FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

MBA em Gestão de Redes e Segurança da Informação

Williams Farias Santos

O CRESCIMENTO E EVOLUÇÃO DAS REDES SEM FIO NO MUNDO

Um Passo Evolutivo e Promissor Para a Chamada "Era da Mobilidade"

ARACAJU
2016

Williams Farias Santos

O CRESCIMENTO E EVOLUÇÃO DAS REDES SEM FIO NO MUNDO

Um Passo Evolutivo e Promissor Para a Chamada "Era da Mobilidade"

Trabalho de TCC (Trabalho de Conclusão de Curso) apresentado ao programa de pós graduação, para a Faculdade de Administração e Negócios de Sergipe - FANESE como requisito para a obtenção de certificação de pós graduado em MBA Gestão em Redes e Segurança da Informação.

ARACAJU
2016

RESUMO

Em vista a um grande e crescente publico que adere às conexões de redes sem fio, seja corporativos ou domésticos, e do outro lado uma grande massa que resiste e opta em manter conexões por cabos nas residências ou corporações, por acharem o nível de estabilidade e interferências menores comparadas as conexões sem fio, venho através deste trabalho, explorar e detalhar o crescimento e o quadro evolutivo das redes Wifi e a visão que as grandes corporações têm sobre elas. Alem da detalhada forma evolutiva da tecnologia que será mostrado, o trabalho consistirão também os motivos de escolha por grandes corporações em migrar todas as suas estruturas internas adotando o meio sem fio como forma de acesso. Iremos abordar também que com seu crescimento evoluíram-se também seus variados métodos de criptografia de dados, protocolos e seus devidos algoritmos que os compõe, foram remodelados para dar maiores níveis de segurança neste tipo de conexão mostrando o crescimento simultâneo com a própria tecnologia.

Um ponto muito questionado é a segurança desse tipo de acesso, irei compara os métodos de antigamente e os da atualidade, evoluímos bastante e a tendência é crescer cada vez mais.

Portanto o trabalho mostrará que trata de um meio ainda em evolução, mais um tanto promissor, que a cada ano especialistas da área aumentam gradativamente sua estima quanto a esse método de acesso, e que só estamos no começo da "*Era da Mobilidade*".

PALAVRAS-CHAVE: Wifi. Estabilidade. Evolução. Tecnologias. Segurança.

OBJETIVOS GERAIS: O estudo tem como foco mostrar a evolução histórica desse tipo de conexão, deixando claro que esse método veio para ser uma escolha ativa e não paliativa como uma grande massa de consumidores deste recurso ainda pensa, e principalmente explorar todas as mudanças e novos recursos que a quinta geração sem fio veio a nos oferecer, frisar as futuras evoluções e enxergar o caminho promissor que esta tecnologia tem a nos oferecer.

OBJETIVOS ESPECIFICOS:

- Demonstrar as crescentes evoluções históricas, das gerações sem fio;
- Mostrar o crescimento significativo de usuários e perspectivas de crescimento;
- Apresentar e detalhar os novos recursos do ultimo padrão lançado (802.11ac);
- Mostrar métodos de criptografia e segurança de acesso e suas evoluções.
- Vantagens e desvantagens para cada tipo de protocolo de autenticação.
- Redes sem fio para as corporações.
- Mostrar aspectos promissores e o caminho que essa tecnologia esta tomando;

JUSTIFICATIVAS

Mostrar seu crescimento dos últimos anos, e o quanto esse tipo de tecnologia é viável para usuários domésticos e pequenos, médios e grandes corporações, com possibilidades de migração das redes locais adotadas em sua grande maioria na atualidade (cabeada), para conexões WiFi, com seus vários recursos, levando em consideração custos e benefícios, nível de segurança e etc. Para sua implementação. Perspectiva de crescimento simultâneo com a segurança de acesso de dados.

INTRODUÇÃO

Não é de agora que o crescimento exponencial das redes sem fio vem aumentando no Brasil e no mundo, principalmente pelas grandes corporações que vêem nesse método de conexão algo atrativo tanto no baixo custo de implementação e manutenção, quanto no nível de segurança que também vem crescendo junto com a própria tecnologia. O numero de assinantes de telefones celulares já aumentaram em 34 milhões, números registrado logo no início da década de 90. Estima-se que até o fim da próxima década teremos em todo mundo mais de quatro bilhões de assinantes moveis ultrapassando assim o numero de assinantes fixos.

De acordo com a empresa *CISCO SYSTEM*, uma das maiores empresas de tecnologia e infra-estrutura do mundo, em 14 de maio de 2015, cita que o maior responsável por esse significativo crescimento, dar-se a criação de tecnologias e dispositivos moveis mais potentes, combinados a um acesso mais amplo a celulares e conexões mais rápidas serão de fato as principais responsáveis pelo aumento significativo no volume do trafego móvel. Ainda de acordo com a empresa, acredita-se que até o ano de 2019 o aumento global de trafego móvel, irá ultrapassar o aumento global de trafego fixo, pelo fator de quatro principais tendências que impulsionarão o aumento induzido do trafego de dados móvel, são elas:

- **Mais usuários moveis:** Até 2019, a empresa estima-se que haverá 5,2 bilhões de usuários com dispositivos moveis, atualmente quase 59% da população mundial são usuários moveis, até 2019 este numero deverá subir para 69% da população mundial, equivalente e 7,6 bilhões de pessoas.
- **Mais conexões moveis:** Até 2019 haverá cerca de 11,5 bilhões de dispositivos/conexões.
- **Velocidades moveis mais rápidas:** A velocidade estará 2,4 vezes maior que o atual.
- **Mais vídeos moveis:** Até 2019 o volume de vídeos moveis representará 72% do trafego global, superando os 55% registrados no inicio do ano.
  (Dados da Cisco System, 14 de maio de 2015)

O crescimento desta tecnologia dar-se também a evolução significativa de seus padrões, tais como as novidades imprescindíveis trazidas por eles, novidades de peso serão abordadas e

comparadas umas com as outras. A tecnologia Wifi vem trazendo nos últimos anos grandes inovações, no que refere-se ao setor de comunicações, ela esta sendo considerada a maior inovação no setor, dentre essas inovações, estar o novo padrão recém lançado, o 802.11ac, nele estarei mostrando todos os novos recursos e diferenciais comparado aos padrões anteriores. De acordo uma pesquisa feita pela empresa ***Epitiro, empresa especializada em redes de comunicação,*** *os consumidores perdem até 30% da velocidade da Wi-fi por contas de interferências de outros aparelhos eletrônicos e de barreiras como paredes, moveis e portas(Correios Braziliense, Ataide Almeida Jr. 03/05/2011)* .

Entretanto, detalharei um grande recurso composta em seu ultimo padrão que poderá sanar este problema, e tornar a conexão mais estável. São necessidades de resoluções como estas, que grandes empresas vem adotando cada vez mais este método de comunicação de dados como primário, vendo todo crescimento de recursos, segurança, desempenho, praticidade e baixos custos, não seria convencional não despertar o interesse pela tecnologia e a vontade de implementá-las em seus ambientes, e escolhendo esse meio de comunicação para gestão e controle de seus dados.

SURGIMENTO E SEU HISTÓRICO EVOLUTIVO

Nos tempos atuais definimos qualquer trafego de dados sem a presença de um meio físico e comutador de Redes Wireless, ou seja, é toda conexão entre dispositivos com o objetivo comum na troca de informações sem a necessidade de um meio físico para interligá-los. Antes mesmo dessa definição se tornar parte de nossa atualidade, as atuais redes sem fio foram originadas das antigas transmissões por ondas de rádio. A partir daí, descobriram-se uma serie de descobertas e avanços científicos que foram se desenvolvendo. Há vários relatos sobre o surgimento das redes Wi-fi, para diversos períodos e anos, muitos afirmam que o surgimento dessa tecnologia foi durante a segunda guerra mundial, mas também não sabem que as primeiras faíscas de idéias surgiram bem antes disso. Na verdade a segunda guerra mundial beneficiou-se e muito com essa tecnologia, durante a guerra muitos militares usavam para trocar informação sobre a guerra e troca de mensagens entre ambos.

