Laboratório de Hardware

Redes Wireless

Redes Wireless

- O termo Wireless, que significa sem fio, possui alguns sinônimos, tais como:
  - Rede sem fio
  - Comunicação sem fio
  - Computação móvel
  - Wi-Fi

Wi-Fi

- Marca registrada pela Wi-Fi Alliance
- Expressão tornou-se sinônimo de redes sem fio
- A origem do termo, diferente do que muitos acreditam, 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
- Portanto, Wi-Fi é 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 comunicação via rádio AM e FM e a própria televisão

Vantagens da rede wireless

- Flexibilidade
  - Em uma área de cobertura pode se comunicar sem nenhuma restrição, limitada apenas por velocidade.
  - Permite que a rede alcance locais onde fios não podem passar ou chegar.
- Facilidade
  - Rápida instalação
  - Evita passagens de fios por paredes e forros
  - Eficiência no uso do espaço físico
- Redução de Custo
  - O custo inicial pode ser maior, mas a manutenção é mais barata

Desvantagens da rede wireless

- Qualidade de Serviço
  - A qualidade de serviço ainda é, em média, inferior às redes cabeadas devido à restrição de banda limitada pela forma de transmissão (radiotransmissão) e a alta taxa de erros devido à interferência
- Custo inicial
  - Custo de alguns equipamentos de Redes sem Fio podem ser mais altos para se inicializar uma rede Wi-Fi
- Segurança
  - Os canais sem fio são mais suscetíveis a interceptores
  - Interferências em outros equipamentos, como por exemplo os hospitalares. Equipamentos elétricos podem causar interferência e aumento na taxa de erros na transmissão

Indicações de uso para rede wireless

- Indicado sempre que for inviável ou muito difícil a instalação de cabos. Exemplos de situações para redes sem fio:
  - Ofertar recursos de rede para dispositivos móveis
  - Edificações temporárias sem infraestrutura para cabeamento
  - Salas de uso compartilhado e com mudança recorrente de público, como salas de reunião
  - Ambientes residenciais onde a quebra de paredes é inviável para instalação de cabos, ou difícil até mesmo a passagem de cabos por rodapés

Padrão IEEE para redes wireless

- Padrão 802.11 para redes locais sem fio, criado na década de 90, específica para várias taxas e frequências
  - São identificados por letras e cada um deles define como as informações são codificadas, as frequências e as taxas 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 frequências de 5.1 a 5.8 GHz
  - Transmissão de até 54 Mbps
  - Não comum nos equipamentos brasileiros
  - Alcance 15m (Indoor) e 80m (Outdoor)
- IEEE 802.11b
  - Frequência de 2.4 GHz
  - Transmissão de até 11Mbps
  - Alcance 30m (Indoor) e 160m (Outdoor)
- IEEE 802.11g
  - Frequência de 2.4 GHz
  - Transmissão de 54 Mbps
  - Alcance de 100m (Indoor)
- IEEE 802.11n – Wi-Fi 4
  - Pode trabalhar em frequências de 2.4 GHz e 5 GHz
  - Transmissão de até 300Mbps (2.4 GHz) e 600Mbps (5 GHz)
  - Utiliza Tecnologia MIMO
    - O termo significa “inputs múltiplos, outputs múltiplos” (*“multiple input, multiple outputs”*). O MIMO usa várias antenas conectadas no mesmo dispositivo, que operam em conjunto para minimizar erros, otimizar a velocidade de dados e melhorar a capacidade de transmissão.

