# Redes Wireless (Wi-Fi)

# WIRELESS

- O termo wireless, significa sem fio, possui alguns sinônimos tais como:
  - **Rede sem fio**
  - **Comunicação sem fio**
  - **Computação Móvel**
  - **Wi-FI?**

# WI-FI?


- Wi-Fi é uma marca registrada pela ***Wi-Fi Alliance***, a expressão se tornou um sinônimo de redes sem fio.

- A origem do termo, diferente do que muito acreditam e não tem um significado específico.

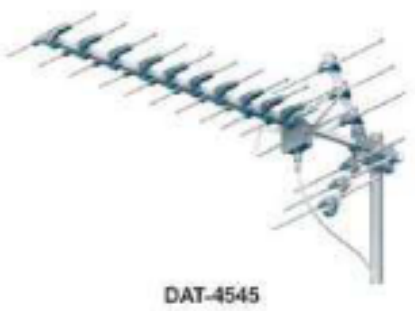
- A expressão Wi-Fi surgiu como uma alusão à expressão ***High Fidelity (Hi-Fi),*** utilizada pela indústria fonográfica na década de 50.

- Wi-Fi nada mais é do que a contração das palavras Wireless Fidelity

# O QUE É UMA REDE WIRELESS?

- A comunicação sem fio é baseada no estabelecimento da comunicação por meio de ondas eletromagnéticas que são propagadas pelo espaço.

- Como exemplo deste tipo de transmissão temos a comunicação via rádio Am e FM e a própria televisão.




# VANTAGENS

- Flexibilidade
  - Em uma área de cobertura pode se comunicar sem nenhuma restrição, limitada apenas por velocidade. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar.
- Facilidade
  - A instalação rápida, é evitada a passagem de cabos através de paredes e forros, usa o espaço físico eficientemente.
- Redução de custo
  - Mesmo possuindo um custo inicial maior, sua manutenção é muito mais barata.

# DESVANTAGENS

- Qualidade de serviço
  - A qualidade do serviço ainda é inferior que a das redes *cabeadas* devido a pequena banda que é limitada pela forma de transmissão (radiotransmissão) e a alta taxa de erro devido à interferência.
- Custo
  - O preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes *cabeadas*.
- Segurança
  - Os canais sem fio são mais suscetíveis a interceptores, pode interferir em outros equipamentos, como por exemplo, os utilizados em hospitais. Equipamentos elétricos são capazes de interferir na transmissão acarretando em alta taxa de erros na transmissão.

# INDICAÇÕES

- Seu uso é indicado sempre que for inviável ou muito difícil a instalação de cabos. As situações em que podem ser interessante instalar redes sem fio são:
  - Exposições na qual não existe infra-estrutura pronta para um cabeamento normal;
  - Salas de reuniões onde computadores são instalados deforma provisória.
  - Em uma residência, onde pode ser inviável quebrar paredes para instalar cabos, ou fixar cabos através dos rodapés.

# Padrão IEEE

- O padrão 802.11 para redes locais sem fio criado na década de 90, especifica várias velocidades e freqüências.


## IEEE 802.11


- São identificados por letras e cada um deles define como as informações são codificadas, as freqüências e as velocidades de transmissão possíveis

- **802.11a**
- **802.11b**
- 802.11d
- 802.11e
- 802.11f
- **802.11g**
- 802.11h
- 802.11i
- 802.11k
- 802.11m
- **802.11n**
- 802.11p
- 802.11r
- 802.11s
- 802.11t
- 802.11u
- 802.11v
- 802.11x
- 802.11w
- 802.11z

# IEEE 802.11

- IEEE 802.11a
  - Trabalha com Freqüência de 5.1 a 5.8 Ghz
  - velocidade de transmissão de até 54 Mbps
  - *Este padrão não é comum nos equipamentos fabricados no Brasil*

- IEEE 802.11g
  - freqüência de 2,4 Ghz
  - transmissão de até 54 Mbps
  - é o padrão mais utilizados em equipamentos wireless

- IEEE 802.11n
  - pode trabalhar a 2,4 Ghz como a 5 Ghz
  - Transmissão de até 150 Mbps.