1831 – Michael Faraday descobre os princípios da indução eletromagnética.

1842 – Joseph Henry descobre que uma faísca elétrica entre dois condutores pode ser utilizada para induzir magnetismo entre agulhas, esse efeito é detectado a uma distância de 30 metros.

1858 – Feddersen descobre o caráter oscilatório das faíscas elétricas.

1867 – James Clarck Maxwell desenvolve sua teoria do eletromagnetismo e prediz a existência de ondas elétricas no éter.

1870 – Von Bezold descobre a interferência com descargas de compensadores.

1875 – Thomas Edison nota um fenômeno que denominou "força entérica", mas abandonou a idéia quando Elihu Thompson, dentre outros, ridicularizaram a idéia.

1879 – David E. Hughes descobre que um tubo de arquivamentos férreos fica condutivo por ação à distância através de faíscas elétricas, ele faz um sinal audível em um fone em uma distância de 500 metros, mas parou suas experiências, pois Sir George Stokes julgou que os acontecimentos demonstravam indução simples.

1882 – Graham Bell e William H. Preece transmitem sinais de Telégrafo *Wireless* através do mar por meios de indução, entre a Inglaterra e a Ilha Wight.

1887 – Heinrich Rudolph Hertz, professor privado em Kiel, descobre que o efeito de faíscas elétricas está baseado nos fenômenos das ondas no éter. Ele confirmou a teoria de Maxwell, onde as ondas viajam pela mesma velocidade de luz.

1890 – Branly chama a atenção às propriedades de tubos com arquivamentos férreos que foram redescobertos e desenvolve o primeiro *coh erer* para detectar ondas de rádio.

1892 – Preece sinaliza no canal de Bristol com seu sistema de indução.

1893 – Tesla demonstra publicamente a comunicação *wireless* via rádio em St. Louis, descrevendo em detalhes os princípios da comunicação via rádio.

1894 – Ledge repete os testes de Herz com um *coherer*.

1895 – em seqüência, Tesla encontra sinais de recebimento das telegrafias de seu laboratório em Nova Iorque em West Point, Marconi transmite o primeiro telégrafo, e Popoff constrói um receptor para ondas elétricas naturais onde tenta descobrir temporais.

1896 – Marconi demonstra a telegrafia *wireless* ao escritório de telégrafo inglês, após um ano testando na Itália. Ele prova as possibilidades de telegrafia sem fios com um *coherer*.

1897 – Marconi adquire a patente do telégrafo *wireless* e estabelece a primeira "Estação Marconi" em Needles (Ilha Wight), esta estação envia um sinal à costa inglesa a mais de 22 km.

1898 – em 3 de junho é enviado a primeira telegrafia *wireless* paga, enviada de Needles, e em 20 julho, a primeira mensagem de jornal é enviada de um navio para o Daily Express sobre os resultados de uma competição de navegação.

1901 – Marconi usa sintonia entre os receptores e transmissores, e em 12 e 13 dezembro,

primeiro sinais são enviados pelo Oceano Atlântico de Poldhu para New Foundland (2800 km).

1902 – Marconi desenvolve o detector magnético, e há a primeira comunicação bidirecional através do Atlântico.

1903 – Schlömilch desenvolve o detector eletrolítico, Poulsen descobre a transmissão de ondas contínuas com um arco elétrico, e surge o primeiro serviço de notícias para navios em mar, o "Serviço Marconi" *wireless* de Londres para o "Handelsblad"holandês.

1971 – Primeira rede *wireless*, a Alohanet, na Universidade do Hawaii.

(Fonte: Ghz tecnologia, postado por: George Batista em 8 de abril de 2013).

A partir da comprovação do surgimento da primeira conectividade sem fio, surgia para o mundo uma grande revolução no que desrespeito ao método de interconexão de dispositivos e trafego de dados, devido ao único método de conexões existente na época e suas limitações, custos e complexidade na criação e estruturação de cabos para um ambiente e sua interligação, o surgimento desse novo método, trouxe consigo novos conceitos de infra-estrutura e flexibilidade de adaptação. Com o passar dos anos, a recém descoberta foi ganhando força e popularidade, e aumento de demanda para esta descoberta.

Depositando todas as fichas nessa nova promessa tecnológica, o Instituto de Engenheiros Elétricos e Eletrônicos - IEEE formou um grupo de pesquisa para criar padrões que pudesse tornar essa novidade cada vez mais em realidade, denominando assim em 1990 o projeto Padrão IEEE 802.11, durante sete anos esse projeto ficou em papel por fatores que impediam desse projeto ganhar vida própria e sair do papel. Depois desses anos de espera, algumas empresas começaram a enxergar o projeto como promissor efetuando assim generosos investimentos na tecnologia originando não só o padrão origem (802.11), como também diversas variações desse mesmo padrão para cada uma delas, trazendo novidades e melhorias não só em velocidade como também em segurança, desenhando um futuro promissor.

PRINCIPAIS PADRÕES E SUAS EVOLUÇÕES

Padrão 802.11b

Esse padrão trabalha de forma spectral, ou seja por seqüência direta para transmitir e receber dados em 11 megabits. Contudo esses 11 megabits incluem todo o everhead(Processamento ou armazenamento excessivo) na rede no incio e no final dos pacotes na rede, tava de throughput(Quantidade de dados transmitido de um emissor a um recptor) é teoricamente cerca de 7 Mbps, mas a maioria dos usuários não conseguem atingir esta taxa conseguindo em torno de 4 ou 5 Mbps.

Esse padrão possui 5 taxas de transferências, 11 Mbps, 5,5 Mbps., 2 Mbps,1 Mbps e 512 Kbps iniciando pela mais alta, chegando a mais baixa caso haja interferências no ambiente, importante ressaltar que as velocidades mais baixas, foram originadas do protocolo original seu antecessor 802.11, velocidades nas quais alguns equipamentos da atualidade não mais o suportam.

Padrão 802.11a

Esse padrão surgiu em meados de 2002, curioso por que esse padrão veio depois da linha 802.b desordenando a seqüência alfabética, na verdade o órgão responsável pela padronização desses procedimentos, ratificou os dois protocolos de forma simultânea, mais uma parte do espectro em que deveria operar ainda não estava disponível, tendo como resultado a liberação do protocolo 802.11b primeiro que o protocolo 802.11a.

Em relação ao protocolo 802.11b, ele possuem alguns avanços relevantes como:

- Executa em uma velocidade maior, bruta de 54Mbps ou aproximadamente 25 Mbps de throughput real.
- Funciona somente em mais curtas distâncias, mas tem melhores protocolos que o 802.11b para distinguir a reflexão interna de sinais.
- Suporta um numero maior de usuários conectados em largura de bandas completas no mesmo espaço físico.

Devido a utilização de banda de 5Ghz que o protocolo 802.11a utiliza, ele passa ser incompatível com os dispositivos 802.11b.

Padrão 802.11g

Em meados de 2003, surge mais um padrão, o diferencial 802.11g, devido a incompatibilidade de velocidade entre os protocolos anteriores, este novo protocolo fez a diferença, operando também em 54Mbps como o 802.11a, e possuindo retro compatibilidade total com as especificações antigas.

Uma das grandes vantagens do 802.11g em relação aos demais, é que ele trata mais apropriadamente a inevitável reflexão do sinal. Sinais de rádios colidem com diferentes tipos de materiais, chão, metais, até mesmo o ar ao seu redor, o 802.11g divide o espectro de maneira que permita que os receptores tratem essas reflexões de forma mais simples e mais efetiva que os demais.

