Introdução e Ondas Eletromagnéticas

Uma rede sem fios (redes wireless), como o próprio nome já diz, é uma rede de dispositivos, geralmente computadores e dispositivos móveis, que trocam dados entre si, sem o uso de cabos. A rede sem fios se comunicam através de ondas eletromagnéticas.

Basicamente, uma onda eletromagnética é uma oscilação, em fase, dos campos elétricos e magnéticos que se autopropagam pelo espaço livre, em qualquer ponto desse espaço, independente de ter ar ou não (por isso existem comunicações do tipo no espaço, por exemplo).

As ondas eletromagnéticas podem ser classificadas de formas distintas, as três principais são a amplitude, a frequência e a fase.

A amplitude é a “altura” da onda, ou seja, a medida do valor de pico da energia transmitida (potência), quando maior a amplitude de uma onda, maior será sua energia intrínseca.

A amplitude pode ser medida, por exemplo, em volts.

A frequência de uma onda se refere ao número de ciclos completos que ocorrem a cada segundo. Por exemplo, se uma onda oscila uma vez por segundo, sua frequência é de mil ciclos por segundo.

Na prática, usamos a unidade de medida Hertz (Hz) para representar a frequência de uma onda, sendo que 1 Hz é 1 ciclo por segundo.

Assim como outras medidas, usamos prefixos multiplicadores para representar os valores de frequências, até porque na maioria das vezes os Hertz são valores muitos altos, por isso são utilizados o Kilohertz (1.000 ciclos por segundo), Megahertz (1.000.000 de ciclos por segundo, Gigahertz (1.000.000.000 de ciclos por segundo) e assim por diante.

Um exemplo seria um sinal de telefone sem fio, que opera na frequência de 900 Mhz, que é 900 milhões de ciclos por segundo.

Note a diferença entre duas ondas, sendo a primeira de frequência mais alta do que a segunda, e portanto, de comprimento de onda (tamanho da onda) menor.

Pode ver que na segunda onda, tem mais oscilações (hertz) no mesmo tempo que a primeira, e portanto, a frequência maior.

A fase de uma onda pode ser entendida como a posição relativa da onda em relação a um ponto específico da outra onda, assim, uma onda pode estar em fase com outra onda (ondas idênticas), ou defasada de x graus, como por exemplo ondas defasadas em 180° (ondas totalmente inversas entre si).

A fase é uma característica muito importante em diversas áreas de pesquisa e tecnologia de ondas eletromagnéticas.

Dessas características, a frequência é a que vamos abordar com mais importância.

O espectro eletromagnético consiste em uma classificação das ondas eletromagnéticas pelo seu comprimento de onda, em ordem crescente, mostrando a aplicação das diversas frequências mostradas na forma de uma figura ou gráfico.

Quanto maior a frequência de uma onda eletromagnética, menor será seu comprimento de onda e mais energética ela será, oscilando um número maior de vezes por segundo.

Perceba que a luz visível também é uma forma de onda eletromagnética, assim como as ondas de rádio AM e FM, raios infravermelhos e ultravioletas, raios-X e radiação gama.

No caso, uma onda de rádio (frequência mais baixa) tem cerca de 1000 metros (por exemplo, rádios AM e FM), já uma onda de uma rede sem fio tem cerca de 12 cm (cerca de 2,4 Ghz). Quanto mais encolhemos essa onda, maior a frequência, até chegar ao infravermelho, a luz visível (as cores de tudo são definidas pelas diferenças de frequências da luz) e assim por diante. Não confundir com a amplitude da onda.

E abaixo temos as definições para as siglas apresentadas na tabela anterior, na coluna de classes:

Sigla	Significado	Tradução Livre/Aproximada
γ	Gamma Rays	Raios Gama
HX	Hard X-Rays	Raios-X Hard
SX	Soft X-Rays	Raios-X Soft
EUV	Extreme Ultraviolet	Ultravioleta Extremo
NUV	Near Ultraviolet	Ultravioleta Próximo
NIR	Near Infrared	Infravermelho Próximo
MIR	Mid Infrared	Infravermelho Médio
FIR	Far Infrared	Infravermelho Distante
EHF	Extremely High Frequency	Frequência Extremamente Alta
SHF	Super High Frequency	Frequência Super Alta
UHF	Ultra High Frequency	Frequência Ultra Alta
VHF	Very High Frequency	Frequência Muito Alta
HF	High Frequency	Frequência Alta
MF	Medium Frequecy	Frequência Média
LF	Low Frequency	Frequência Baixa
VLF	Very Low Frequency	Frequência Muito Baixa
ULF	Ultra Low Frequency	Frequência Ultra Baixa
SLF	Super Low Frequency	Frequência Super Baixa
ELF	Extremely Low Frequency	Frequência Extremamente Baixa