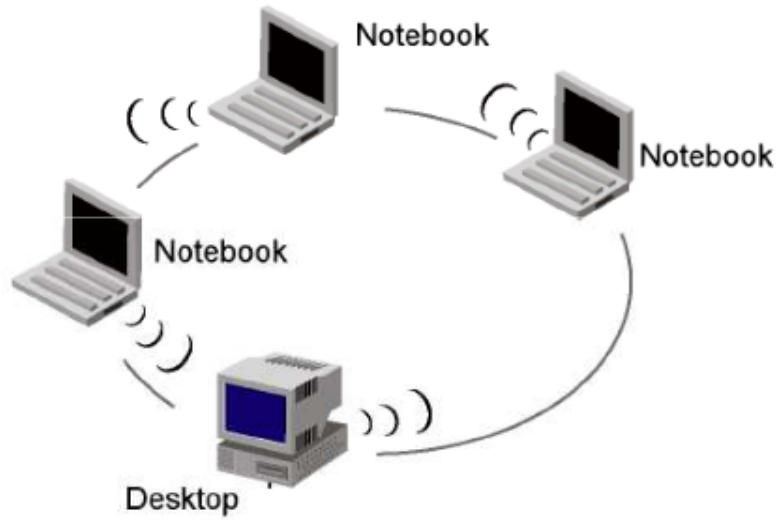
- IEEE 802.11b
  - freqüência de 2,4 Ghz
  - transmissão de até 11 Mbps

| IEEE 802.11 | Freqüência | Taxa de Transmissão | Alcance indoor/outdoor |
|---|---|---|---|
| **802.11b** | 2.4 GHz | 11 Mbps | 30m / 160m |
| **802.11a** | 5 GHz | 54 Mbps | 15m / 80m |
| **802.11g** | 2.4 GHz | 54 Mbps | |
| **802.11h** | 5 GHz | 54 Mbps | 15m / 80m |
| **802.11n** | 2.4 GHz / 5 GHz | 300 – 600 Mbps | 400m / – |

- O alcance depende de vários fatores.
  - Obstáculos atenuam o sinal.
    - Paredes
    - Móveis
    - Colunas
    - Espelhos
    - Objetos de metal

# ARQUITETURAS AD-HOC

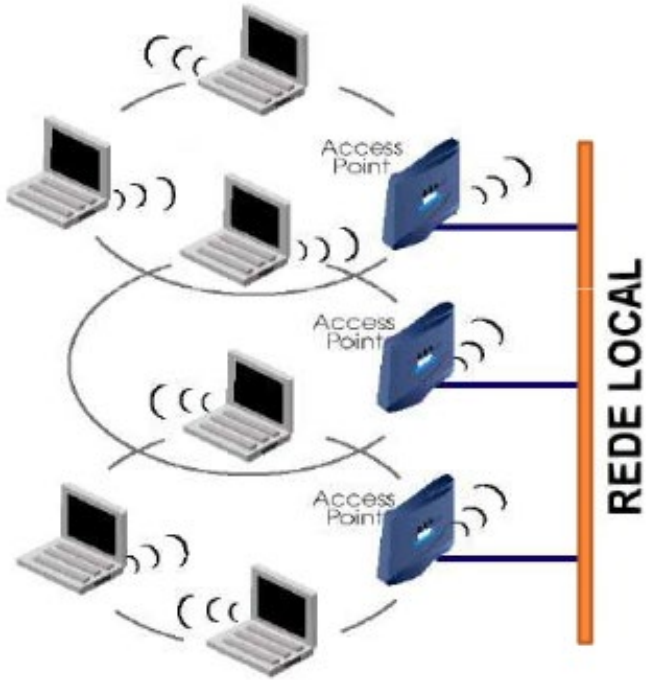
- Uma rede sem fio é “AD-HOC” quando não possui cabos de rede.
  - AD-HOC
    - Em termos simples uma rede Ad Hoc é uma rede em que não é necessário um Acess Point ou ponto de acesso.
- Todos os dispositivos devem utilizar apenas placas de rede wireless.
- Cada dispositivo é capaz de transmitir e receber informações para todos os demais.