Evoluções das taxas de transmissões

PADRÃO	LARGURA DE BANDA (MHz)
802.11	1
802.11b	5

802.11a/g	20
802.11n	20 / 40
802.11ac (fase 1)	80
802.11ac (fase 2)	160

***Figura 1**, fonte: www.teleco.com.br, publicado por Arnaldo de Carvalho Jr. Em 26/08/2013.*

Padrão 802.11n

As versões antecessores operavam sobre o canal de 20Mhz, surgi o padrão 802.11n que introduz a possibilidade de trabalho com canais de 40Mhz de banda permitindo duplicar as taxas de transferências por canal, mais que isso permite que 2 canais adjacentes sem superposição de 20Mhz sejam combinados para formar um único canal de 40Mhz. Desta forma o protocolo 802.11n pode ser configurado com 20Mhz, 40Mhz ou conversão inversa de 40Mhz para 20Mhz.

Quando se utiliza este protocolo com canais de 20Mhz na banda de 2,4Ghz, pode-se atingir até 288,9 Mbps. De forma análoga, na banda de 5Ghz qualquer canal disponível pode ser designado com largura de 40Mhz, permitindo atingir expressivas taxas de 600Mbps.

O padrão IEEE 802.11n permite uma modulação e codificação mais eficiente do que seus predecessores, empacotando mais informação em cada subportadora. Isto se deve ao fato que dispõe de um conjunto muito mais amplo de taxas de modulação. As taxas de modulação, referidas pelo IEEE como *Modulationand Coding Schemes – MCS* referem-se a técnica de modulação (por exemplo, *Binary Phase Shift Keying - BPSK, Quadrature Phase Shift Keying – QPSK, Quadrature Amplitude Modulation – QAM*, etc..), a taxa de codificação (proporção útil de informação contida no código transmitido) e ao número de fluxos espaciais transmitidos.

Mais recente Padrão 802.11ac

Há 15 anos depois, do seu primeiro esboço de conexões sem fio, nasce o atual protocolo com características bastantes relevantes, causando um enorme diferencial dos demais protocolos criados até o momento.

Em conexões de redes sem fio, 3 funções imprescindíveis são fundamentais e inter-relacionados de modo a permitir estabilidades de sinal e maiores taxas de transmissão. São eles:

- Aumento da largura de banda utilizada;
- Aumento da eficiência espectral;
- Relação Sinal/Ruído.

Assim como os padrões anteriores, o padrão 802.11ac explora justamente estes itens de modo a permitir o aumento da taxa de transmissão. A largura de banda utilizada por um canal de tem sido aumentada a cada novo padrão WLAN utilizado.

Com o aumento do fluxo de dados, na medida em que a tecnologia evolui e a necessidade por redes cada vez mais seguras e rápidas para suportar aplicativos que requerem mais larguras de bandas como vídeos, imagens de altas resoluções, aplicativos voip que estão causando impactos em todos os setores. Para acompanhar e atender esta demanda, o ultimo padrão lançado veio como nunca despertar interesse de grandes corporações e uma solução para que até então as redes sem fio não atendiam, tratando-se de estabilidade e velocidade, agora tráfegos em Ghz, o novo padrão oferecerá um desempenho três vezes maior em relação ao 802.11n.

A nova tecnologia wireless garante velocidades de até 1.300 Mbps em uma freqüência de 5Ghz, e são totalmente compatíveis com redes 802.11n. Permite que os roteadores e seus devidos receptores possam trocar dados com o objetivo de transmitir vídeos em Full HD e totalmente compatíveis também com as tecnologias 3D. É permitido realizar com esse novo padrão, múltiplas conexões de alta velocidade. Segundo os fabricantes um dos principais diferencias é o raio de amplitude, comparado ao padrão antecessor, a amplitude dobrou, podendo efetuar transmissões que estejam em até 200 metros de distância.

Comparação de velocidades e alcance

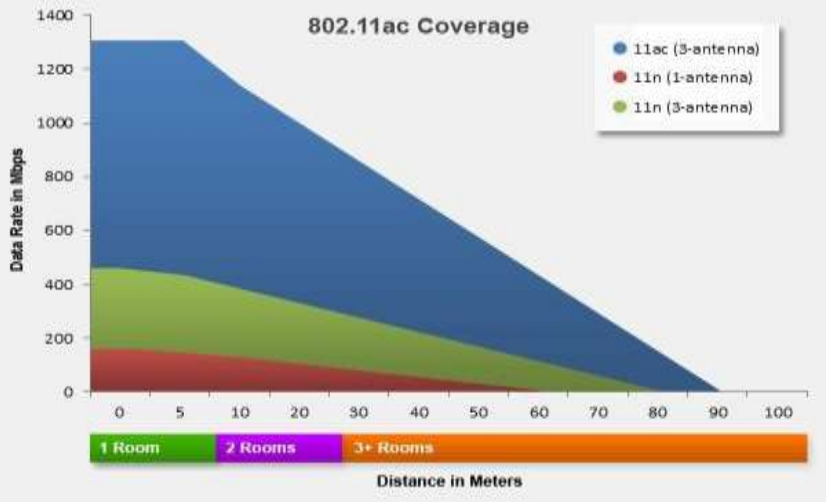


***Figura 2**, fonte: www.tecmundo.com.br, publicado por Fábio Jordão. Em 22/02/2012.*

Outro importante diferencial desta nova tecnologia, e os dispositivos que os suportam é a qualidade do sinal, chega ser tão superior que tanto faz ter um ponto de transmissão para 20,30, 50 metros, os dispositivos que trabalham com esse padrão conseguem enviar e receber dados da mesma maneira como se estivesse a menos de 5 metros de distância do pronto transmissor, ou seja, nada importa a distância nesse caso, desde que os pontos de emissão e recepção estejam respeitando os 200 metros conforme o protocolo garante, a comunicação irá acontecer normalmente.

Outro importante fator é a forma de propagar sinal, inteligentemente em vez de propagar sinal de forma uniforme, para todas as direções, os dispositivos suportados por esta tecnologia, identificam pontos ativos no raio alcançado, direcionando e reforçando de forma automática o sinal onde há dispositivos identificados por ele, denominando tecnologia *Beamforming*, garantindo comunicação direta entre os dispositivos da rede, sem propagação desnecessária para o ambiente. A imagem abaixo mostra a diferença de propagação dos dispositivos atuais, para os novos dispositivos compondo tecnologia *Beamforming.*

Comparação na forma de propagação de sinal

***Figura 3**, fonte: www.tecmundo.com.br, publicado por Fábio Jordão. Em 22/02/2012.*

Para melhor entendimento da transformação fundamental das redes sem fio, é como tivéssemos que transportar, por exemplo, uma enorme carga, onde precisaríamos de uma quantidade x de caminhões para o transporte, colocando em prática esse novo padrão 802.11ac, a partir do inicio do transporte do primeiro caminhão, onde todos percorrerão um mesmo trajeto, quanto maior a velocidade de entrega de cada caminhão, menor será o tempo de entrega total da carga, ou seja, a velocidade dos caminhões transitarem e liberando o percurso, os caminhões seguintes terão seu trajeto livre para percurso e conseqüentemente o tempo de transporte será muito mais rápido. O meio estará livre e mais rápido, devido a altas taxas de transmissões possibilitando um maior número de clientes conectados de forma simultânea. Devido a velocidade os dispositivos como smartphones e tablets terão uma vantagem extra, estarão transmitindo por menos tempo, que resulta em menor consumo de bateria, dando mais durabilidade aos dispositivos dessa espécie.

Ainda que os dispositivos contivessem o padrão 802.11ac ampliem qualidade de sinal, a velocidade e eliminem alguns defeitos, essa tecnologia não terá eficiência completa na questão velocidade, em vista que uma parte das regiões do Brasil ainda operam com velocidades de internet abaixo do que os roteadores conseguem transmitir. Quanto aos padrões antecessores, provavelmente irão entrar em extinção, para compatibilidade com o

novo padrão será necessárias infinitas adaptações que tornarão as redes coorporativas extremamente complexas e virtualmente impossível de gerenciar.

Em geral as vantagens e a confiabilidade que este padrão vem trazendo, com certeza mudará significativamente o modo pelo qual as redes sem fio progredirão a partir desta genial inovação.