Pode ver que muitas dessas siglas são familiares, como a VHF e UHF, usadas em transmissão de TV.

Arquitetura de Redes Wi-Fi

A arquitetura de uma rede se refere ao modo como os dispositivos são interligados e ao tipo de equipamentos necessários para implementar tal rede.

No caso de redes locais wi-fi (WLAN) há três tipos de arquiteturas básicas: IBSS, BSS e ESS.

Todos os dispositivos que se conectam a uma rede sem fio são denominados estações (podem ser computadores, celulares, tablets), que podem ser access points ou clientes de rede, e se comunicam com a rede por meio de uma interface de rede wireless.

A IBSS (Independent Basic Service Set) são dispositivos que se comunicam entre si (apenas clientes, incluindo PCs, notebookes, tablets, smartphones e outros dispositivos). Para isso necessitam apenas de uma interface de rede wireless e antenas apropriadas. As WLANs IBSS também são denominadas redes Ad-Hoc.

A BSS (Basic Service Set) é onde os dispositivos clientes (computadores, impressoras, tablets) são interconectados através do uso de um dispositivo central denominado access point (AP), que age como uma espécie de switch wireless. Toda rede BSS possui um nome que a identifica, conhecido pela sigla SSID (Service Set Identifier).

A ESS (Extended Service Set) é o conjunto de BSS interconectadas com o intuito de aumentar o alcance e a capacidade da rede wi-fi, podendo consistir em até dezenas de access points e conter milhares de hosts conectados. Access points em uma ESS são conectados por meio de um serviço de distribuição (DS ou Distribuition System), que pode ser cabeado ou wireless.

Pode ver que tem um pedacinho de uma BSS que sobrepõe a outra.

O que é o SSID

O service identifier (identificador do conjunto de serviço) é o nome de identificação associado a uma rede local sem fio, no padrão 802.11 de redes wireless (Wi-Fi).

É utilizado pelos clientes para identificar e se conectar a rede, e diferencia uma rede wireless de outra na mesma localidade física.

Pode ser um ESSID ou BSSID, dependendo da arquitetura da rede local wireless, no geral, chamamos apenas de SSID, cada AP e cliente de rede em uma rede usam o mesmo SSID.

O SSID de uma rede sem fio fica armazenado em um Access Point. O nome da rede pode ser enviado em broadcast (“anunciado”) para ajudar as estações a encontrá-la e se conectarem.

É possível configurar o AP/roteador para não realizar esse broadcast, e inclusive ocultar o nome da rede.

O SSID é uma string de texto e números com no máximo 32 caracteres, case-sensitive. Roteadores banda-larga possuem um nome padrão para a rede sem fio, que pode (e deve) ser alterado durante sua configuração, por razões de segurança.

Para se conectar a uma rede sem fio, os PCs, smartphones, tablets, etc. varrem as redes sem fio locais em busca de dispositivos que estejam anunciando seus SSIDs, e então mostram ao usuário uma lista de nomes disponíveis. Então, o usuário pode selecionar a rede à qual quer se conectar, escolhendo um dos SSIDs da lista.

A conexão pode ou não usar opções de segurança, como uma senha, que deverá ser fornecida caso requisitada para que seja possível conectar à rede escolhida. Na maioria dos caso a opção de segurança é habilitada.

É possível salvar as redes sem fio em seu dispositivo cliente, de modo a realizar a conexão automática do dispositivo sempre que estiver na área de alcance da rede identificada.