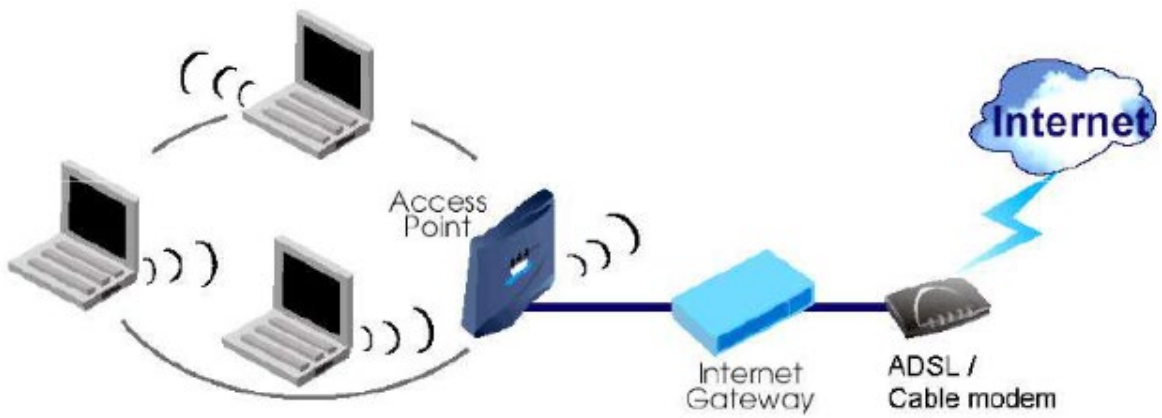



**NÃO CONFUNDA COM TOPOLOGIA ANEL!!!**

# Access Point

- Uma rede sem fio pode ser integrada a uma rede *cabeada* por meio de aparelhos chamados “Access Points” pontos de acesso.
- Pode ser utilizado com forma de aumentar a cobertura da rede.
- O **access point** faz o papel do hub ou switch na rede sem fio. É preciso ter ainda o roteador e o modem caso seja necessária a comunicação com outras redes e a internet.
- Existem aparelhos que acumulam as funções de ***Access Point*** e roteador.



## Access point

## Placa de rede PCI Wi-Fi

- Não só os dispositivos móveis podem fazer parte de uma rede sem fio. Computadores desktop também podem, com a instalação de uma placa de interface PCI Wi-Fi apropriada.