IEEE 802.11

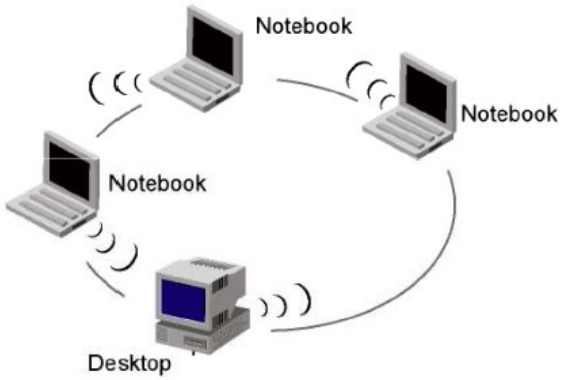
- 802.11ac (Wi-Fi 5):
  - Lançado em 2013
  - Opera exclusivamente na frequência de 5 GHz
  - Usa tecnologia MU-MIMO
    - Em um sistema MU-MIMO, cada antena do roteador ficaria encarregada de transmitir um dado diferente para cada usuário (dispositivo) conectado. Dependendo da configuração, ele pode contar com duas ou três antenas para transmissão, e outras duas ou três para recepção de dados. Assim, um par ficaria dedicado ao PC, e outro a um videogame, sem que haja interrupção da conexão.
  - Suportar Beamforming.
    - Técnica de processamento de sinal que concentra a transmissão de dados em direção a dispositivos específicos, em vez de irradiar em todas as direções
- 802.11ax (Wi-Fi 6 e 6E):
  - Lançado em 2021, o padrão 802.11ax
  - Utiliza as frequências de 2,4 GHz e 5 GHz,
    - A versão Wi-Fi 6E também utiliza o espectro de 6 GHz.
  - O Wi-Fi 6/6E tem velocidade máxima teórica de 9,6 Gb/s.
- 802.11be (Wi-Fi 7):
  - Certificação em 2024
  - Pode chegar a velocidades de até 46,1 Gb/s.
  - Seu principal diferencial é a agregação multi-link, que permite comunicação em mais de uma frequência simultânea entre o dispositivo e o roteador.

IEEE 802.11

- O alcance do sinal depende de vários fatores
  - Obstáculos atenuam o sinal
    - Paredes
    - Móveis
    - Colunas
    - Espelhos
    - Objetos de metal
  - A antena deve estar sempre no local mais alto possível
    - Sinal Wi-Fi no “sobe”
    - A distribuição em formato de parábola

Redes AD-HOC

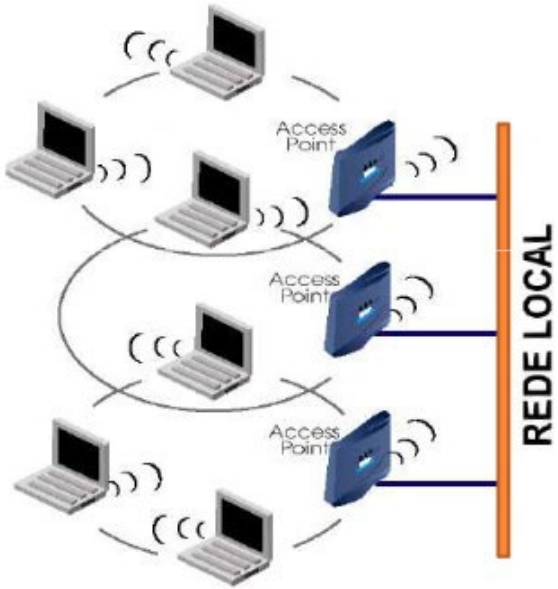
- Uma rede sem fio é “AD-HOC” quando não possui cabos de rede
  - Uma rede AD-HOC é uma rede em que não é necessário Access Point (Ponto de Acesso)
- Todos os dispositivos devem utilizar apenas placas de rede wireless
- Cada dispositivo é capaz de transmitir e receber informações para todos os demais

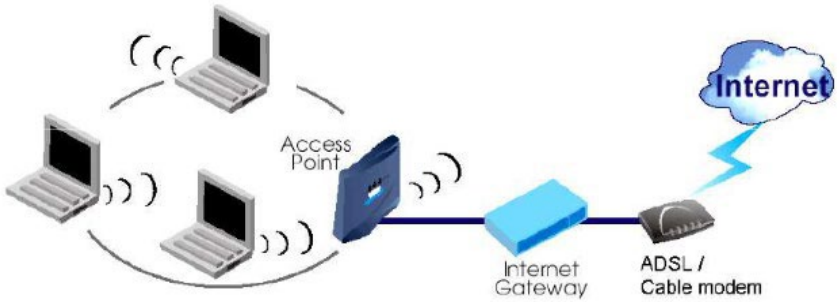


NÃO CONFUNDA COM TOPOLOGIA ANEL!!!