PRINCIPAIS CRIPTOGRAFIAS E SEGUNRANÇA DE ACESSO

Com o crescente popularismo das redes sem fio no mundo, fez-se de grande exigência também crescer, ampliar também de forma simultânea a segurança deste tipo de acesso, não basta no mundo das tecnologias proporcionar meios de acesso sem ao menos pensar em segurança de acesso e tráfego dos dados. Como a tecnologia cresce no mundo a segurança também suas crescente evoluções, os grandes desafios dos especialistas de segurança, seria conciliar segurança com a interoperabilidade entre diversos dispositivos e aplicações de diversos tipos de fabricantes, fazendo com que todos eles utilizem da segurança e possibilite de padronização junto ao órgão competente responsável por controla essa tecnologia IEEE 802.11.

Com todo crescimento fez com que o órgão iniciasse estudos para prover segurança a este tipo de acesso, em vista de que quando temos um meio compartilhado com possibilidades de muito acesso faz jus um protocolo que gerencie isso, evitando assim que os sinais enviados por vários remetentes não causem interferências nos receptores, causando sobrecarga na rede e inatividade da mesma.

Para isso ressalto a importância de falar sobre um dos primeiros protocolos e gestão de acesso criado para as redes sem fio, trata-se do protocolo CDMA.

O CDMA (Code Division Multiple Access) significa acesso *múltiplo por divisão de código*, funciona da forma que os dados transmitidos se transforme em um sinal de radio codificado, recebidos pelas antenas e convertidos para o receptor final. A energia de cada sinal é codificado e espalha para toda largara de banda especificada pelo um código especifico para cada usuário. Nesse protocolo o ruído é algo que tem de ser tratado, quanto maior a quantidade de usuários disputando a mesma banda o ruído pode aumentar, recomenda-se usar um controle de trafego para evitar sobrecarga na rede e tornam a mesma inoperante, geralmente ocorre em períodos comuns em época de festas comemorativas.

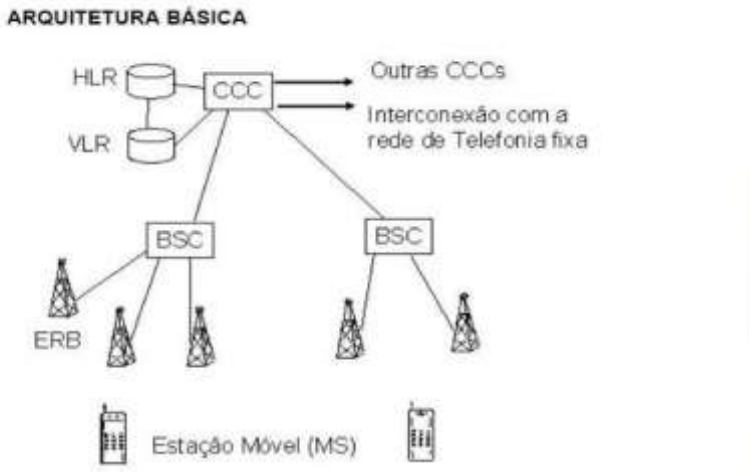


***Figura 4**, fonte:* http://www.ebah.com.br/content/ABAAAAOsYAC/trabalho-cdma*, publicado por Patrick Simoni Rocha. Em maio de 2013.*

Ms – estação móvel é identificada por um MIN- Mobile Identification Number, o equipamento ainda dispõe de um numero de equipamento.

ERB – Estação de rádio responsável pela comunicação com as estações moveis e a sua determinada área de cobertura.

BSC – Responsável por controla um numero de ERB´s, em alguns sistema CDMA as funções do BSC são implementadas na CCC.

CCC – Central de comutação e controle é responsável pelas funções de controle e comutação nas estações moveis localizada em uma área geograficamente designada.

HLR – Registro de assinantes locais e base de dados que contem informações sobre assinantes de um sistema de celular.

VLR – Registro de assinantes visitantes é a base de dados que contem informações sobre os assinantes em visitas a um sistema de celular.

fonte: http://www.ebah.com.br/content/ABAAAAOsYAC/trabalho-cdma*, publicado por Patrick Simoni Rocha. Em maio de 2013.*

Embora estivesse quase absoleto e com o surgimento de sua grande concorrente, a tecnologia GSM – Global Mobile System / Sistema global de comunicação móvel, trazendo assim mais vantagens e recursos, os desenvolvedores do CDMA, trataram logo de corre atrás do prejuízo e começaram a melhorar o protocolo, tornando-o um dos melhores em cominações multimídias, ganhando novamente mais respeito no mercado e oferecendo cada vez mais velocidades nas transmissões de dados. Embora não seja a tecnologia mais usada mundialmente mais trás excelentes recursos e perspectivas de serviços relacionados à voz e dados.

Com desenvolvimento e expansão do padrão 802.11 e grande concorrência das tecnologias referenciadas a gerenciamento de acessos e tráfegos de dados, e seu respectivo crescimento exponencial de aderentes as redes Wlan´s, faz-se necessário pensar a fundo na segurança de

acesso e tráfegos dos dados. Junto com a norma padrão responsável, em setembro de 1999 foi criado o protocolo **WEP (Wired Equiavalent Privacy)** primeiro protocolo criptografado criado e ainda usado nos dias de hoje, mesmo ainda havendo varias falhas de segurança.

Como todo protocolo que refere-se à transferência de dados, dar-se a exigência de alguns itens imprescindíveis tais como:

- **Privacidade:** Permite que ao dados trafegados no meio esteja em sigilo, privativos em total restrição a pessoas não autorizadas a ler, tais exigências dar-se ao mecanismo de privacidade dos dados, onde somente quem tem autorização para lê-los e que terão acesso.
- **Criptografia:** Processo de embaralhamento dos dados, onde o mecanismo resume em dificultar a leitura dos mesmos a quem não esta autorizado a ler, a cifra desses dados só podem ser decifrados pelo ponto emissor com autorização para tal ação, com isso garanti-se a total integridade das informações, ou seja, sem riscos de violação.
- **Autenticação:** Deve ser de forma mutua, exigindo com que todos dispositivos que queiram ingressar em uma rede sejam exigidas pelos dispositivos controlador (AP - Access Point) sua senha de permissão para penetra na rede e poder usufruir de seus recursos.
- **Controle de acesso:** Gerenciado também pelo ponto de acesso (AP – Access Point) e deve fazer controle de quem entra e quem não entra em uma rede que possui controle de permissões de acesso. O gerenciador fará todo processo de autenticação de quem é permitido e negação de ingresso a rede a quem não tiver acesso.

Com as exigências citadas acima, o órgão responsável (802.11) por cuidar de todos os procedimentos ao que refere-se segurança e estabelecer o meio comunicativo com total padrão de uso, independente dos seus variados fabricantes, foi que se fez necessários criar protocolos que nos dê segurança no trafego de dados, evitando assim a captura e leitura dos mesmos por pessoas não autorizadas que o órgão criou seu primeiro protocolo de segurança, segue abaixo:

Wep

Primeiro protocolo criado pelo padrão 802.11, basicamente consiste em uma senha que possa ser compartilhada com a função de criptografa os dados sendo usada de forma estática, e fornece somente um controle de acesso e de privacidade de dados na rede.

A criação deste protocolo veio com a intenção de dar compatibilidade a redes cabeadas no quesito segurança, quem provem de chaves de acesso de 64 a 128 bits, acompanhado de seu algoritmo nomeado de RC4, que fará a função de criptografa todos os pacotes nela trafegado. Alem disso o mesmo algoritmo se encarrega de detectar erros de pacotes verificando a autenticidade dos mesmos. Quando a autenticação WEP é definida cada dispositivos que deseja integrar-se a rede através de seus prontos de acessos faz necessário possuir uma chave, nela você terá a possibilidade de ingresso como é usada para cifrar (encriptar) os dados antes de começarem a serem transmitidos pelas ondas de rádio, quando o receptor recebe dados não

encriptados e com a chave respectiva ao acesso, o dado é inteiramente descartado e não conseguira chega ao seu destino, com esse mecanismo impede o acesso de dispositivos não autorizados garantindo assim um acesso seguro e restritivo.

