11n	600 Mbps ¹	2,4 GHz ou 5 GHz	MIMO-OFDM	Ver Tabela 6.13
802.11ac	7 Gbps ²	5 GHz	MIMO-OFDM	Ver Tabelas 6.15 e 6.16

Referências Bibliográficas

- <https://www.techtudo.com.br/noticias/2018/04/tudo-sobre-o-protocolo-wpa3-que-deixa-a-internet-wi-fi-mais-segura.ghml>
- <https://www.netspotapp.com/pt/wifi-encryption-and-security.html>
- Torres, Gabriel. Redes de Computadores, 2ª edição. Nova Terra, 2014.