Access Point (Ponto de Acesso)

- Uma rede sem fio pode ser integrada a uma rede cabeada por meio de aparelhos chamados Access Point
- Pode ser utilizado como forma de aumentar a cobertura de rede
- O Access Point faz o papel do hub ou switch na rede sem fio. É preciso ter ainda um roteador e um modem caso seja necessária a comunicação com outras redes e a internet.
- Pode-se contemplar Modem, Roteador, Switch e Access Point no mesmo aparelho





Access Point (Ponto de Acesso)

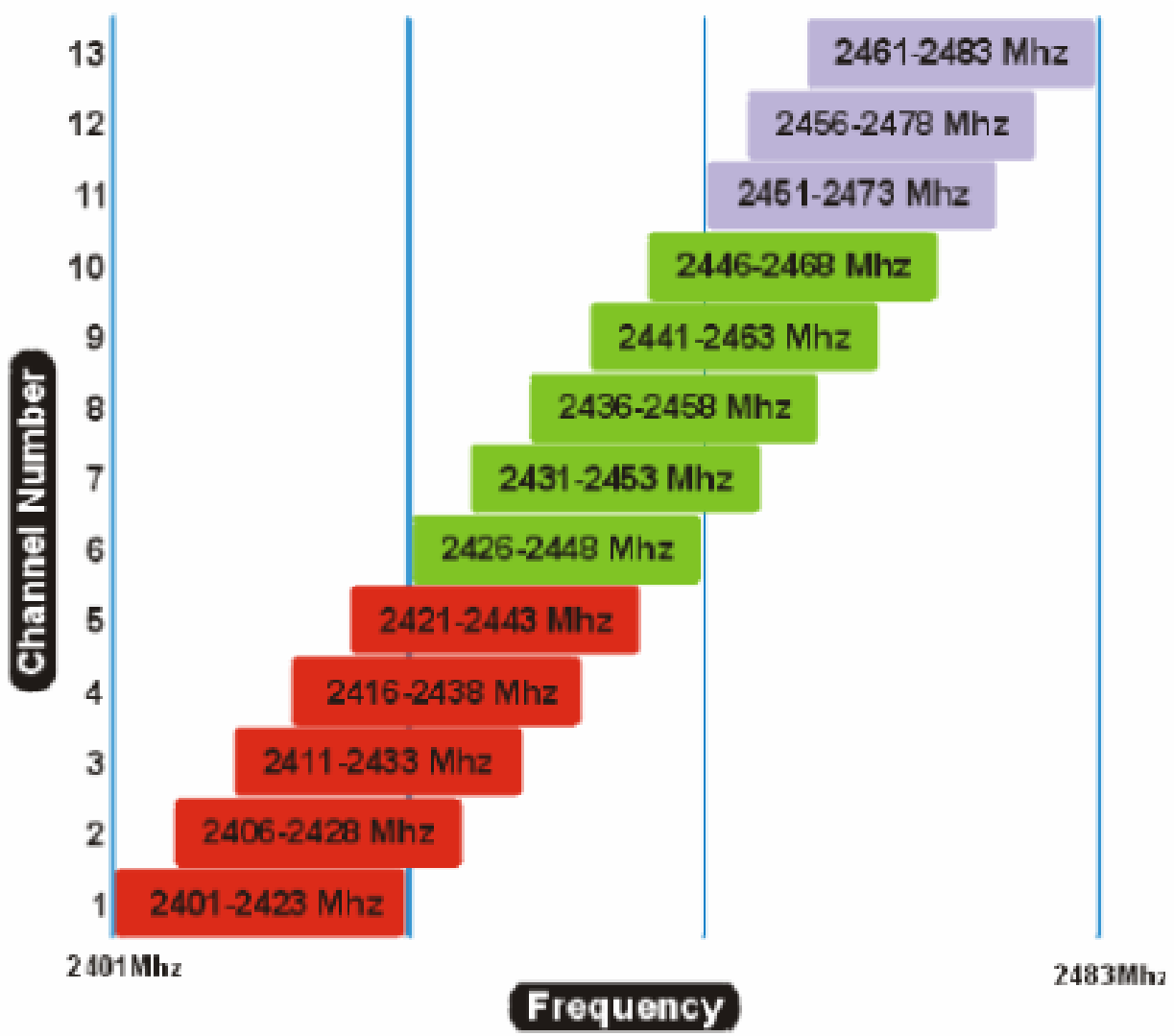
Dispositivos de Conexão

- Não apenas dispositivos móveis, com interfaces Wi-Fi integradas podem fazer parte de uma rede sem fio
- Computadores desktop, por exemplo, podem fazer parte da rede com placas de interface PCI ou PCI Express apropriada
- Adaptadores Wireless funcionam como as placas, mas utilizam interfaces de comunicação externa como a USB
  - São indicados quando há indisponibilidade de conectar placas