O processo de autenticação a rede e dada da seguinte forma:

- **Open System** – Sistema aberto: Permite que qualquer um dispositivo acesso a rede, basta somente selecionar o SSID – *Service Set Indentifier (Nome da Rede),* dessa forma os pacotes são enviados sem nenhuma criptografia são enviados via broadcast. Para autenticação deste método no ponto de acesso, é simples o dispositivo com a intenção de acesso faz o pedido para autenticar, logo em seguida o ponto de acesso o envia uma mensagem informando que a sua autenticação foi efetuada e este dispositivo passa a esta em associação com ponto de acesso, a partir dai o dispositivo conectado entra em um canal de comunicação definido pelo ponto para a sua comunicação, e a taxa de transferência definida pelo órgão regente.

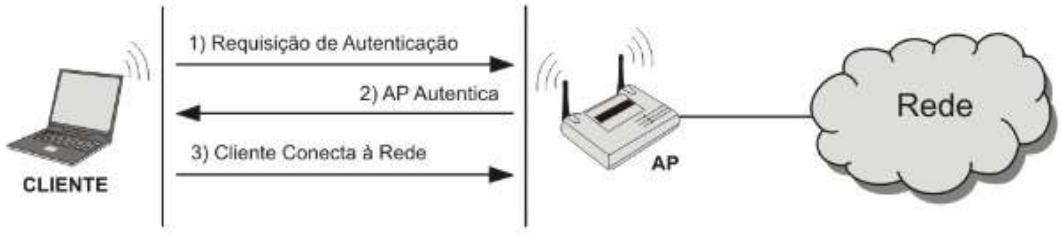


***Figura 5**, fonte:Artigo, Uma analise dos mecanismos de segurança, publicado por André Guedes Linhares e Paulo André da S. Gonçalves*

Acima mostra pedido de autenticação de um cliente para um ponto de acesso, pelo fato de ser uma conexão aberta o ponto de acesso autentica de imediato informando ao dispositivo que requisita autenticação que o mesmo já encontra-se autenticado e pronto para utilizar os recursos da rede.

- **Chave compartilhada:** O processo de autenticação com uma chave compartilhada é dada na forma que o cliente tem em poder uma chave de acesso onde o mesmo envia um frame de autenticação para o ponto de acesso, quando o ponto de acesso recebe este frame, em seguida responde com outro frame contendo 128 bytes de texto randômicos criptografados pelo protocolo (WEP). O cliente recebe este frame, e o reenvia com a chave compartilhada também encriptada, o ponto de acesso recebe e a compara com o frame inicialmente enviado e sua respectiva senha compartilhada, se estiver correto, é retornado ao cliente uma mensagem de ingresso na rede com sucesso, caso contrario ele responde com uma mensagem negando de que seu acesso não pode ser efetuado, e volta a pedir novamente a chave compartilhada, fazendo com quê o processo volte ao inicio. A figura abaixo ilustrará com clareza uma autenticação através de chave compartilhada.

.

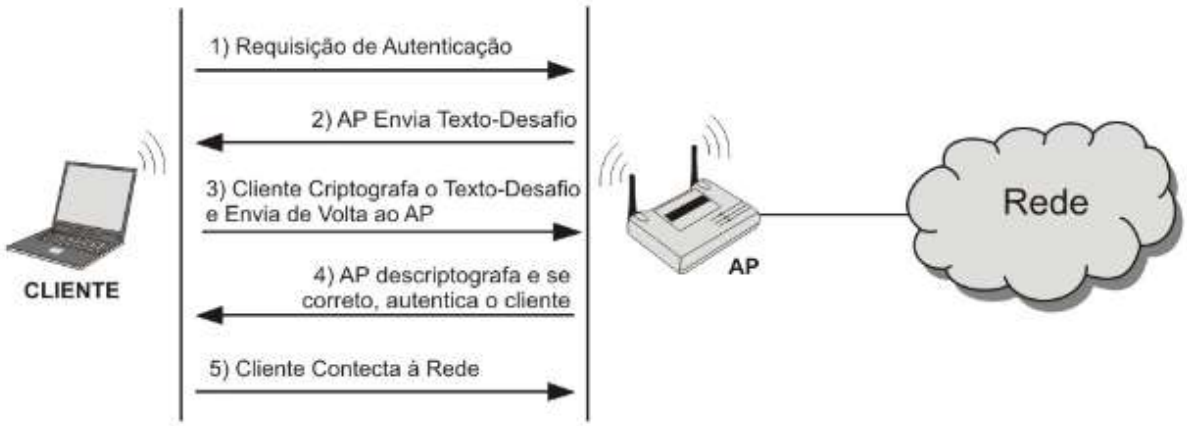


***Figura 6**, fonte:Artigo, Uma analise dos mecanismos de segurança, publicado por André Guedes Linhares e Paulo André da S. Gonçalves*

Desvantagens

Como toda solução tecnológica não é perfeita e nem um "mar de rosas" com o passar do tempo e seu uso o WEP foi mostrando varias vulnerabilidades, na qual inviabilizaram o sucesso do protocolo, dentre elas estão:

- Qualquer cracker que utilize de uma ferramenta dedica como WEPcrack e Aircrack dentre outras pode-se decodificar quadros que estão codificados e trafegando na rede.
- Alem disso o checksum (checagem de erros) do protocolo é inseguro, possibilitando alguém mal intencionado condições de alterar os mensagens.
- Vetores de inicialização são curtos e são enviados sem criptografia.
- Um usuário sem autenticação não existem criptografia.
- Não trabalha por autenticação, baseado na associação ao endereço MAC.

Dos problemas de segurança listadas acima, o protocolo perdeu mercado, a segurança para o protocolo não foi criada de forma fim a fim, visa somente interferir ataques de acesso a rede (não- autenticação) e a leitura de dados, em vista que a criptografia somente é dada para uma conexão com chave compartilhada.

Com intuído de corrigir o "fracasso" que foi o WEP, as grandes corporações preocupadas com as visíveis vulnerabilidades apresentadas, temiam muito pela possibilidade de interceptações de seus dados o órgão responsável 802.11 criou um *Task* que correspondia a um grupo de especialista que seriam responsáveis em criar uma segurança superior ao protocolo recém fracassado. Com toda a necessidade de criar uma solução com mais segurança e rápida devido ao grande crescimento dos dispositivos sem fio, o novo grupo denominou-se **802.11i** onde para atender a grande necessidade de segurança deixada a desejar pelo WEP, começaram a desenvolver um novo protocolo cuja finalidade era tratar de todas as vulnerabilidades identificadas em seu protocolo anterior. Com isso criou-se o **TKIP(***Temporal Key Integry Protocol*).

Tkip

Criado em 2002 e considerado por muitos o sucessor do WEP, onde o seu antecessor tinha grandes dificuldades nas trocas das chaves, o mais novo protocolo veio de fato corrigir isso. A troca da chave nesse novo processo é trocada a cada 10.000 pacotes trafegados na rede, isso significa que, se um atacante quebre a sua senha, isso será efetivo de forma temporária, por que como o protocolo utiliza-se de renovação periódica a chave do atacante recém adquirida com passar do tempo já não valerá de nada. Para efetua essa contagem o protocolo dispõe do vetor de inicialização de pacotes, o mesmo utilizado pela tecnologia anterior, mais alterado, melhorado para esta tecnologia.

O TKIP dobrou o tamanho do vetor de inicialização, o tamanho foi aumentado para 48 bits, 24 bits a mais comparado a tecnologia anterior possibilitando um espaço maior de *keyStreams*, que nada mais é o espaço utilizado para o armazenamento de cifras de chaves.

Outra melhoria feita no TKIP foi usar uma combinação de chaves compartilhada entre o ponto de acesso e endereço Mac do cliente, o adaptador do cliente dessa forma terá uma chave única e diferente para cada cliente que venha a se conectar, uma chave temporal adquirida pelo mesmo, denominada de Temporal Key, nome que forma parte da nomenclatura do protocolo correspondente.

