FACULDADE DE TECNOLOGIA SENAC GOIÁS

Arthur Oliveira, Isadora Serrano

João Moita e Matheus dos Santos Ferreira

PROJETO DE REDES DE COMPUTADORES

PADRÃO IEEE 802.11 - Wireless

Goiânia

2018

SUMÁRIO

Introdução

Com a crescente evolução de equipamentos eletrônicos de rede móveis: telefone sem fio, laptops, notebooks, smartphones, etc. surge a necessidade do desenvolvimento de uma rede independente de cabeamento, de forma que os dispositivos não fiquem presos a um lugar com cabeamento de rede.

Um bom exemplo da necessidade da implementação de uma rede sem fio, é a necessidade de múltiplos usuários que utilizam dispositivos moveis se conectarem a uma rede que possui um número limitado de pontos de rede, geraria uma situação onde poucos poderiam se conectar a rede, uma rede sem fio possibilitaria a conexão de todos esses componentes. O protocolo de acesso ao meio utilizado pela rede sem fio utilizado na rede sem fio, é o CDMA – *Code Division Multiple Acess* (Acesso Múltiplo por Divisão de Código), está presente na camada de enlace, **Camada 2 do modelo OSI.** A rede sem fio(Wi-Fi), é regulada pelo padrão IEEE 802.11.

A seguinte imagem mostra os principais componentes de uma rede sem fio:

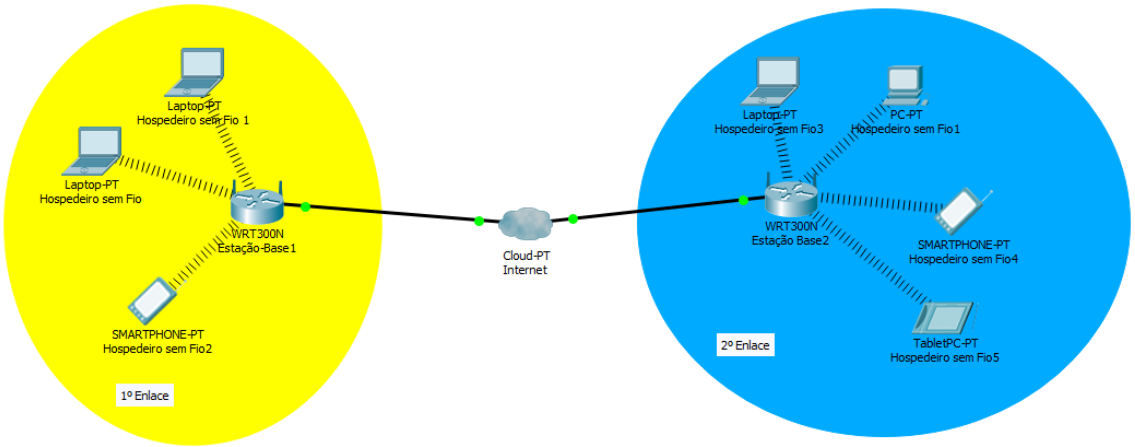

Figura 1: Estrutura Rede sem Fio

Hospedeiro sem fio: Os hospedeiros são os hosts (computadores, impressoras, telefones, etc) que possuem interface de conexão sem fio e são capazes de executar aplicações, Os hospedeiros sem fio podem ser moveis ou não.

Enlaces sem fio: Um hospedeiro sem fio necessita de uma estação-base para se conectar, um exemplo de uma estação-base seria o modem. Modens, ou ponto de acesso sem fio, são muito utilizados hoje em dia para conectar vários dispositivos simultaneamente a rede, esses também podem utilizados para conectar roteadores, comutadores e outros equipamentos de rede, esses equipamentos são conectados à rede por meio de um enlace sem fio. Enlaces sem fio pode possuir taxas de transmissão diferentes, assim como a distância da transmissão pode variar. Os equipamentos modem podem variar sua taxa de transmissão de 56 Kbps (Kbits por segundo), até 54 Mbps. Alguns exemplos desse padrão:

- 56 Kbps = IS-95, CDMA, GSM. Transmissão 2G;
- 384 Kbps = UMTS/WCDMA, CDMA 2000. Transmissão 3G;
- 1 Mbps = 802.15

- 5 – 11 = 802.11b
- 802.11{a,g}

Estação-base: A estação-base é o principal componente de uma rede sem fio, utilizada para transmissão e recebimento de dados entre hospedeiro sem fio que estão associados a ela através de um enlace. Uma estação-base pode ser um modem, ou até um hospedeiro sem fio, que está retransmitindo o sinal que recebe. Esse equipamento pode coordenar, monitorar e bloquear a transmissão dos dados na rede. Um exemplo de uma estação-base são torres de celulares, pontos de acesso, entre outros. Uma estação-base é utilizada para conectar hospedeiros de rede com a rede mundial de computadores, internet, ou seja, funciona como uma retransmissora de camada de enlace.

Quando um dispositivo está conectado em uma enlace de rede é fornecido a esse vários serviços como, atribuição de endereço IP, roteamento, e conexão à rede, entre outros, esse serviço passa a operar em modo de infraestrutura. Quando um dispositivo não opera nesse modo, ele deve prover seus próprios serviços de atribuição de endereço, tradução de endereços DNS, um exemplo desse tipo de serviço é o 3G e 4G, serviço de rede disponibilizado por muitas operadoras a smartphones.

Quando um dispositivo muda de estação, ou seja, se movimenta para outro local com um rede diferente, dá se um processo de transferência (*handoff*), onde este recebe um novo endereçamento e se adapta as configurações dessa rede.

Infraestrutura de rede: É a rede maior com que o dispositivo pode se conectar. A infraestrutura sem fio pode ser classificada em dois critérios, primeiro, se um pacote na rede sem fio atravessa somente um enlace, salto único ou múltiplos saltos sem fio, e se há infraestrutura na rede, como uma estação base.

Salto único com Infraestrutura: A estação base está conectada à rede cabeada, e é necessário somente um único salto sem fio, um exemplo dessa rede é a que utilizamos em casa, lanchonetes, centros de ensino, etc.