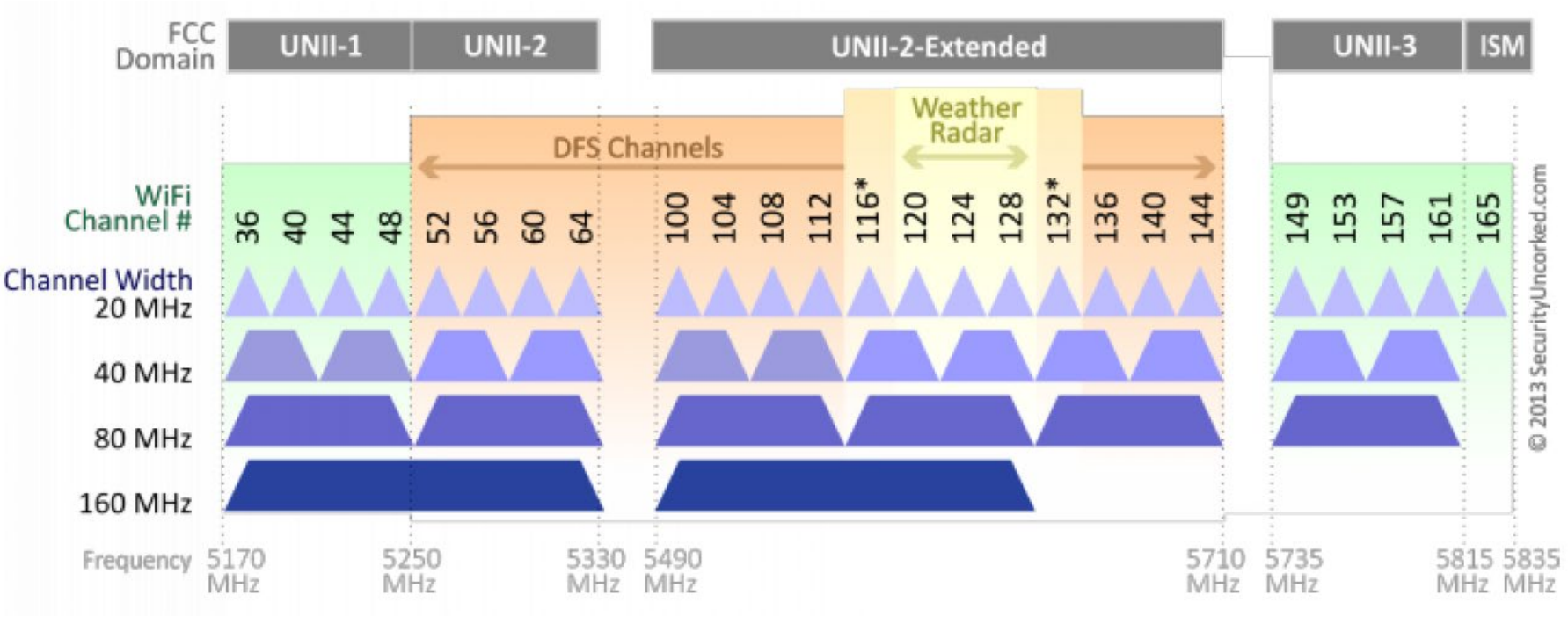
Canais e Faixas de Frequência

- A faixa de 2,4 GHz é utilizada pelos padrões 802.11b/g/n. Apesar do crescimento da popularidade da faixa de 5 GHz no Brasil, a faixa de 2,4 GHz ainda é comum. Contudo, sofre interferências de dispositivos como telefones sem fio, micro-ondas, fones Bluetooth, entre outros.
  - No Brasil, para a faixa de 2,4 GHz, a ANATEL permite a utilização de 13 canais de 20 MHz cada. Idealmente, é recomendável manter um espaço de 2 MHz entre canais para garantir proteção e atenuação ao longo da borda da célula do Access Point ou Roteador Wi-Fi.
- A faixa de 5 GHz é utilizada pelos padrões 802.11a/n/ac, oferecendo maior largura de banda e 24 canais no Brasil.
  - No Brasil 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. 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).