Aes

O AES (*Advanced Encription Standard*) foi projetado para permitir a expansão das chaves quando necessário, com propósito de ser trabalhado tanto com nível de software como no de hardware que permite o seu uso em diversas aplicações. Possui uma chave criptografada e blocos ambos de tamanho 128, 192 e 256 bits.

Usar este mecanismo de cifras garante sim uma maior segurança, a única desvantagem é que exigi-se muito processamento, em equipamentos com menor custo onde o processamento não é superior, causa ouverhead na da rede, ou seja devido a seu alto processamento com equipamentos de baixo controle e gerenciamentos desses processos acabam travando, impedindo assim de serem executadas qualquer tarefa.

Wpa

No ano seguinte em 2003, baseado no projeto do ano anterior o TKIP, e reajustando alguns mecanismos de criptografia, foi criado o WPA (Wifi Protected Access) originada do padrão 802.11i e da progressão de estudo dos desenvolvimentos de mecanismo TKIP e AES. É considerada uma solução interina para protocolo WEP, o novo padrão de autenticação foi criado para dois fins, um fim empresarial para grandes empresas podendo ser operado por servidores *RADIUS*, que são servidores de autenticação composta pelo padrão IEEE 802.1x que trouxeram visíveis melhorias para a segurança no que diz respeito às integridades, autenticidade e privacidade. E por fim para pessoal o PSK (*Pré Shared Key*), ou seja, para usuários comuns, nesse método todo ponto de acesso receberia a mesma chave, em vista a comparação com as soluções empresariais deduzi-se que trata-se de uma solução bem menos escalável, onde a segurança depende muito da força e sigilo das chaves.

O WPA é compatível inclusive com o protocolo antecessor WEP como também é compatível com os mecanismo de criptografia TKIP e AES e também com padrão 802.1x que são geralmente usados por servidores de autenticação de dispositivos sem fio (*Radius*). Seu funcionamento é dado através de uma chave temporal (*Temporal Key Integrity Protocol – TKIP*) encriptando dados através do melhoramento na concatenação das chaves, verificando a integridade das mensagens com MIC (*Message Integrity Check*), efetuando melhoramentos nos vetores de inicialização – IV, possuindo também um eficiente mecanismo de atualização de chaves a cada sessão.

O WPA possui dois tipos de chaves que são do tipo *Paiwise KEy e Group Key*, a primeira é dada quando se tem uma comunicação direta entre o dispositivo cliente e seu ponto de acesso, tendo a grande necessidade de se ter conhecimento sobre as duas partes sobre a chave que esta sendo compartilhada, comunicações desse tipo ponto a ponto no mundo tecnológico é denominado de comunicações *Unicast.*

Quanto ao *Group Key* é basicamente ao contrário, consiste em uma comunicação com todos dispositivos da rede, como próprio nome já diz. Neste caso a chave que estará sendo compartilhada terá necessidade de ter conhecimento de todos os dispositivos da rede, tais comunicações é denominado do tipo *Multicast*, onde um dispositivo solicita conversa com um certo grupo da rede ou ao mesmo tempo com todos.

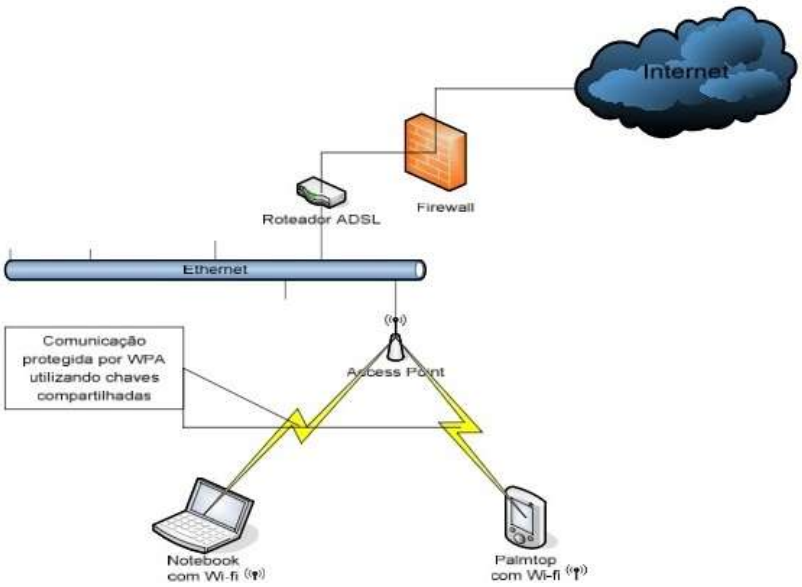


***Figura 7**, fonte:Artigo, Segurança em redes wireless, publicado por Roberto Rivelino da S. Vilela e Delmar da Silva Ribeiro em 05/06/2007.*

A figura 7 mostra uma comunicação sendo utilizada pelo protocolo WPA, utilizando o recurso de chave compartilhada, ou seja, dois dispositivos associados ao ponto de acesso, compartilhando da mesma chave de acesso.

Embora o estudo e evolução da segurança é visível e que o WPA comparando ao seu antecessor WEP traz algumas melhorias de segurança, em comparação simultânea aos dois protocolos temos um quadro comparativo dessas duas soluções.

Cifragem	WEP	WPA
	Com falhas, segurança quebrada por cientistas e hackers	Resolve todas as falhas do WEP
	Chaves de 64 e 128 bits estáticas, sendo 24 bits para o Vetor de Incialização	Chaves dinâmicas de 128 bits + combinação de sessão de logon.
	Distribuição de chaves manual	Distribuição de chaves automática.
Autenticação	Com falhas; Autentica somente o dispositivo	Autenticação baseada no usuário, com a utilização da arquitetura 802.1x/EAP

***Figura 8**, fonte:Artigo, Segurança em redes wireless, publicado por Roberto Rivelino da S. Vilela e Delmar da Silva Ribeiro em 05/06/2007.*

Mesmo com as maravilhosas correções de segurança trazidas no WPA, de acordo com o quadro acima, o órgão responsável pela criação não se dava por satisfeito. Sabendo ainda que ainda podia fazer melhoramentos no ultimo protocolo lançado, no ano seguinte em 2004 o órgão lançou o WPA2, numero (2) adicionado a nomenclatura referente a segunda versão do anterior. O principal desafio dos desenvolvedores era fazer protocolo mais próximo e compatível com as exigências de segurança, não ainda atendidas no protocolo anterior, por esse motivo lançou um protocolo provendo ainda mais de segurança de acesso e trafego de dados.

Wpa2

Protocolo lançado com principal objetivo de reforçar normas, especificações de segurança. E vem com uma diferença visível, enquanto seu antecessor trabalhava com o algoritimo RC4, o mesmo sistema de encriptação utilizado no WEP, garantindo a troca garantindo a troca periódica de chaves com TKIP, é inteiramente compatível com outro mecanismo de segurança o AES, que trata também de um sistema de encriptação porem mais seguro e pesado comparado TKIP. Basicamente a principal mudança de seu antecessor para o WPA2 foi toda a reformulação dos algoritimos de criptografia e integridade dos dados, o mecanismo de autenticação permanece o mesmo, varias mensagens trocadas em sua negociação com o AP e o cliente, causando um atraso no estabelecimento na autenticação e também uma notável interrupção quando cliente esta movimento deixando associação do primeiro AP para um segundo, principalmente quando se trafega dados de voz e vídeo. Para diminuir esse tempo os dispositivos dispõe de fábrica de um recurso chamado PMK, que basicamente guarda informações (cache) de autenticações na tentativa de diminuir o numero de mensagens trocadas e conseqüentemente o tempo de re-autenticação e consiste também em fazer associações a outros dispositivos próximos prevenindo assim com uma eventual mudança de AP pelo cliente, o mesmo não sofra perda de tempo com a autenticação.