## Adaptador Wireless

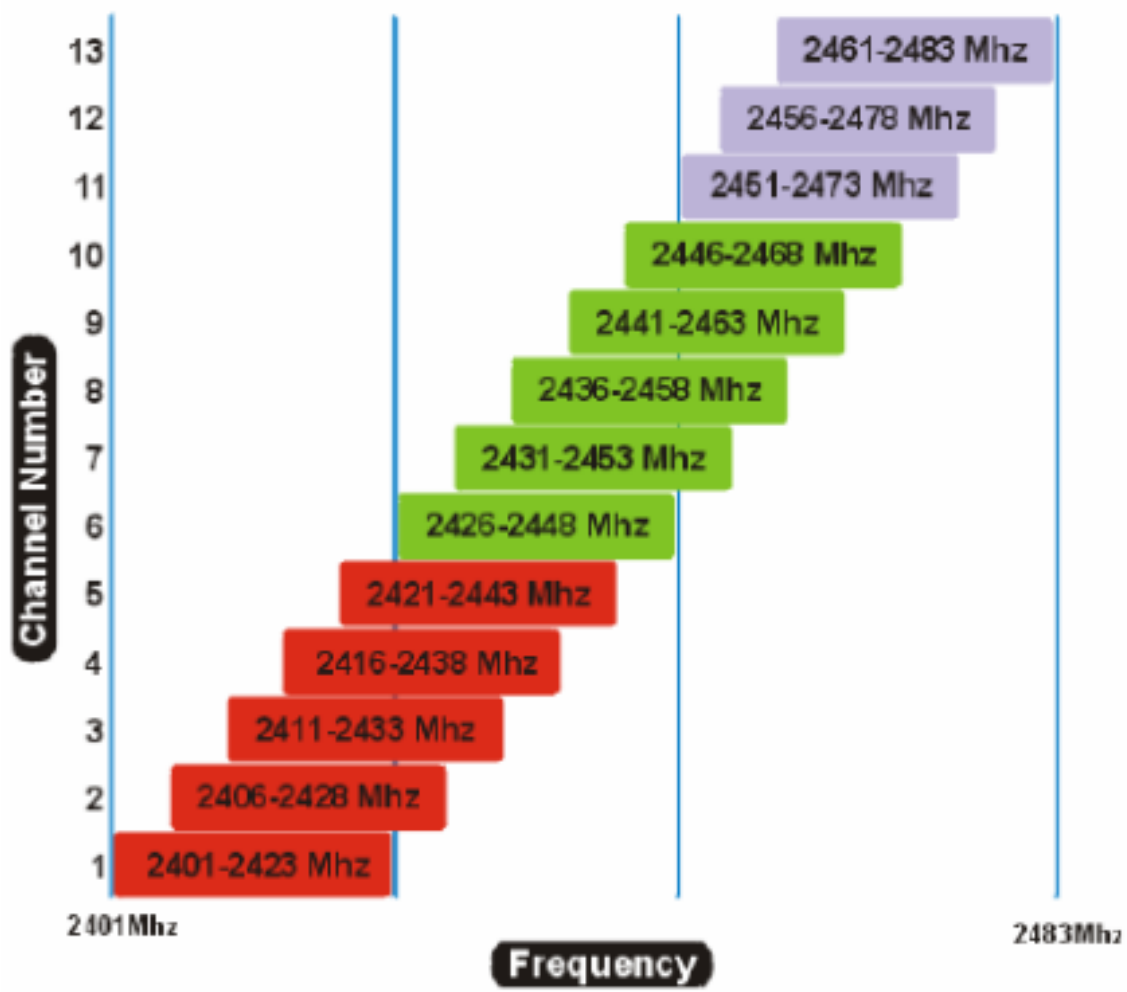
- Funcionam como placas de rede wireless, mas, utilizam interface usb.

- São indicados nos casos onde há impossibilidade de conectar placas PCI ou PCMCIA .