Canais e Faixas de Frequência



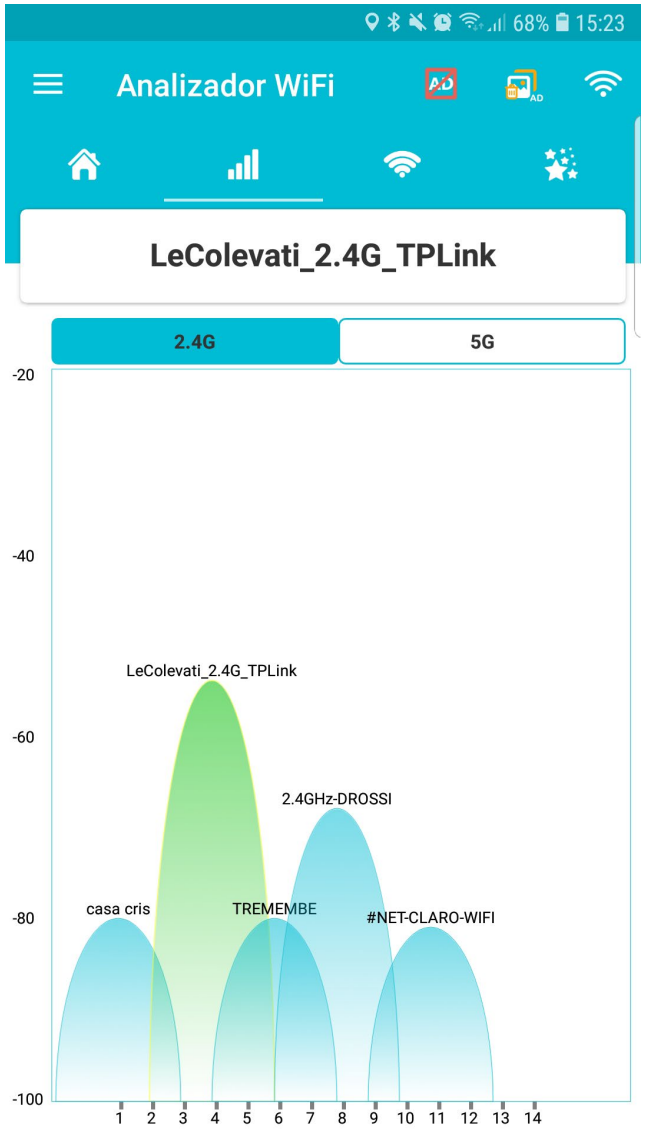
Canais e Faixas de Frequência

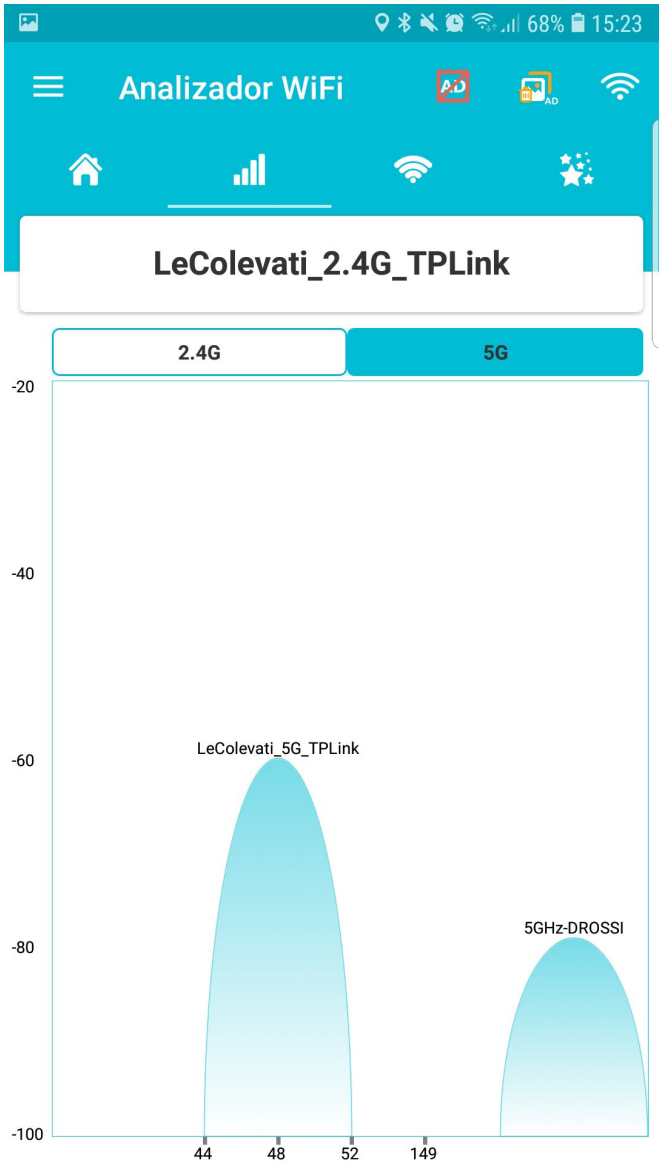


Canais e Faixas de Frequência

- Quando um grupo de pessoas está conversando em um mesmo ambiente, pode ser difícil distinguir o que é dito por uma determinada pessoa.
- Com as redes sem fio esse tipo de problema também ocorre. Como elas se comunicam em frequências específicas, outros aparelhos que trabalham na mesma frequência atrapalham a comunicação.
  - Telefones sem fio, Forno micro-ondas, Dispositivos bluetooth e outras redes sem fio interferem no sinal Wi-Fi
- Para não haver impacto de um aparelho de uma rede sem fio em outro, estes devem estar se comunicando em frequências diferentes.
  - Esse impacto podo ocorrer, inclusive entre vizinhos
  - O sinal da rede Wi-Fi ficará atenuado e pode inclusive ser "perdido" em alguns locais onde o choque de sinais é muito forte
- Quando aplicamos a mudança do canal da rede sem fio, aplicamos uma pequena mudança na frequência de comunicação, que nos leva a diminuir o impacto da frequência de outros aparelhos
- Atualmente, alguns Access Point fazem a mudança automática de canal caso identifiquem forte interferência.

Analisador Wi-Fi





Segurança - WEP

- Como as redes sem fio transmitem dados por meio de ondas de rádio, os dados podem ser facilmente interceptados, a menos que medidas de segurança sejam implementadas. Introduzido em 1997, o Wired Equivalent Privacy (WEP) foi a primeira tentativa de proteção sem fio. O objetivo era adicionar