Salto único sem Infraestrutura: Nessa rede não existe uma estação base, a conexão pode estar sendo retransmitida a partir de um hospedeiro conectado a um salto único com infraestrutura, um exemplo dessa rede é o sistema *bluetooth*.

Múltiplos saltos com infraestrutura: As redes de malha sem fio podem se encaixar nessa categoria, por estabelecer conexão a vários dispositivos, a partir de um conectado a uma estação-base de rede.

Múltiplos saltos sem infraestrutura: Assim como no salto único, não existe um estação base, os nós tem de reestabelecer mensagens entre diversos outros nós para chegar a um destino.

Características de enlaces e redes sem fio

Uma das principais, e mais notáveis, características de um rede sem fio é que esta pode substituir praticamente todos os pontos de redes necessários para conectar os dispositivos via cabo, sendo que necessitaria de apenas um ponto para conectar um *Access Point*, substituindo o comutador Ethernet. Na camada de rede as mudanças quase não seriam notadas, dependendo do

número de dispositivos conectados. Isso se torna uma grande vantagem quanto ao custo gasto com manutenção e equipamentos. Porem um dos principais fatores seria na camada de enlace, onde o sinal sofreria variações quando se encontra com alguma barreira física, o que dissipa o sinal, e também a questão de quanto maior a distância mais fraco o sinal, sinais de interferência provocados por ondas de rádio que emitem sinal na mesma frequência que a rede, fontes que emitem ruídos eletromagnéticos (raios, trovões, máquinas, etc) e propagações de objeto físicos que interferem na emissão do sinal.

Como erros de bits, envio de sinal, são mais comuns em enlaces sem fio do que em enlaces com fio, esse possui vários protocolos baseados em códigos de detecção de erros que retransmite o sinal diversas vezes, um exemplo é protocolo CRC (*Cyclic Redundancy Check* – Verificação Cíclica de Redundância) e o ARQ (*Automatic Repeat Request* – Repetidor de Sinal Automático), além dos códigos de detecção de erro também são incrementados protocolos de transferência de dados confiável em nível de enlace.

Quando um sinal de rede sem fio é transmitido via o dispositivo recebe um sinal eletromagnético de forma variada, com relação ao sinal original transmitido, isso acontece devido a atenuação e interferência do sinal, conhecido como **relação sinal-ruído** (SNR – signal-to-noise ratio) está se trata de uma medida relativa da potência do sinal recebido e o ruído, costuma ser calcula em dB (Decibéis), essa medida é vinte vezes a razão do logaritmo de base 10 da amplitude do sinal recebido à amplitude do ruído.

A probabilidade de um bit transmitido ser recebido com erro no destinatário vai de encontro a três de modulação diferentes para codificar informações para a transmissão em um canal sem fio idealizado. Há diversas características da camada física que são importantes para entender os protocolos de comunicação sem fio da camada superior.

Para um dos esquemas de modulação, quanto mais alta for o sinal-ruído mais baixo será a taxa de erro de bit. O remetente pode ter esse controle aumentando a potência de transmissão o que faz com que o SNR diminua, isso fornece uma certa vantagem no recebimento de pacotes, no entanto há um gasto maior de energia além da probabilidade de interferência em outras transmissões.

Algumas SNR algumas técnicas de modulação com uma taxa de transmissão de bit maior poderão ter mais erros de bit de rádio.

A seleção dinâmica da técnica de modulação da camada física pode ser usada para adaptar a técnica de modulação para condições de canal, com isso a SNR pode sofrer variações. A modulação adaptativa e a codificação são usadas em sistemas de dados Wi-Fi 802.11 e celular 3G. Quando uma técnica de modulação é selecionada, esta pode oferecer alta taxa de transmissão sujeita a limitação na BER.

As taxas de erros de bits SNR, não são as únicas diferenças entre uma rede cabeada e uma rede sem fio. Nas redes cabeadas cada ponto na rede recebe a taxa de transmissão do outro, Em redes sem fio qualquer objeto físico se torna uma barreira, desde um pequeno, como um bloco ou maiores, o fato é quanto maior a barreira maior a oscilação. Outro fator importante é a intensidade do sinal, sendo que quando é forte entre duas estações e para outra é fraca o sinal pode sofrer oscilações para esta.

CDMA

Sempre que hosts se comunicam em uma rede é necessário um protocolo para impedir que sinais enviados por estes não interfiram uns nos outros esse protocolo pode ser criado a partir de um canal, acesso aleatório ou revezamento, O protocolo utilizado no caso das redes sem fio, é o acesso múltiplo por divisão de código (code division multiple access - CDMA), este se dá através de um canal.

O protocolo CDMA tem como função codificar, por multiplicação do bit, cada pacote que é enviado na rede e decodifica-lo quando chega ao remetente, esse processo vai acelerando com o tempo, o que é conhecido como taxa de chipping.

Há uma formula para se obter a saída do codificador CDMA, está é obtida através de uma unidade de tempo representada por um intervalo de um bit, sendo d o valor do bit para o i-ésimo intervalo de bit (di) o bit deve ser representado pelo valor 0 e -1, cada intervalo de bit é subdividido em M mini intervalos, uma sequência de valores é representado pro (Cm). sendo assim a saída do codificador é dado pelo i-ésimo de dados para o m-ésimo mini intervalo do tempo de transmissão de bits de (Di) multiplicado pelo m-ésimo bit do código.

1º Equação:

$$Z_{i,m} = d_i \cdot c_m$$

Caso o remetente esteja recebendo os bits codificados(Zi,m), recuperando os bits de dados originais (Di), a formula é a seguinte:

2º Equação:

$$d_i = \frac{1}{M} \sum_{m=1}^{M} Z_{i,m} \cdot c_m$$

Quando um remetente esta enviando dados utilizando um código diferente, os bits são embaralhados, a função do CDMA é exatamente codificar os bits originais de forma que estes sejam reconhecidos, decodificados e enviados ao destinatário correto.