O Que são Wireless, WLAN, Wi-Fi, WiMAX e WMAN

Provavelmente você já ouviu algumas dessas frases: “Vou montar uma rede wireless em meu escritório”, “você tem a senha do Wi-Fi”, “aqui tempos acesso à internet via WiMAX”, “preciso comprar um roteador wireless mais potente”, “entro na WLAN, conecto à WMAN e acesso à internet”. Isso são todos termos técnicos do mundo das redes em fios, alguns tem suas semelhanças.

Basicamente, essas são as peculiaridades deles:

- **Wireless:** É uma palavra inglesa que significa “sem fio”. Termo genérico utilizado para redes de dados que não usam cabos para comunicação entre os dispositivos, empregando em vez disso, ondas eletromagnéticas.
- **WLAN:** É o mesmo que “LAN sem fio”. Uma rede WLAN se refere a uma rede local (LAN) em uma residência, escritório ou outros locais onde seja necessária uma rede com pequena área de cobertura sem o emprego de cabeamento para conectar as estações. Quando pedimos a senha de um Wi-Fi, estamos pedindo a senha do WLAN.
- **Wi-Fi:** Significa “wireless fidelity”. Se trata de um tipo de rede wireless WLAN para a construção de LANs para comunicação de computadores e dispositivos portáteis, como tablets, notebooks e smartphones, entre outros, a redes como a internet ou outras redes locais, cabeadas ou não. É uma rede de transmissão de alta qualidade (é uma analogia aos sons Hi-Fi).
- **WiMAX:** Significa “worldwide interoperability for microwave access” (interoperabilidade mundial para acesso de micro-ondas). É um padrão criado por um consórcio de empresas que especifica uma interface para redes de banda larga sem fio em um escopo metropolitano (WMAN). O padrão é 802.16.

Alguns tipos de redes wireless são o Bluetooth, Wi-Fi, rádio (AM/FN0, satélite (como GPS), ZigBee, LTE, Li-Fi, UMTS e WiMAX.

Atualmente, a rede WLAN padrão é a rede baseada nos padrões IEEE 802.11, também chamada de Wi-Fi. Outros tipos já existiram, como a HiperLAN.

Wi-Fi é marca registrada da Wi-Fi Alliance, que restringe o uso da expressão Wi-Fi Certified a produtos que passaram em teste de cerficicação de interoperabilidade. As redes Wi-Fi são padronizadas como IEEE 802.11, com várias revisões (a, b, g, n, etc.), cada uma com características tecnológicas específicas.

Uma diferença entre o padrão WiMAX e o Wi-Fi é o raio de alcance de cada rede. O WiMAX foi projetado para uso em redes de área metropolitana sem fio (WMAN), cobrindo em torno de 50 Km de área com sinal. Wi-Fi é usado em ambientes privados em áreas restritas, tem alcance máximo de poucas centenas de metros.

As aplicações do WiMAX são: Fornecer conectividade móvel de banda larga em e entre cidades, alternativa sem fios aos serviços de cabo e DSL para acesso à banda larga de última milha, fornecer serviços de VoIP e IPTV em conjunto com dados (Triple Play), entre outros.

Analisando seu Ambiente Wi-Fi

Temos várias ferramentas para analisarmos o ambiente Wi-Fi ao redor.

No Android temos para isso o aplicativo Wi-FI Analyzer Classic, que permite nós visualizarmos quais redes Wi-Fi estão próximas, qual está com a onda mais alta, quais canais elas estão e se alguma rede está sobrepondo outra (o que causa interferência na transmissão de dados).

No Windows, em computadores com placa de rede Wi-Fi, podemos usar o Xirrus para analisar a rede Wi-Fi.

Caso esteja utilizando o Linux, instale o LinSSID.

Quanto mais alta a onda da rede Wi-Fi, mais forte ela está, e ela não deve estar no mesmo nível de outra, no mesmo canal, pois dá interferência em ambas.

Alguns roteadores costumam mudar de canal para conseguir uma transmissão melhor e sem interferências. Nessa situação ele desconecta todos os dispositivos e os reconecta ao achar um canal livre.

Os padrões Wi-Fi são esses:

Nome do Padrão	Velocidade da Rede
802.11.A	54 Mbps
802.11.B	11 Mbps
802.11.G	54 Mbps
802.11.N	600 Mbps
802.11.AC	3,6 Gbps
802.11.AX	10 Gbps

Sempre escolha no roteador, o melhor padrão para Wi-Fi, mas o dispositivo também deverá ser compatível com o mesmo padrão, o que pode ter problemas com alguns dispositivos, principalmente os mais antigos, por isso que o padrão em muitos roteadores é o Mixed, mas ele diminui o desempenho.