segurança às redes sem fio criptografando dados. Se os dados sem fio fossem interceptados, eles seriam irreconhecíveis para os interceptores, uma vez que haviam sido criptografados. No entanto, os sistemas autorizados na rede seriam capazes de reconhecer e descriptografar os dados. Isso ocorre porque os dispositivos na rede usam o mesmo algoritmo de criptografia.
- O WEP criptografa o tráfego usando uma chave de 64 ou 128 bits em hexadecimal. Esta é uma chave estática, o que significa que todo o tráfego, independentemente do dispositivo, é criptografado usando uma única chave. Uma chave WEP permite que os computadores em uma rede troquem mensagens codificadas enquanto escondem o conteúdo das mensagens de intrusos. Essa chave é usada para se conectar a uma rede habilitada para segurança sem fio.
- Um dos principais objetivos do WEP era evitar ataques Man-in-the-Middle, o que fez por um tempo. No entanto, apesar das revisões do protocolo e do aumento do tamanho da chave, várias falhas de segurança foram descobertas no padrão WEP ao longo do tempo. À medida que o poder da computação aumentava, ficou mais fácil explorar para os criminosos explorarem essas falhas. Devido às suas vulnerabilidades, a Wi-Fi Alliance retirou oficialmente o WEP em 2004. Hoje, a segurança WEP é considerada obsoleta, embora às vezes ainda esteja em uso, ou porque os administradores de rede não alteraram a segurança padrão em seus roteadores sem fio, ou porque os dispositivos são muito antigos para suportar métodos de criptografia mais recentes como WPA.