Se tratando de vários remetentes a formula para calcular as transmissões codificadas, é semelhante a 1º equação, acrescentando a soma dos bits transmitidos de todos os N remetentes durante o mini intervalo:

3º Equação:

$$Z^{*}_{i,m} = \sum_{s=1}^{N} Z^{s}_{i,m}$$

Os códigos de bits podem ser selecionados pelo usuário, dependendo da sequência escolhida, o receptor pode recuperar os dados enviados por um dado remetente a partir do sinal agregado, a seguinte formula pode ser utilizada para a recuperação:

4º Equação:

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z^{*}_{i,m} \cdot c_m$$

A imagem abaixo demonstra como funciona o processo de codificação do CDMA remetente/receptor, com um remetente simples.

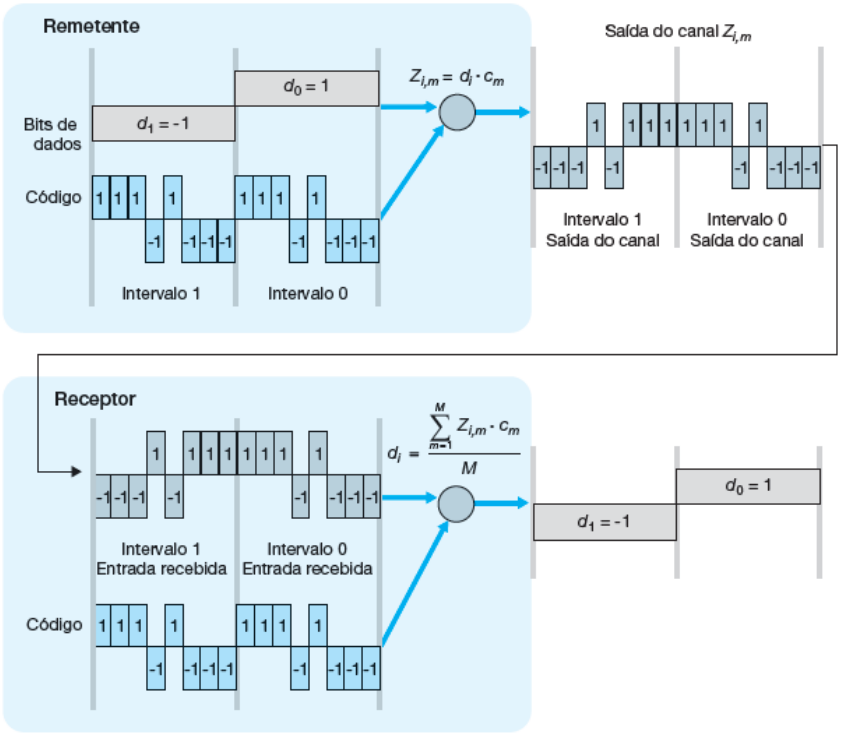

Figura 2: Estrutura CDMA

Como descrito acima esse processo pode ocorrer com mais de um remetente, a imagem abaixo ilustra esse processo, assim como detalha a sequência de bits utilizada por cada um, nota-se que o receptor consegue extrair o código original do 1º remetente mesmo com a interferência de um segundo:

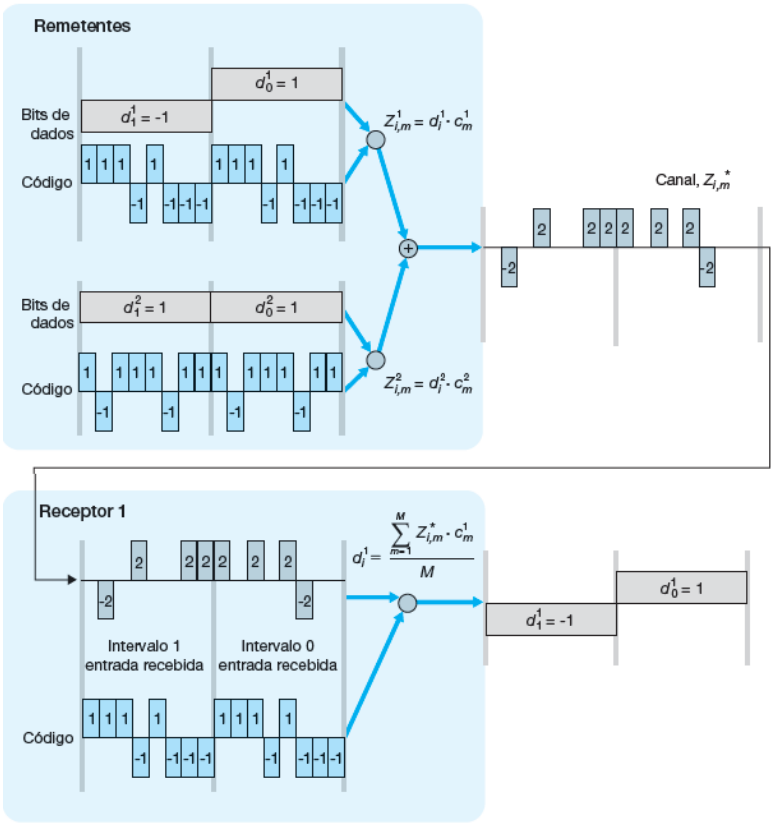

Figura 3: Estrutura CDMA com dois Remetentes

Resumindo o protocolo CDMA é responsável por codificar e decodificar os pacotes que são transmitidos na rede, tendo o cuidado de selecionar cada código, e como a intensidade dos sinais recebidos é a mesma, quando se tem vários transmissores o processo se torna mais difícil, esse é um dos vários fatores de quando mais hosts conectados em transmissão sem fio, mais lento o sinal fica.

Wi-Fi: LANs sem fio 802.11

A rede sem fio uma das mais utilizadas hoje em dia começou a ser desenvolvida na década de 90, tiveram muitas tentativas sem sucesso, no entanto o padrão que se destacou e conseguiu êxito foi o 802.11 também conhecido como Wi-Fi. Foram desenvolvidas vários padrões desse protocolo entre eles o 802.11b, 802.11a e 802.11g, também foram desenvolvidas variações entre esses padrões, de forma dupla: 802.11a/g e tripla 802.11a/b/g.