Sua principal inovação foi o protocolo de refinamento criptográfico o **CCMP** (*Modo Contador e Encadeamento de Mensagens de Autenticação*). Uma solução quase completa, responsável pela encriptação, integridade e confidência dos dados do WPA2, muito usado pelo governo americano EUA, sua criação foi inspirada no mecanismo recém falado o AES, seu componente contador guarda informações privativas enquanto o encadeamento das mensagens fornecem dados de integridade e autenticação, o reforço de segurança para os dados em privado requer um poder de processamento adicional do hardware, necessitando assim seus administradores manterem sempre atualizados.

Mesmo com toda melhoria, principalmente citados de forma enfática a criptografia e integridade, o uso do WPA2 ainda é o mais recomendável, mesmo assim precisa de alguns ajustes nos quais refere-se a principal preocupação dos especialistas "segurança", onde já foram notadas e mostro-lhes abaixo algumas delas. Lembrando que as vulnerabilidades abaixo mostradas são válidas também para o WPA, partindo do ponto em que o surgimento do WPA2 foi com base em seu protocolo anterior (WPA).

Desvantagens

- Não compatível com dispositivos de padrões anteriores (Ex: 802.11a, 802.11b).
- Baixa abrangência de interoperabilidade.
- Utilizado no modo PSK(*Personal Shared Key*) possui vulnerabilidades, em suas chaves, sujeito a ataque do tipo dicionário (*Ataque Dicionário - Ação maliciosa com a tentativa de decifrar senhas de autenticação efetuando combinações de todas as letras e palavras composta em um dicionário com o objetivo de capturar senha*).
- Requer uma qualidade intermediária de hardware, devido ao seu considerável processamento.

Percebe-se que com seus mecanismos atrelados o AES e CCMP o WPA2 ganhou notoriedade no mercado e seu uso se tornou mais ainda popular, um protocolo sólido com seu nível de segurança destacada comparada aos demais, e que não trata de uma solução perfeita, podendo ainda com passar dos anos descubram-se mais vulnerabilidades, em contra partida melhores especialistas em segurança do mundo analisam seu funcionamento, e nos mostra a grande evolução de segurança que tivemos nos últimos 20 anos, nos mostrando cada vez mais confiabilidade que este meio de acesso vem nos passando.

REDES SEM FIO PARA AS CORPORAÇÕES

Para grandes corporações a rede sem fio já foi algo muito ponderado em fazer parte de suas estruturas, com a visível evolução deste método, inovações e eficientes mecanismos de segurança, item imprescindível e exigido pelas empresas, fizeram com que a visibilidade por elas tenha mudado. Na era da criptografia, segundo o escritor *Tanenbaum, em redes de*

computadores 2011, pag. 539 "Qualquer pessoa que instale o *PGP (Pretty Good Provacy – Programa de computador de encriptção e descriptografia de dados)* e utilize uma chave de segurança com nível elevado, pode ter certeza que ninguém conseguirá decifrar pacotes". Um dos principais motivos de uma empresa adotar as redes sem fio para a sua estrutura, conforme citado seria a segurança, com o surgimento dos últimos protocolos de autenticação como, por exemplo, o WPA2 no modo enterprise que dispõe de uma rígida segurança e a necessidade de um servidor de autenticação (RADIUS), para seu gerenciamento com base em políticas de regras, determinadas pelos administradores de rede. Com isso as corporações despertam interesses em sua implementação sem contar é claro com a mobilidade e o baixo custo.

Uma pesquisa feita pela empresa *E-Consulting*, realizado no segundo semestre de 2009 com executivos de grandes empresas no Brasil, disse: "*A necessidade de ferramentas de mobilidade é uma constante*". Um ponto muito considerado pelas empresas para a mobilidade são os investimentos, em conseqüência de sua evolução tecnológica as redes sem fio se tornaram mais seguras e economicamente gerenciáveis, nas empresas entrevistadas para a pesquisa na grande maioria adotam alguma solução de mobilidade sejam redes sem fio ou adoção de aplicativos móbile, 72% dessas empresas possuem aplicativos dessa natureza e as demais pretendem adotar nos próximos anos. Avaliando as áreas de negócio que mais demandam soluções de mobilidade identificamos:

- Áreas de Gestão e Administração (77% já utilizavam)
- Automação de Força de Vendas e Equipe de Campo (74%)
- Trade (28%)
- Automação Industrial e de Produção (22%)
- Supply Chain RFID (8%)

A tendência é que tais percentuais avancem a cada ano e que novas áreas, atividades e processos corporativos adotem soluções de mobilidade.

Fonte: E-Consulting em http://www.e-consultingcorp.com.br/mobilidade-corporativa-realidade-presente 27 de dezembro de 2012.

É notória a expansão em que os dispositivos móveis abrange e enquadra suas variadas estratégias de marketing e disponibilidades de serviço que as empresas disponibilizam através das redes sem fio. Por uso de tabletes conectados a rede vários restaurantes do Brasil já aboliram o cardápio físico (Em papel) e passaram a disponibilizar aos seus cliente cardápios virtuais, onde os cliente ao sentarem a mesa anteriormente agendada por aplicativos instalados em seus smartphones que dispõe desse serviço podendo assim efetuar reservas de mesas no restaurante escolhido. O cliente ao sentar-se à mesa que já foi agendada tem um disponível tablet em sua mesa com a opção de consultar o cardápio do restaurante, selecionando o prato escolhido para a refeição, dando mais praticidade e controle de gerenciamento a empresa, sem contar no fato ecológico, o modelo de acesso ao menu dispensaria folha de papel. Com mesmo método estendem-se também outras empresas de diferentes seguimentos, como por exemplo, grandes lojas de roupas substituíram seus catálogos de coleções (Em papel) por tabletes em suas lojas, o cliente ao chegar à loja, no balcão tem disponível um tablet onde o mesmo possa acessar o aplicativo da própria loja e verificar toda coleção e estoque de roupas que compõe a rede da loja, além de contribuir com meio ambiente torna-se ao cliente um grande atrativo e assim o ajuda-o na escolha de uma compra.

Figura 9, fonte: https://www.google.com.br

Figura 10, fonte: https://www.google.com.br

Segundo o **portal G1** "*As empresas estão cada vez mais adotando a comunicação móvel para automatizar processos e conectar colaboradores, aumentando a produtividade e a velocidade para a tomada de decisões. A mobilidade esta sendo usadas em seus negócios movidas pela computação em nuvem e pelo conceito de virtualização, que possibilita aos funcionários acessarem aplicativos corporativos sem precisarem esta no escritório*". constata o professor de cursos de pós-graduação e graduação do Instituto Nacional de Telecomunicações (Inatel), Afonso Celso Soares. Segundo ele, as organizações conectadas alcançam clientes mais rapidamente e podem praticar a inovação de forma mais intensa, para serem mais competitivas.

Fonte:http://g1.globo.com/economia/especial-publicitario/embratel/pense-inovacao/noticia/2015/01/mobilidade-corporativa-conecta-negocios-com-inovacao.html Em: 08/01/2015.

Aos méritos de crescimento destinados a redes sem fio, também esta ligada as grandes operadoras também evoluírem simultaneamente com o objetivo de dar condições a grande demanda de dispositivos moveis comercializados no país e no mundo, grandes tecnologias se aliaram a isso como conexões 3G, seguidas de 4G e o seu mais novo sucessor o 5G que poderá atingir velocidades de 20 Gbps(Giga bits por segundo), permitindo as corporações desfrutarem de grandes recursos que a mobilidade pode trazer.

De fato é um mercado assustador em vendas de dispositivos móveis, ainda segundo o **portal G1** citada pelo instituto de pesquisa IDC, estimaram que certa de 52 milhões de smartphones foram vendidos no Brasil no ano de 2015. Hoje mais de 70% das empresas com mais de cem funcionários já utilizam smartphones e celulares corporativos. Destas, 41% contratam também plano de dados, segundo a pesquisa "Conectividade das Empresas do Brasil", realizada pelo Teleco e pela Embratel com 400 companhias. Outro termômetro do avanço da mobilidade no Brasil é o crescimento da base de usuários de celulares. Dados da Agência Nacional de Telecomunicações (Anatel) revelam que o país tinha em outubro 279,3 milhões de linhas móveis em serviço.