# Canais e associação

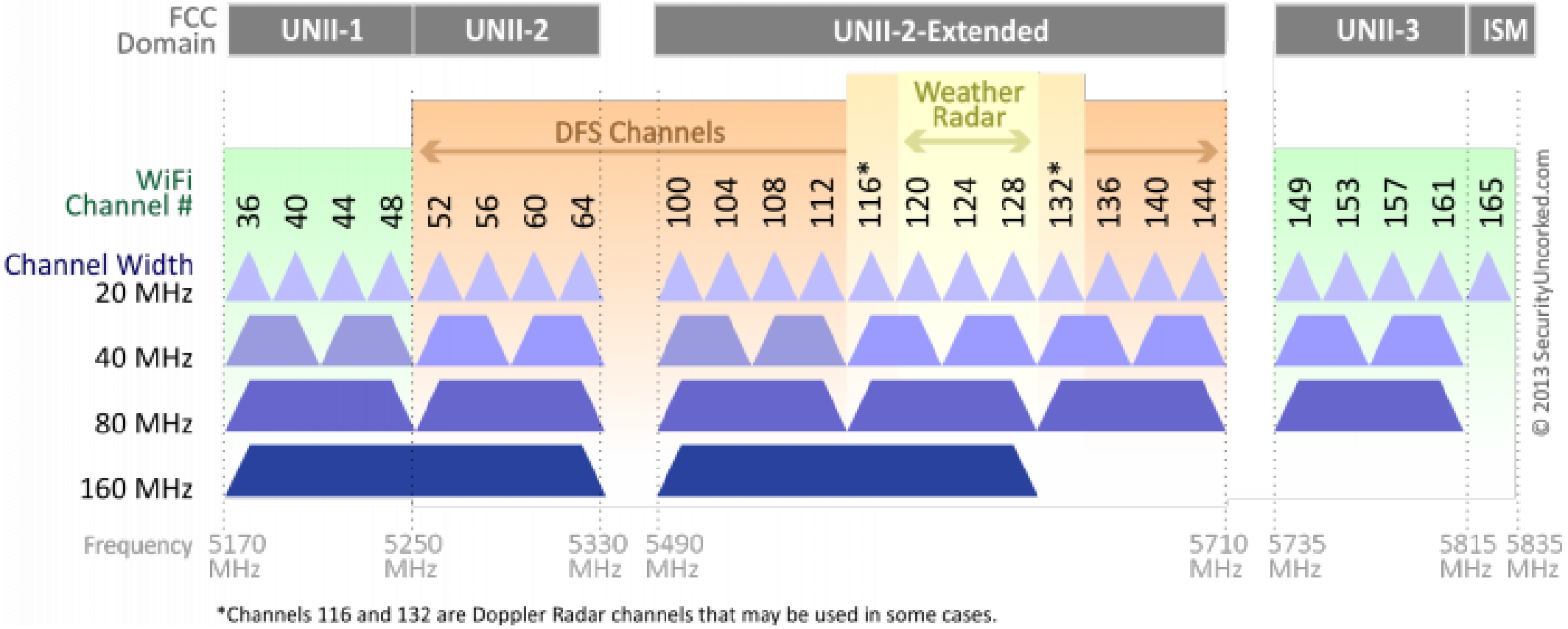
- Em 802.11, cada estação sem fio precisa se associar com um AP antes de poder enviar ou receber dados da camada de rede.
- Ao instalar um AP, um administrador de rede designa ao ponto de acesso um **Identificador de Conjunto de Serviços** composto de uma ou duas palavras.
- Ele também deve designar um número de canal ao AP.
- Uma **selva de Wi-Fis** é qualquer localização física na qual uma estação sem fio recebe um sinal suficientemente forte de dois ou mais APs.

# Canais e associação




Source: www.draytek.co.uk/support

# 802.11ac Channel Allocation (N America)




*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

# Redes wireless se chocam ?

- Se por acaso outras pessoas estiverem conversando ao mesmo momento, pode ser difícil distinguir o que a pessoa que você está conversando está dizendo em meio ao caos de vozes.
- Com as redes sem fio esse tipo de problema também ocorre. Como elas se comunicam em frequências específicas,

outros aparelhos que trabalham nessas frequências atrapalham a comunicação.

**Telefones sem fio, micro-ondas, dispositivos bluetooth e outros dispositivos sem fio**, como outras redes sem fio interferem no sinal Wi-Fi.

"Como assim, um Wi-Fi atrapalha outro?”

- Bem, sim e não. Se dois equipamentos trabalharem em frequências diferentes esse problema não ocorre,