Esses três protocolos trabalham na camada de enlace e possuem várias características semelhantes e utilizam o mesmo protocolo de acesso ao meio: CSMA/CA. Esses padrões também podem reduzir sua taxa de transmissão para alcançar maiores distâncias e seus padrões permitem dois modos: infraestrutura e ad hoc, apesar dessas semelhanças esses protocolos possuem diferenças na camada física, a tabela seguinte demonstra as principais características desses padrões:

Padrão	Faixa de Frequências (EUA)	Taxa de dados
802.11b	2,4 – 2,485 GHz	Até 11 Mbits/s
802.11a	5,1 – 5,8 GHz	Até 54 Mbits/s
802.11g	2,4 – 2,485 GHz	Até 54 Mbits/s

O padrão 802.11b opera em uma frequência de 2,4 à 2,485 GHz, está que é semelhante a frequências de fogão elétrico, telefones e fornos micro-ondas, clientes que utilizam esse padrão costumam ter muita interferência em telefones ou na qualidade da internet. No padrão 802.11a a rede consegue trabalhar com uma taxa de bits mais alta e com uma frequência mais alta, por esse motivo o padrão opera a uma distância mais curta em determinados níveis de potência sofrendo com propagação multivias. As LANs 802.11g opera na mesma taxa de frequência que o 802.11b o que a torna compatível com esse padrão, o que o torna melhor é a sua taxa de bits ser maior que do padrão b.

Um novo padrão desenvolvido em 2012, 802.11n, se utiliza de múltiplas antenas para aumentar a taxa de transmissão para centenas de megabits por segundo. Essas múltiplas antenas podem ser instaladas tanto do lado do remetente quanto do destinatário que transmitem ou recebem dados em taxas de transmissão diferentes essa novo padrão é conhecido como MIMO – *Multiples In Multiples Out.*

A Arquitetura 802.11

A arquitetura 802.11 é composta por vários componentes, o principal deles é o conjunto básico de serviço (*basic service set* - **BSS**)**,** cada BSS pode conter uma ou mais estações sem fio e uma estação-base central conhecida como ponto de acesso (*Access Point* - ***AP***). A imagem seguinte mostra um AP interligando dois BSSs, conectado a um dispositivo de interconexão que fazem a distribuição da internet.

<IMAGEM arquitetura de lan IEEE 802.11>

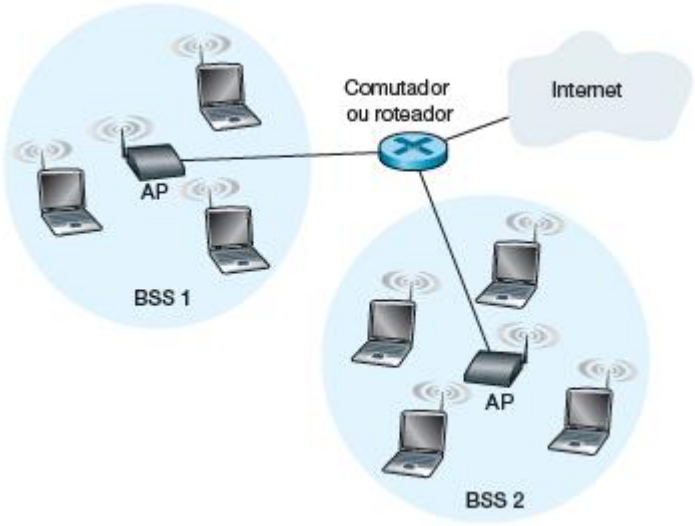

Figura 4: Estrutura com múltiplos BSS

Assim como os computadores e dispositivos Ethernet, as estações sem fio também possuem um endereço MAC, este é fica armazenado no *firmware* do adaptador da estação, é composto 6 bytes, os *access point* também possuem endereço MAC, ambos os dois dispositivos são administrados pelo IEEE, sendo exclusivos.

Como descrito anteriormente quando uma LAN sem fio disponibiliza de um AP, essa é denominada LAN sem fio de infraestrutura, ou seja, os access point na infraestrutura de ethernet conecta os APs e um roteador. A imagem seguinte demonstra que o padrão 802.11 pode formar uma rede sem nenhum controle central – ad hoc, esse exemplo acontece quando temos a necessidade de conecta dispositivos móveis que não possuem uma infraestrutura de rede, essas redes podem ser criadas quando se tem dois dispositivos em um mesmo ambiente que podem se comunicar via rede, sem a necessidade de um meio centralizado.

<Rede AD hock>

Figura 5: Estação de Rede sem fio

Canais e Associação

No padrão 802.11, um access point é necessário para a conexão com a rede sem fio, quando este é instalado o administrador define um Identificador de conjunto de serviços (*Service Set Identifier* - SSID) composto de poucos caracteres. Também é configurado um número de canal para o AP, esse canal é definido dentro da faixa de frequência em que o padrão opera, por exemplo como o 802.11b trabalha em uma faixa de 2,4GHz a 2,485GHz, para este pode ser definido uma faixa de 11 canais, que podem se sobrepor em parte, somente não vai haver sobreposição para padrões que operam somente com 4 canais. O canais 1, 6 e 11 podem ser os mais confiáveis, isto é, que não possuem sobreposição.

Quando um usuário necessita se conectar a um access point, e porventura encontra um ambiente com vários, sendo estes de subredes com IP diferentes, ele poderá se associar a somente um desses, transmitindo e recebendo dados, que poderá estabelecer uma conexão formando uma espécie de vinculo único entre o AP e a estação sem fio do usuário, sem sofrer interferência das outras.

Para que um AP seja localizado é necessário que este envie a todo instantes quadros de localização, sinal, onde é incluído seu SSID e o endereço MAC do AP. A estação sem fio fara o reconhecimento da localização do AP através de seus canais, ao encontrar um desses o hospedeiro sem fio faz a escolha da rede e se associa.