Segurança - WPA

- Wi-Fi Protected Access. Apresentado em 2003, este protocolo foi o substituto da Wi-Fi Alliance para WEP. Ele compartilhava semelhanças com o WEP, mas oferecia melhorias no modo como lida com as chaves de segurança e na forma como os usuários são autorizados. Enquanto o WEP fornece a cada sistema autorizado a mesma chave, o WPA usa o protocolo de integridade de chave temporal (TKIP), que altera dinamicamente a chave que os sistemas usam. Isso evita que invasores criem sua própria chave de criptografia para corresponder à usada pela rede segura. O padrão de criptografia TKIP foi posteriormente substituído pelo Advanced Encryption Standard (AES).
- Além disso, o WPA incluiu verificações de integridade de mensagens para determinar se um invasor capturou ou alterou pacotes de dados. As chaves usadas pelo WPA eram de 256 bits, um aumento significativo em relação às chaves de 64 e 128 bits usadas no sistema WEP. No entanto, apesar dessas melhorias, elementos do WPA passaram a ser explorados, o que levou ao WPA2.
- O WPA2 oferece criptografia mais poderosa do que o WPA original, corrigindo falhas anteriores. O WPA2 usa o Advanced Encryption System (AES), que utiliza chaves de até 256 bits para criptografar e descriptografar dados. O AES é usado pelo governo dos EUA para proteger dados confidenciais.
- O WPA2 opera em dois modos:
  - Modo pessoal ou chave pré-compartilhada (WPA2-PSK): Depende de uma senha compartilhada para acesso e é geralmente usado em ambientes domésticos.
  - Modo empresarial (WPA2-EAP): É mais adequado para uso organizacional ou empresarial.

Segurança – WPA 3

- WPA3 é a terceira iteração do protocolo Wi-Fi Protected Access. A Wi-Fi Alliance lançou o WPA3 em 2018. O WPA3 introduziu novos recursos para uso pessoal e empresarial, incluindo:
  - Criptografia de dados individualizada: ao fazer login em uma rede pública, o WPA3 inscreve um novo dispositivo por meio de um processo diferente de uma senha compartilhada. O WPA3 usa um sistema de protocolo de provisionamento de dispositivo (DPP) Wi-Fi que permite aos usuários usar tags NFC (Near Field Communication) ou códigos QR para permitir dispositivos na rede. Além disso, a segurança WPA3 usa criptografia GCMP-256 em vez da criptografia de 128 bits usada anteriormente.
  - Protocolo de autenticação simultânea de iguais: usado para criar um handshake seguro, em que um dispositivo de rede se conecta a um ponto de acesso sem fio, e ambos os dispositivos se comunicam para verificar a autenticação e a conexão. Mesmo se a senha de um usuário for fraca, o WPA3 fornece um handshake mais seguro usando Wi-Fi DPP.
  - Proteção mais forte contra ataque de força bruta: o WPA3 protege contra adivinhações de senha off-line, permitindo ao usuário apenas uma adivinhação, forçando o usuário a interagir com o dispositivo Wi-Fi diretamente, o que significa que ele teria que estar fisicamente presente toda vez que quisesse adivinhar a senha. WPA2 carece de criptografia integrada e privacidade em redes públicas abertas, tornando os ataques de força bruta uma ameaça significativa.
- Os dispositivos WPA3 tornaram-se amplamente disponíveis em 2019 e são compatíveis com os dispositivos que usam o protocolo WPA2.

Segurança – WPS

- WPS é uma sigla para Wi-Fi Protected Setup — em tradução livre, significa Wi-Fi de configuração protegida. Trata-se de um padrão de segurança utilizado por roteadores Wi-Fi para facilitar a conexão de dispositivos, dispensando a utilização de senhas complexas.
- O WPS pode funcionar de duas formas no roteador: via PIN pré-programado e botão físico ou virtual. Ambas opções permitem a conexão rápida na rede Wi-Fi, sem necessidade de digitar senhas complexas.
- Em uma rede Wi-Fi com WPS via PIN, basta encontrar a SSID (nome da rede) no seu smartphone, tablet, smart TV ou outro dispositivo, e digitar a chave numérica existente (geralmente localizada na etiqueta de informações do roteador).
- Após a inserção do PIN, a conexão na rede Wi-Fi será estabelecida entre o roteador e o outro dispositivo. O roteador irá compartilhar automaticamente a senha complexa (WPA), permitindo que o outro dispositivo continue acessando a rede Wi-Fi sem ter que repetir o processo de conexão WPS.
- Em redes Wi-Fi com WPS via botão físico ou virtual, o roteador libera o acesso sem senha à rede no momento em que a tecla WPS é pressionada. Com a função ativada, basta localizar a SSID da rede na lista de conexões Wi-Fi do seu celular, computador ou smart TV para se conectar sem a necessidade de inserir qualquer tipo de código. Assim, a chave WPA (senha) será compartilhada com os dispositivos, permitindo que novas conexões sejam estabelecidas rapidamente, sem a necessidade de repetir o processo de configuração do WPS.
- Não é seguro utilizar o WPS. Apesar de utilizar criptografia WPA, o padrão não garante a segurança da rede Wi-Fi por estar suscetível a ataques de força bruta, isto é, técnicas de tentativa e erro que permitem o roubo de senhas e outras informações sigilosas. Por esse motivo, diversos dispositivos e sistemas removeram suporte para conexões via WPS. O melhor jeito de garantir a segurança da sua rede Wi-Fi é utilizar uma senha complexa.
- Vantagens
  - Configuração simplificada: o WPS pode ser ativado rapidamente via PIN ou botão físico/virtual;
  - Acesso rápido à rede Wi-Fi: o WPS dispensa o uso de senhas complexas, permitindo maior praticidade para conectar múltiplos dispositivos a uma rede sem fio, especialmente aqueles em que a digitação é difícil, como impressoras e smart TVs.
- Desvantagens
  - Riscos de segurança: a tecnologia WPS possui vulnerabilidades de segurança e facilitam a entrada de intrusos na sua rede Wi-Fi;
  - Compatibilidade: o padrão WPS não é adotado por todos os dispositivos compatíveis com Wi-Fi. O WPS nunca esteve disponível no iPhone e foi removido nas versões mais recentes do Android.