Sobre o canal de comunicação, aqui no Brasil tem 13, mas geralmente o melhor é usar o 1, 6 ou 11.

Protegendo seu Wi-Fi

No seu navegador, acesse o IP do seu roteador (indo em ipconfig, no caso do Windows, e pegando o endereço do gateway padrão), como por exemplo *192.168.15.1*.

Na tela de login, acesse usando o login e senha padrões (que é recomendado serem mudados posteriormente). É recomendado também mudar os nomes e senha da rede Wi-Fi.

Toda rede Wi-Fi possui um protocolo de segurança, que define sua senha e a criptografa. Prefira os protocolos WPA3 ou WPA2, evite o protocolo WEP, que é mais vulnerável.

Apesar da função WPS ser útil para conectar um dispositivo a rede Wi-FI, ele também tem vulnerabilidades, pois facilita o acesso a invasores na rede, e por isso é recomendado desativá-lo.

Já a opção SSID define se mostrará ou não a Wi-Fi para as pessoas, caso ela não seja mostrada teremos que configurar manualmente no dispositivo (mas isso pode ser burlado por um hacker).

Temos também um filtro de MAC na configuração do Wi-Fi, onde podemos bloquear ou permitir determinados endereços físicos.

Procure também atualizações para o firmware do seu roteador.

Para que alguns programas funcionem corretamente, é necessário deixar algumas portas abertas no roteador, no entanto, quando elas não estão em uso, é recomendado fechá-las para não serem exploradas por invasores.

O Que é o Mecanismo RTS/CTS

O problema do nó oculto ocorre quando estações em uma BSS estão distantes entre si, e não se enxergam, apesar de enxergarem o AP. Pode ocasionar a tentativa de transmissão simultânea de pacotes, levando a colisões. Impacta negativamente a performance da rede sem fio. Pode ser resolvido com o emprego do mecanismo RTS/CTS.

Sobre o mecanismo RTS/CTS:

- Processo simples que controla o acesso das estações ao meio de transmissão.
- Uma estação anuncia que deseja transmitir dados, e todos na rede são avisados de que devem esperar essa transmissão recorrer, e a estação realiza então usa transmissão de quadros.
- Por padrão, é desabilitado nos equipamentos para evitar overload.

Operação do RTS/CTS:

- Uma estação com o RTS/CTS habilitado deseja transmitir dados para algum outro host na rede.
- Essa estação envia um quadro RTS ao access point (ou a outra estação diretamente).
- Esse quadro RTS é usado para a distribuição de NAV, notificando todas as outras estações que elas devem esperar até que quadros CTS, de dados e ACK tenham sido transmitidos.
- O AP então envia um quadro CTS, também usado para distribuição de NAV. Se alguma estação não tiver escutado o quadro RTS, escutará o quadro CTS, pois todas as estações são membros do mesmo BSS (Basic Service Set).
- As estações que recebem os quadros RTS ou CTS ajustam seu NAV para o valor fornecido.
- Os dados da estação transmissora são enviados até a transmissão receptora.
- AP envia quadro ACK para confirmar fim da transmissão e liberar as transmissões novas.

O quadro RTS (20 bytes) contém cinco campos, que são:

- **Controle de Quadro:** Tipo do quadro, entre outras coisas. 1011 para RTS.
- **Duração:** Tempo estimado para a transmissão do quadro de dados, inclui tempo para os quadros CTS, ACK e SIFS.
- **RA (Receiver Address):** Endereço MAC do AP (BSSID).
- **TA (Transmitter Address):** Endereço MAC do AP (BSSID).
- **FCS:** Control de erros.

Já um quadro CTS (14 bytes) possui quatro campos:

- **Controle de Quadro:** Tipo do quadro, entre outras coisas. 1100 para CTS.
- **Duração:** Tempo do RTS, menos SIFS e tempo de transmissão do quadro CTS.
- **RA (Receiver Address):** TA do quadro RTS se torna o RA aqui.
- **FCS:** Controle de erros.