O padrão 802.11 é selecionado pelo projetista do firmware e do software e logo após é implantado no AP ou em um hospedeiro de rede, geralmente quanto maior o sinal transmitido pelo AP, maior é a probabilidade deste ser escolhido. No entanto se um AP com intensidade de sinal forte é escolhido por múltiplos hospedeiros sem fio, esse fica sobrecarregado e a sua potência pode perder força para um AP com menor intensidade de sinal.

Esse processo de procurar por canais ouvindo quadro de sinalizações é chamado de **varredura passiva**, no entanto quando um hospedeiro transmite um quadro de investigação que pode ser recebido por todos os APs dentro de uma faixa do hospedeiro sem fio, esse está fazendo uma **varredura ativa**, em resposta a essa varredura os APs poderão responder através de um quadro de resposta e o hospedeiro poderá selecionar um desses APs para se associar. Após essa associação o hospedeiro manda uma mensagem de descoberta DHCP á subrede por meio de um AP, e em resposta, o endereço é obtido e a conexão é estabelecida e o hospedeiro identificado na rede.

Para que o hospedeiro se conecte a um determinado AP pode ser solicitado uma autenticação, o que acontece na maioria dos casos, comprovando que este tem privilégios para acessar aquela rede. Essa autenticação pode ser obtida através de várias formas:

- Endereço MAC de um hospedeiro especifico;
- Usuário e Senha;
- Etc.

Em todos os casos o AP se comunica com um servidor de autenticação usando um protocolo, como por exemplo o RADIUS ou o DIAMETER. Um servidor de autenticação de AP pode atender a diversos, onde é centralizado as decisões de autenticação e acesso em um único servidor mantendo o baixo custo e complexidade do AP.

O Protocolo MAC 802.11

Quando um hospedeiro se conecta a um AP, este começa a enviar quadro de dados, recebendo e transmitindo informações, porem quanto mais hospedeiros associados a uma estação de rede pelo mesmo canal maior será o trafego, nesse meio surge a necessidade de se estabelecer um protocolo para a administração desses múltiplos acessos. Existem três classes de protocolos desenvolvidas para esse fim, a partição de canal, acesso aleatório e revezamento. Foi escolhido um protocolo de acesso aleatório para as LANs sem fio 802.11, esse protocolo é denominado CSMA com prevenção de colisão, que quer dizer: acesso múltiplo por detecção de portadora, ou seja, cada estação sonda o canal, verificando se este está ocupado ou não, antes de iniciar uma transmissão, esse recurso é bom, porem já é utilizado por outro padrões, um dos diferenciais do protocolo MAC, é que ao invés de utilizar detecção de colisão, ele utiliza técnicas de prevenção de colisão. Outro ponto e que utiliza um esquema de reconhecimento / retransmissão (ARQ) de camada de enlace.

Como o protocolo 802.11 possui um algoritmo de detecção de colisão, quando estiver transmitindo e detectar que existe outra estação também transmitindo, esse aborta e tenta novamente após um período de tempo. O protocolo MAC 802.11 não implementa detecção de colisão por dois motivos: o sinal de resposta é muito fraco, e o custo para implantar um hardware

adicional é muito alto e mesmo que fosse implantado a garantia de que detecção de colisão não é confiável.

Assim que uma estação começa a transmitir quadros de dados não há volta, ou seja, se houver uma colisão o trafego pode sofrer degradações no protocolo de acesso múltiplos, por exemplo quando estamos em uma rede sem fio e um site demora para carregar ou muitas vezes não completa a carga. Para evitar essas colisões o protocolo implementa algumas técnicas de prevenção de colisão, com o objetivo de evitar esse tipo de problema, o protocolo MAC 802.11 implementa reconhecimentos de camada de enlace. Esse reconhecimento funciona da seguinte forma: Uma estação de destino ao receber um quadro que passou pela verificação CRC aguarda um certo tempo, conhecido como **Espaçamento Curto Interquadros** (*Short Inter-Frame Spacing* – SIFS), em seguida devolve um quadro de reconhecimento. Caso a estação não tenha recebido a confirmação desse reconhecimento essa emite um novo quadro usando o protocolo CSMA/CA para acessar o canal. Se o quadro ainda não for recebido a estação transmissora descartará o quadro.

O protocolo 802.11 além de realizar esse processo também possui o protocolo CSMA/CA, descrito acima, quando uma estação utiliza esse e possui um quadro para transmitir, o processo acontece da seguinte forma:

1º A estação faz uma verificação no canal, se este estiver ocioso ela transmite um quadro após um período curto de tempo, conhecido como **Espaçamento Interquadros Distribuído** (*Distributec Inter-Frame Space* - DIFS);

2º O canal não estando ocioso, a estação escolhe um valor aleatório de recuo usando o recuo exponencial binário e faz uma contagem regressiva a partir desse, se o canal ainda estiver ocupado o valor do contador permanecerá congelado;

3º Quando o contador chega a zero, e o canal não está ocupado, a estação emite um quadro inteiro e fica aguardando um reconhecimento;

4º A estação finalizará o processo de envio quando receber um reconhecimento de entrega do quadro da estação de destino. Tendo outro quadro a ser transmitido a estação inicia o protocolo CSMA/CA na 2º etapa, o quadro não sendo recebido o processo volta para a 2º etapa, escolhendo um valor aleatório em um intervalo maior.

Nota-se que o protocolo de acesso múltiplo CSMA/CD tem a possibilidade de detectar se o canal está ocioso ou não, o CSMA/CA a estação não transmite enquanto o canal não estiver ocioso e inicia uma contagem regressiva.

O CSMA/CD começa a realizar transmissões assim que o canal fica ocioso, o que pode ocasionar em colisão, o que não é um problema, pelo fato dela abortar a transmissão do restante do quadro, no entanto com o 802.11 essa transmissão não é abortada, o quadro é transmitido integralmente. O objetivo do 802.11 é evitar essa colisão sempre que possível, para isso quando o protocolo percebe que uma estação está ocupada o envio do quadro entra em estado de *backoff* aleatório e escolhe valores diferentes, e assim que a estação fica ocioso a transmissão se inicia. Caso exista mais de uma estação transmitindo, uma delas emitirá um sinal de que está transmitindo e a outra aguarda a sua vez, o que evita uma colisão dispendiosa. Caso os valores de *backoff* escolhidos sejam próximos ou iguais, ou haja algum terminal oculto, o risco de haver colisão é grande.