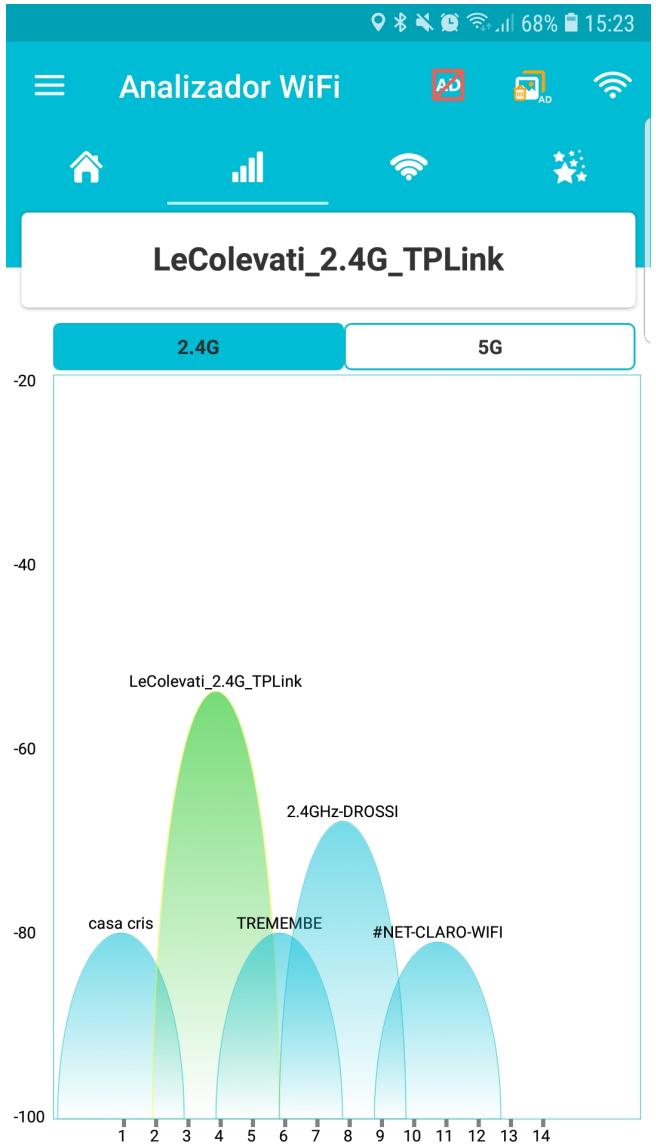
pois seria como se duas pessoas estivessem se comunicando por voz e outras duas estivessem por texto. As “frequências” não se encontram.

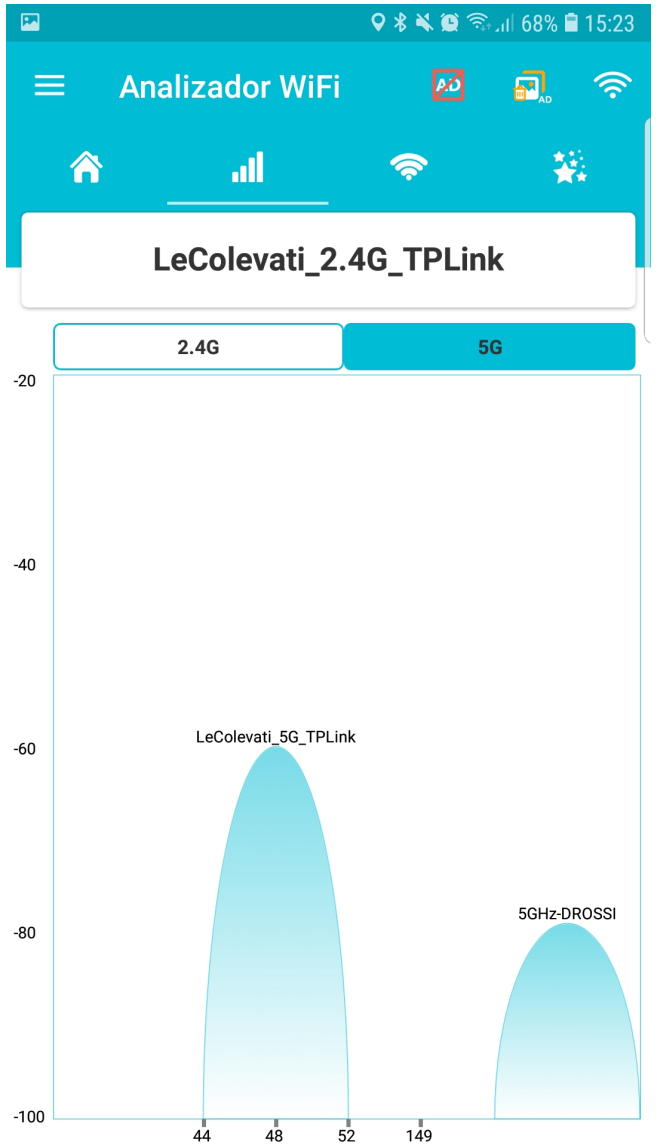
- Agora, se dois equipamentos trabalharem na mesma faixa de frequência, isso já se torna perceptível.