Existem, basicamente, três modos possíveis de configuração do mecanismo RTS/CTS:

- Desligado (é o padrão).
- Ligado.
- Ligado, com o RTS Threshold (limite).

Threshold: É possível controlar quais pacotes, acima de um certo tamanho determinado por um limite (threshold), são anunciados pelo mecanismo para envio pelas estações.

Esses são os problemas do nó exposto:

- Problema no qual uma estação wireless nas proximidades, porém conectada a um outro access point, escuta a transmissão de quadros RTS e CTS e para de transmitir quadros pelo tempo especificado no RTS (mesmo não fazendo parte da rede em questão).
- Pode ocorrer quando ambas as redes em questão estão usando o mesmo canal de transmissão wireless, causando assim o que chamamos de interferência co-canal (ou interferência de canal).

E tem essas dicas:

- Se uma rede sem fio tem uma performance muito baixa por excesso de usuários conectados, interferência eletromagnética ou colisões de pacotes, diminua o limite RTS até conseguir uma melhora na performance da rede.
- Monitore a rede para verificar se ocorrem colisões. Caso haja muitas colisões, e se os usuários estiverem fisicamente distantes, ative o mecanismo RTS/CTS.
- Se a rede estiver com baixa performance por outro motivo que não o dos nós ocultos, ativar o mecanismo RTS/CTS pode diminuir ainda mais sua performance, pois está sendo adicionada mais uma etapa para a transmissão de dados na LAN.
- Valor recomendado para o RTS Threshold: Cerca de 500. Valores mais baixos significam pacotes RTS transmitidos com mais frequência, útil para melhorar a performance caso ocorram muitas colisões, sobrecarga de tráfego ou interferência eletromagnética.
- Sempre ajuste o RTS em pequenos valores, e teste para ver se obteve o efeito desejado.

O que é WPA e WPA2

Ao configurar uma rede Wi-Fi, é importante escolher uma boa chave de criptografia para garantir a segurança dos dados. O WPA e WPA2 são os protocolos mais usados para evitar o acesso de cibercriminosos, que podem coletar informações para atividades ilegais ou instalar malwares.

Lançado em 2003, o WPA resolver diversas vulnerabilidades do seu antecessor, o WEP. Esse protocolo é mais seguro porque usa uma chave de 256 bits para criptografia, representando uma grande melhoria com relação às chaves de 64 e 128 bits do padrão anterior.

Outra característica do WPA é o Temporal Key Integrity Protocol (TKIP), responsável por gerar dinamicamente uma nova chave para cara pacote ou unidade de dados, sendo mais seguro que o sistema de chave fixa do WEP. No entanto, esse padrão ainda entrega um baixo nível de segurança.

A Wi-Fi Alliance, organização que estabelece os protocolos de Wi-Fi, precisou manter alguns elementos do WEP para que dispositivos antigos fossem compatíveis. Por conta disso, o WPA tem brechas que podem ser exploradas com certa facilidade.

Para resolver os problemas, a organização apresentou o protocolo WPA2 em 2004. O novo padrão é mais fácil de configurar e entrega um sistema de segurança mais complexo. A grande diferença está no Advanced Encryption Standard (AES), que substituiu o TKIP.

Essa tecnologia melhorou o nível de segurança ou ponto de ser usada para proteger informações governamentais. Ou seja, o WPA2 fornece uma criptografia forte. No entanto, ele tem uma vulnerabilidade crítica: Se uma pessoa não autorizada conseguir acessar à rede, ela pode atacar outros dispositivos conectados.

O WPA3 foi lançado em 2018 para corrigir as vulnerabilidades das versões anteriores. Ele traz um sistema de criptografia chamado Perfect Forward Secrecy e uma série de melhorias, como novos recursos para simplificar a segurança, autenticação mais robusta e maior força criptográfica.

No entanto, esse padrão ainda não foi amplamente adotado. Há roteadores com WPA3 no mercado, mas eles costumam ser mais caros. Além disso, apesar das fabricantes disponibilizarem a atualização que entrega o novo protocolo, nem todos os modelos vendidos oficialmente têm um hardware capaz de suportá-lo. Em outras palavras, o WPA3 não é uma opção para a maioria das pessoas, pelo menos por enquanto.