Terminais Ocultos: RTS e CTS

Pensando nas colisões geradas por terminais ocultos, o protocolo MAC 802.11 implementa uma reserva inteligente que pode evitar esse tipo de problema. A imagem seguinte demonstra o que pode gerar um terminal oculto, ambos os computadores estão dentro da faixa do AP e ambas se associam a este, no entanto as faixas de cada estação sem fio está limitada ao interior dos círculos, o que faz com que as estações fiquem ocultas entre si, porem visíveis ao AP.

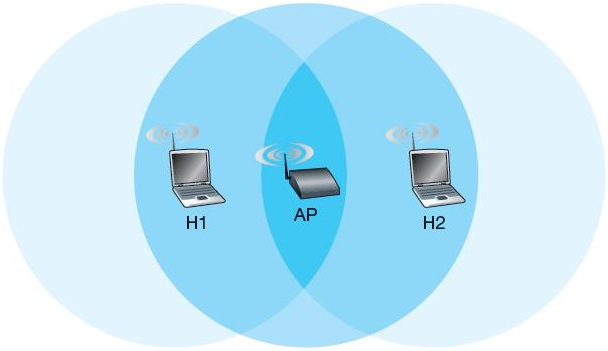

Figura 6: Terminal Oculto

Como a imagem mostra, caso a estação H1 envie uma transmissão para o AP, e H2 deseje fazer o mesmo, ambas não ouvem uma a outra portanto não tem como fazer uma estimativa de quando uma das estações enviará um quadro, ou seja, as duas podem colidir durante a transmissão e o canal será desperdiçado durante a transmissão das duas estações.

Com o objetivo de resolver esse problema o protocolo IEEE 802.11 cria dois quadros de controle, um **RTS (***Request to Send* – solicitação de envio**)** e outro **CTS (***Clear to Send* – pronto para envio**),** assim quando uma estação deseja realizar uma transmissão, essa primeiro envia um quadro RTS indicando o tempo total que será necessário para transmitir um quadro de dados DATA, quando o AP recebe o quadro RTS, ele encaminha um quadro CTS com o objetivo de permitir o envio e alertar as outras estações para que não enviem quadros nesse intervalo de tempo. Portanto, no exemplo da imagem acima, assim que uma das estações for enviar um quadro de dados, essa faz uma transmissão por meio de um quadro RTS, que será ouvida por todas as estações que estirem no seu alcance, incluído o AP, essa então recebe uma resposta de um quadro CTS que também será ouvida por todas as estações que estiverem em seu alcance, como resultado a estação que deseja realizar a transmissão poderá iniciar e as outras vão ficar ociosas pelo período de tempo determinado pelo quadro RTS.

Esses quadros reduzem drasticamente o risco de colisões visto que, um quadro longo de dados pode ser enviado apenas após o canal ter sido reservado, o que reduz o problema da estação oculta. E como esses quadro são curtos, uma colisão duraria somente o tempo dos quadro RTS ou CTS.

Esse recurso, apesar de ser muito útil, provoca consideráveis atrasos e recursos do canal, por isso a troca RTS/CTS é utilizada somente na transmissão de grandes quantidade de dados. Cada estação pode estabelecer um patamar RTS sendo que RTS/CTS será utilizada somente se o quadro for mais longo que o patamar, caso não, a solicitação é ignorada.

O conteúdo descrito até aqui retrata as colisões e o funcionamento do 802.11 com múltiplo acesso. O protocolo 802.11 também implementa um enlace ponto a ponto, que se dá quando duas estações, que possuem antenas, direcionam sua conexão uma para a outra começando a executar o protocolo 802.11. O baixo custo dessas antenas de transmissão ajudaram a rede sem

fio a se difundir pelo mundo, sendo que quando o usuário deseja expandir o seu alcance basta comprar uma antena com maior potência.

O quadro IEEE 802.11

O quadro IEEE 802.11, assim como o quadro Ethernet, é composto por vários campos e subcampos, a imagem abaixo demonstra o funcionamento desse quadro, onde os números acime de cada campo representa o cumprimento em bytes, e os que estão acima dos subcampos representa seu cumprimento em bits:

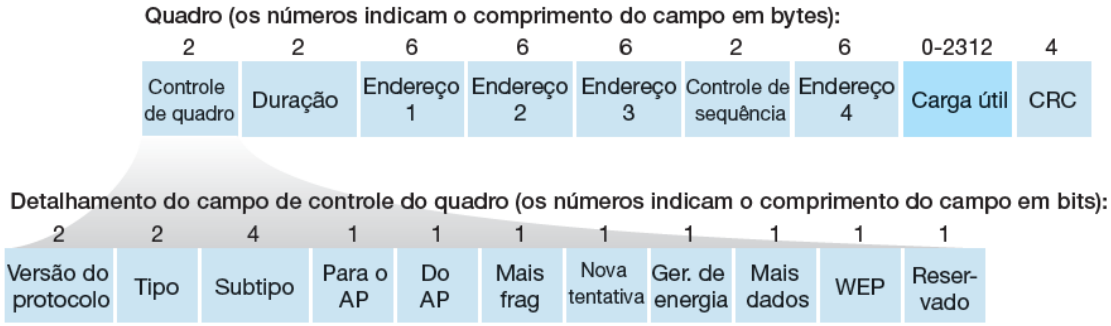

Figura 7: Quadro IEEE 802.11

O principal campo do quadro é o da Carga útil, que é composto pelo datagrama IP ou um pacote ARP, embora o cumprimento desse campo seja de 2.312 bytes, ele costuma ser menor que 1.500 bytes. Um recurso que esse quadro possui, herdado do protocolo Ethernet, é a verificação de redundância cíclica (CRC), onde o receptor consegue detectar erros de bits no quadro recebido.