- “Existe alguma maneira de resolvermos esse problema?”
- Existe uma possibilidade, que é de modificar um pouco a frequência na qual a rede atua. Assim o sinal de uma não interfere em outra.

- Quando alteramos essa pequena fração da frequência, falamos que estamos **alterando o canal da rede sem fio.**

# Analisador Wi-fi



# Segurança


## WEP. Wired Equivalent Privacy

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

1 ★☆☆☆☆ Segurança • Fraca

1 ★☆☆☆☆ Configuração • Difícil

---

**O WEP** foi desenvolvido para redes sem fio e aprovado como padrão de segurança Wi-Fi em setembro de 1999. O WEP 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.

Apesar de todo o trabalho que tem sido feito para melhorar o sistema WEP, ele ainda é uma solução altamente vulnerável. Os sistemas que dependem deste protocolo devem ser ou atualizados ou substituídos por dispositivos caso a atualização da segurança não esteja disponível. O WEP foi oficialmente abandonado pela Wi-Fi Alliance em 2004.

# Segurança


## WPA. Wi-Fi Protected Access

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

2 ★★☆☆☆ Segurança • Fraca

3 ★★★☆☆ Configuração • Mais ou menos

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 (/ti?'k?p/) para criptografia. O WPA Enterprise usa um servidor de autenticação para gerar chaves e certificados.

O WPA foi uma melhoria significativa sobre o WEP, mas como os principais componentes foram feitos para que eles pudessem ser implementados através de atualizações de firmware em dispositivos habilitados para WEP, ele ainda se baseava em elementos vulneráveis.

O WPA, assim como WEP, depois de sido submetido a uma prova de conceito e aplicado a demonstrações públicas acabou, por sua vez, sendo muito vulnerável a invasões. 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.

# Segurança


## WPA2. Versão 2 do Wi-Fi Protected Access

Desde 2004. Criptografia AES.

4 ★★★★☆ Segurança • Boa

4 ★★★★☆ Configuração • Normal

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

***O ADVANCED ENCRYPTION STANDARD É APROVADO PELO GOVERNO DOS EUA***

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.

# WPS

- WPS é a sigla de *Wi-Fi Protected Setup,* ou configuração protegida de Wi-Fi. Seu objetivo é facilitar a conexão do dispositivo sem fio com o roteador. O WPS faz com que não seja necessário conectar a rede Wi-Fi e somente depois inserir uma senha.
- Tudo isso acontece por conta do protocolo criptografado WPA (*Wi-Fi Protected Access*) criando um PIN dentro do roteador. Esse PIN é usado para conectar o dispositivo wireless ao SSID (*Service Set Identifier*), ou simplesmente o “nome” da sua rede, que aparece ao buscar conexões no dispositivo.

# WPS – Utilização e Segurança

- Utilizando a configuração protegida você entra automaticamente em uma rede, sem necessidade de incluir senha. Quando acionado o botão WPS, caso tenha, o aparelho sem fio já conecta automaticamente, pelo PIN do roteador criado por WPA. O responsável por essa função é o WPS.
- É importante lembrar que neste tipo de conexão a senha não é criada ou modificada pelo usuário. Por padrão, é gerada automaticamente.

- Não é tão seguro. A maioria dos roteadores atuais não tem o botão WPS, a função já vem disponível o tempo todo, mesmo sem o usuário saber. Qual é o grande problema? O protocolo WPA e WPA2 são muito seguros, somente quando as senhas são feitas com letras, maiúscula e minúscula, números e caracteres especiais.
- O PIN criado pelo roteador é simples, dentro do protocolo WPA, somente com números. Como não pode ser alterada pelo usuário isso deixa a conexão vulnerável. Uma vez conectado, se tem acesso a rede e todos os arquivos que transitam nela.
- Com uma busca rápida na internet encontramos diversos softwares, criados para decodificar o PIN de um roteador que utiliza WPS, utilizando da força bruta para descobrir o código .

# Bibiliografia

Notas de Aula:

Prof. M.Sc. Helio Esperidião – Univap

Prof. Rodrigo Ronner T. da Silva – IFRN

Netspotapp.com