PLC – Power Line Communication

- Tecnologia que utiliza uma das redes mais utilizadas em todo o mundo: a rede de energia elétrica. A ideia desta tecnologia não é nova. Ela consiste em transmitir dados e voz em banda larga pela rede de energia eléctrica. Como utiliza uma infra-estrutura já disponível, não necessita de obras numa edificação para ser implantada.
- A PLC trabalha na camada 2 do modelo ISO/OSI, ou seja, na camada de enlace. Sendo assim, pode ser agregada a uma rede TCP/IP (camada 3) já existente, além de poder trabalhar em conjunto com outras tecnologias de camada 2.
- Apesar de não ser tão popular no Brasil, o PLC é uma excelente solução para transmitir internet em um circuito interno. O Powerline é descrito no padrão da indústria IEEE 1901 e é uma tecnologia que fornece conectividade Ethernet sobre a fiação elétrica existente em casa, garantindo a velocidade e a estabilidade de uma conexão com fio, sem a necessidade de cabos adicionais.
- A energia elétrica é transmitida na frequência dos 50 a 60 Hz, enquanto que o sinal do PLC fica entre 1,7 a 30 Mhz. Por isso, os dois sinais podem passar pelo mesmo fio, sem que um interfira no funcionamento do outro. Eles também são independentes, e continuam funcionando mesmo que o outro pare de ser transmitido.
- Pode ser necessário também, a instalação de um amplificador de sinal, e/ou filtros de linha, a fim de minimizar a interferência causada por certos eletrodomésticos como o secador de cabelo, chuveiro e a furadeira. Vale observar que o sinal do PLC não pode passar por filtros de linha, estabilizadores e no-breaks, já que os mesmos bloqueiam sinais de alta frequência.
- Geralmente o PLC é comercializado em um kit com pelo menos dois adaptadores Powerline para serem conectados ao circuito elétrico. Por isso, é muito importante conhecer bem a estrutura da sua rede elétrica antes de utilizar essa tecnologia para que não haja fuga de sinal da sua rede, comprometendo o desempenho do dispositivo.
- O PLC é de fácil instalação e permite que a rede seja expandida de forma rápida. Além disso, os equipamentos são acessíveis e não exigem a instalação de cabos adicionais, é só plugar o equipamento no roteador e na tomada. Outra vantagem dessa tecnologia é que o alcance pode ser muito maior do que os repetidores, equipamentos utilizados para expandir o alcance da rede doméstica.
- A capacidade de um kit PLC pode variar, mas os aparelhos disponíveis no Brasil conseguem atingir entre 300 Mb/s a 500 Mb/s de velocidade pela fiação.
- O PLC oferece uma estabilidade maior na rede quando comparado a um repetidor e é mais indicado para quando se quer levar internet a um cômodo específico da casa. Mas o repetidor pode ter um custo-benefício melhor e, no Brasil, possui mais opções de aparelhos com diferentes tipos de capacidade e velocidade. A escolha vai depender da sua necessidade.

PLC – Power Line Communication