Uma das principais diferenças do quadro IEEE 802.11 é que esse é composto por 4 campos de endereço e cada um pode conter um endereço MAC de 6 bytes. O três primeiros campos são utilizados para mover o datagrama de uma camada de enlace de estação sem fio para a interface de um roteador, ou seja, para finalidades de interconexão em rede, e o quarto é utilizado quando APs trocam informações entre si, em modo *ad hoc*, voltando aos três primeiros campos eles possuem a seguinte finalidade:

1º - O 2º campo é o endereço MAC da estação que transmite o quadro. Sendo assim toda vez que uma estação ou AP for transmitir um quadro, o seu endereço MAC é registrado nesse campo.

2º - O 1º campo é o endereço MAC da estação que deve receber o quadro. Ao contrário do 2º campo, toda vez que uma estação sem fio ou um AP for fazer uma transmissão o endereço 1 armazena o MAC de destino.

3º - O 3º campo armazena o endereço MAC, da interface de sub-rede no roteador que contém as estações sem fio e o AP. Um AP não fornece e nem recebe endereçamento IP, a sua função é de servir como ponte entre uma estação sem fio, que pode estar alocada a uma sub rede,

e o roteador que fornece acesso à internet e faz o endereçamento IP. O funcionamento desse campo acontece da seguinte forma:

3.1 – O roteador faz o reconhecimento do endereço IP de um host, através do endereço de destino do datagrama, utilizando ARP para determinar o endereço MAC desse host, após a obtenção do endereço MAC, a interface do roteador encapsula o datagrama em um quadro Ethernet. Sendo assim o campo de endereço de origem desse quadro contém o endereço MAC do roteador e o campo de endereço de destino contém o MAC do host;

3.2 – Quando o quadro Ethernet chega ao AP, o quadro 802.3 é convertido em quadro 802.11, antes de transmiti-lo para um canal sem fio. O AP preenche o endereço MAC dos hosts para o campo 3, o AP preenche o endereço de sua interface, assim o AP pode informar o endereço MAC da interface do roteador que enviou o datagrama para a sub-rede;

3.3 – Quando o host recebe o datagrama ele envia uma resposta criando um quadro 802.11 e preenchendo os campo de endereço 1 e 2 com o seu MAC e o do AP, e envia para o 3º campo;

3.4 – Assim que o quadro é recebido pelo roteador, esse converte-o em um quadro Ethernet. O campo de origem para esse quadro é o do host e o campo de destino é o do roteador, sendo assim o endereço 3 permite que o AP, determine qual é o endereço MAC de destino apropriado.

Esses campos também são utilizados para armazenar quadros de associação: RTS, CTS, ACK, dados e WEP (*Wireless Equivalent Privacy*).

No protocolo 802.11, quando uma estação recebe um quadro de outra, essa sempre envia um reconhecimento, mesmo que esse se perca são enviados várias copias, o que permite que receptor faça a distinção entre um quadro e outro que é transmitido, ele também permite que uma estação reserve um tempo para a realização da transmissão, no envio de longos quadros.

Mobilidade na mesma sub-rede IP

Um dos principais fatores das redes sem fio, é a questão da mobilidade, em muitas casas, centros e universidades podemos ver vários APs que mantem as sessões TCP de seu hospedeiro na rede a longas distancias, para ampliar o alcance da rede são instalados diversos APs no mesmo ambiente, o que mantem a conexão do hospedeiro, no entanto para ele se mover entre diversas sub redes mantendo a conexão fixa é necessário um protocolo mais avançado.

A imagem abaixo retrata o funcionamento de um dispositivo, conectado à rede, que está em movimento, como os dois BSSs (estação de rede) estão sendo interconectados por um AP, o endereço IP na subrede se mantem, assim como a conexão TCP, caso a rede fosse interconectada por um roteador, assim que o dispositivo se movesse a conexão TCP poderia ser perdida, e somente após ser atribuído um novo endereçamento IP a conexão se reestabeleceria:

Figura 8: Mobilidade na Rede sem fio

Na imagem acima, como a interconexão acontece por meio de um AP, no momento em que o dispositivo se afasta do BSS 1 o sinal enfraquece, no entanto ele começa a captar o sinal do BSS2, nesse tempo esse se desassocia de BSS1 e associa-se ao BSS2, em alguns casos mantendo o SSID, o IP continua o mesmo e as sessões manterão o seu curso.

O AP consegue facilmente resolver a questão da mobilidade de um dispositivo, porem para um comutador essa questão não é tão simples, quando a movimento é ocasional, o hospedeiro se move a distancias curtas na rede o processo é simples, porém o comutador não consegue manter conexões TCP quando o grau de mobilidade é alto. O comutador consegue captar mudanças entre APs, quando um AP que recebeu um hospedeiro de outro envia um quadro atualizado com o endereço de origem dos hospedeiros, após isso o comutador atualiza sua tabela de repasse, permitindo a mudança de estação de rede.

Recursos Avançados em 802.11

Um dos mais sofisticados recurso do 802.11, é que quando um hospedeiro esta se conectado com uma estação a uma certa distância e com uma taxa de sinal-ruído alta, esse pode utilizar técnicas de modulação da camada física que fornece altas taxas de transmissão, no entanto se o usuário continuar se distanciando da estação de rede, o sinal vai diminuindo de acordo com a distância, até certo ponto onde o hospedeiro não conseguira enviar ou receber quadros de dados.

Em vista disso algumas execuções 802.11 possuem a capacidade de selecionarem suas técnicas de modulação e se adaptarem a esta, e à medida que uma emissão de quadros for ficando fraca com o sinal, este muda para a próxima modulação, sempre subindo de nível quando a força do sinal é forte e descendo um nível quando a força do sinal diminui.

Com o objetivo de facilitar um gerenciamento de energia, o padrão 802.11 minimiza o tempo de funções de percepção, transmissão e recebimento e outros circuitos que são necessários para o seu funcionamento. Um nó na rede pode alternar seu estado para dormir, onde recebe o valor 1 em seu cabeçalho do quadro 802.11, indicando ao ponto de acesso que entrará no estado “dormindo”, nesse tempo o AP não envia nenhum quadro para o hospedeiro, armazenando as informações para um envio posterior. Um temporizador é programado para acordar o nó quando este está em repouso, após ser acordado esse recebe todos quadros destinados a ele. O nó acorda logo após recebe um quadro de sinalização e logo entra em modo ativo, os quadros enviados a

este são mantidos em buffer enquanto ele está no estado dormir, caso ele acorde e não tenha recebido nenhum quadro seu estado volta para dormir.

Segurança Wireless

Os algoritmos de segurança Wi-fi vem se tornando seguro, e evoluindo ao longo do tempo desde 1990 se tornando mais eficaz, esses algoritmos formam um protocolo de segurança para rede sem fio que evita que hospedeiros não autorizados tenham acesso à rede, assim como realiza criptografia dos dados privados enviados através das ondas de rádio. Por mais alto que seja o nível de segurança de uma rede wireless, essa não poderão ser mais segura do que uma rede cabeada, que interliga um ponto A há um ponto B através de um cabo de rede, sem interlocutores, diferente da rede sem fio que transmite o sinal para todos a seu alcance.

Os protocolos de segurança sem fio mais recentes e conhecidos são: WEP, WPA e WPA2.

WEP – Com fio Privacidade Equivalente

Um dos primeiros protocolos de segurança wi-fi, desenvolvido em 1999. Foi implementado com o objetivo de fornecer o mesmo nível de segurança das redes cabeadas, porem teve vários problemas de segurança, o que o tornou fácil de ser quebrado, além disso possui uma configuração muito complexa. Ao longo do tempo foi implementado várias melhoras, no entanto continua sendo um dos protocolos de segurança mais vulneráveis. Por apresentar várias vulnerabilidades o WEP foi posto de lado pela Wi-Fi Alliance em 2004, hoje quase não é mais utilizado e não possui atualizações recentes.

WPA – Wi-Fi Acesso Protegido

Utilizado com uma melhoria temporária para o sistema WEP, esse protocolo foi adotado em 2003. O protocolo utiliza um chave (PSK – *Pre-Shared Key*, Chave pré-compartilhada), referida como chave personal, e usam criptografia TKIP – *Temporal Key Integrity Protocol*. O WPA Enterprise utiliza um servidor de autenticação, que tem como função gerar chaves e certificados. Como o WPA foi uma evolução do WEP, esse utilizou alguns componentes do *firmware* que apresentavam os mesmos elementos vulneráveis, ou seja, apesar de mais seguro que o WEP, ainda existem algumas vulnerabilidades.

Quando a integridade desse protocolo foi posta à prova, ele apresentou muitas vulnerabilidades, uma dessas é que ele fornecia uma conexão a terceiros desautorizados, simplesmente pelo uso de uma ferramenta WPS (Wi-Fi Protected Setup), esta utilizada para facilitar a conexão a Access Point.

WPA 2 – Wi-Fi Acesso Protegido versão 2

Introduzido como uma melhora significativa do WPA, esse protocolo foi desenvolvido em 2004, e trouxe várias vantagens, uma delas foi a criptografia utilizada (AES – *Advanced Encryption Standard*), essa criptografia foi desenvolvida com o objetivo de proteger arquivos secretos do governo americano, o que diz muito a respeito do seu nível de segurança.

O nível de segurança do WPA 2 é muito forte, que é mais fácil um atacante entrar na rede sabendo a senha, ou seja, alguém deve fornece-la para que se obtenha acesso, segurança que está fora de alcance de qualquer máquina, resumindo se a rede tiver um acesso desautorizado é bem provável que a falha tenha sido humana.

Assim como sua antiga versão, o WPA 2 também carrega algumas falhas, porem essas podem levar cerca de 9 a 14 horas para serem encontradas. Dentre os protocolos mais seguros temos a seguinte classificação, lembrando que essas configurações podem ser escolhidas pelo hospedeiro na rede:

1º WPA2 + AES

2º WPA + AES

3º WPA + TKIP/AES

4º WPA + TKIP

5º WEP

6º Rede Aberta, sem qualquer protocolo de segurança definido

Caso o administrador de rede opte por utilizar um protocolo dos últimos na classificação ou não utilize nenhuma, sua ficará vulnerável a ataques, alguém poderá roubar sua largura de banda e instalar aplicações maliciosas que podem monitorar as atividades de quem estiver na rede. Os protocolos mais recomendados são o WPA e WPA2 com a adição da criptografia AES, que impediram que usuários não autorizados tenham acesso facilmente a rede.

Uma desvantagem do WPA2 em relação aos outros protocolos, é que por ser mais seguro, exige uma quantidade maior de processamento, o que exige um equipamento de hardware melhor para que o desempenho não seja perdido. Muitos equipamentos antigos implementa a atualização do firmware para o WPA2, porem o equipamento não possui um hardware muito potente, o que faz com que o protocolo perca seu desempenho. A velocidade de dados pode ser afetada de acordo com o protocolo utilizado.

Apesar do WPA e WPA2 fornecerem um alto nível de segurança, não são as únicas técnicas que o usuário pode utilizar para proteger sua rede, uma senha do tipo “1234” ou “abc”, nome da rede ou do administrador podem ser facilmente quebradas. Para elevar o nível de segurança o administrador pode definir uma senha de até 62 caracteres, o que torna o trabalho de hackers tão complicado que muitos chegaram a desistir de tentar invadir a rede.

Referencias Bibliografia

Protocolos de Segurança de Rede sem Fio, **NETSPOT**, Disponível em: <https://www.netspotapp.com/pt/wifi-encryption-and-security.html>

ROSS, Keith. KUROSE, Jim, **Redes de Computadores e a internet uma abordagem top-down** – 6º ed. – São Paulo, Pearson Education do Brasil, 2013, pags. 380 - 401