Fonte: http://g1.globo.com/economia/especial-publicitario/embratel/pense-inovacao/noticia/2015/01/mobilidade-corporativa-conecta-negocios-com-inovacao.html Em: 08/01/2015.

Visando esse infinito e promissor mercado, grandes empresas não só apóiam como investem para o continuo crescimento e sua maior abrangência de funcionalidades que esse método pode nos proporcionar não só a nós usuários finais como também as próprias operadoras de telefonia que dispõe de estruturas e funcionalidades para este meio de comunicação, barateiam seus serviços de dados em vista as estáticas de vendas de dispositivos móvel, com intuito atrativo de conquistar maior números de clientes possível e conseqüentemente o aumento de seus lucros, lançado para o mercado consumista grandes inovações tecnológicas e com variados recursos, apresentando baixo custo para adquiri-lo, não somente como uma forma de atração ao cliente, mais devido também a alta concorrência de mercado, onde um bom marketing, preços, custos, benefícios e qualidade de serviços são fatores indispensáveis para a conquista de um novo cliente.

A empresa Facebook, dirigida pelo seu fundador *Mark Zuckerberg*, possui um projeto desafiador chamado de *Mobile World Congress (MWC)* que consiste em conectar todas as pessoas do mundo, ou seja, o projeto apóia a mobilidade no mundo incentivando a alta conectividade móvel, e a grandes empresas apresentarem suas inovações ao que se refere à mobilidade, como novos dispositivos e seus novos recursos, uma excelente oportunidade para empresas de telefonia móvel.

Nesse evento a empresa facebook divulgou a Telecom Infra Project, uma parceria com operadoras e fabricantes de equipamentos de telecomunicações para colaborar na criação de novas tecnologias para melhorar acesso e transmissão de conexão de internet de alta velocidade sem fio. Entre os membros do projeto, estão a Intel, a Nokia e as operadoras Deutsche Telekom e SK Telecom. Cada uma das empresas têm suas próprias razões para participar do projeto – as operadoras buscam equipamentos mais baratos, enquanto as fabricantes miram em incrementar suas vendas. Já o Facebook – através de sua organização Internet.org – quer levar a internet para todos os 7 bilhões de pessoas no mundo.

Fonte: http://blogs.estadao.com.br/link/facebook-cria-parceria-com-operadoras-para-melhorar-redes-sem-fio, em 22/02/2016, publicado por Bruno Capelas.

Conforme dito no parágrafo acima, cada qual com seu interesse próprio, de lucro e visibilidade, mais o projeto é um tanto desafiador, mais possível, resumi-se em abrangência mundial de usuários conectados e baixos custos cobrados pelas operadoras. Um projeto audacioso, com objetivo de integrar acesso a grande rede (internet) para a população mundial. Ponto importante para percebermos a evolução das tecnologias sem fio e o que ele esta nos proporcionando, e a qual caminho esta percorrendo. Ainda segundo o próprio Mark "*Acreditamos que o mundo deve ter acesso a internet*," com esse projeto os meios de comunicação tenderão a serem mais rápidos e com baixos custos, com isso milhões de pessoas poderão beneficiar-se de planos de dados e conseqüentemente possuírem internet em seus dispositivos.

Uma gigante da tecnologia mundial a empresa ***Google Inc***. responsáveis pelos maiores projetos tecnológicos da historia, esta com um grande projeto de mobilidade de acesso para as cidades, o projeto esta sendo implementado inicialmente em Nova York, a empresa instalará roteadores sem fio em vários pontos da cidade de forma estratégica com um intuito também

de aproveitar a infraestrutura pública já existente para disponibilizar hubs. Para isso a Google, entrará em parceria com a empresa LyncNyc, inventora do equipamento "*Totens*" que consiste em um dispositivo que transmite imagens publicitárias, alem disso a Google em parceria com a LyncNyc, quer disponibilizar tomadas ou portas USB para estes dispositivos para recargas dos celular dos habitantes de cada cidade onde o projeto será implementado, transmitir nos visores dos equipamentos informações sobre a cidade e possibilitar para seus usuários chamadas locais gratuitas.

O único impasse das empresas é por que mesmo sendo serviços gratuitos gerará receitas. Só em nova York as empresas querem colocar 10 mil hubs na cidade, a pretensão é que seja levado o projeto para outros pontos do país, incluindo áreas rurais, o projeto diminuirá o numero de pessoas que não tem acesso a internet, que são de 55 milhões, segundo o FCC um órgão com atividades semelhantes a do nosso país, o projeto tem pretensões de não só ficar nos Estados Unidos como também ir para outros países.

Fonte: https://tecnoblog.net/180369/google-sidewalk-wifi/ publicado por Emerson Alecrim em julho de 2015.

Outra gigante tecnológica mundial o grupo ***Samsung,*** a empresa coreana investe pesado a cada ano em conexões sem fio, o padrão wifi 802.11ad permite atingir velocidades surpreendentes de até 4,6 Gbps, equivalente a 575 MB por segundo, com essa taxa de velocidade arquivos com seu tamanho de 1GB podem ser baixados em menos de três segundos. O padrão atual 802.11ac atinge velocidades de 866,7 Mbps, equivalente a 108MB por segundo, a Samsung com muito investimento e estudos, diz que wifi pode chegar a velocidades muito maiores, sabendo-se que os principais problemas das redes sem fio são as interferências a Samsung desenvolveu uma poderoso transmissor e um novo designer para a antena, onde a empresa agora desenvolvi equipamentos compatíveis para tais velocidades.

Essas grandes taxas de transferência dar-se ao surgimento futuro de um novo padrão wifi o 802.11ad, conhecida como a tecnologia *Wigig*, este novo protocolo a ser lançado para as redes sem fio não é exclusivo da Samsung varias outras empresas também investem nesse novo método de conexão wifi, tais como a poderosa Apple, Intel, Microsoft e a Qualcomm.

Fonte: http://gizmodo.uol.com.br/samsung-wifi-80211ad/ publicado por Jamie Condlife, em outubro de 2014.

Alem da segurança as grandes corporações temem com as instabilidades e interferências das redes sem fio, com o futuro padrão das redes sem fio comentado nos parágrafos anteriores, a comunicação estará dando um grande passo para resolver mais problemas temidos pelas empresas, o novo padrão trará grandes velocidades e instabilidades em conexões, resolvendo também em muito os problemas causados por interferências de obstáculos (paredes etc.), esta claro que as conexões sem fio encaminha-se cada vez para requeridas e desejadas pelas empresas, claro que para isso também terá de ser feito dispositivos compatíveis com o novo padrão, não deixando os antigos absoletos, mas tendo uma mudança gradativa em relação ao novo método que tudo indica pelas suas características e recursos, que veio para ficar, possibilitando assim grandes projetos de mobilidade corporativa serem criados.

ASPECTOS PROMISSORES

É visível a evolução tecnológica no mundo, e com ela numa crescente simultânea as tecnologias wifi, a cada ano as conexões sem fio com suas evoluções vem nos proporcionando patamares nunca imagináveis e aceitos pelos críticos em segurança e especialistas em conexões instáveis. As formas como as pessoas se relacionam como trabalham a produtividade o rápido acesso a informação, tudo isso se deve as conexões sem fio, sem contar com as gerações de novos negócios pelas empresas disponibilizando novos e rápidos serviços aos seus clientes, sem dúvida nenhuma, esta solução veio para ficar, se comparando aos anos anteriores a evolução é absurda e de fato aceita por grandes empresas no mundo.

Os dispositivos moveis vem ganhando importância nos meios de trabalho, é definida como uma eficiente ferramenta de trabalho incorporando recursos que alguns anos atrás não imaginávamos. Ainda pouco utilizado e falado sobre o padrão que nem durou muito tempo o 802.11ac em sua utilização no mundo, já estamos em um padrão novo, "recém nascido" o padrão 802.11ad a nomeada de conexão *Wigig*, que esta com proposta de transmissões de cinco vezes mais rápida que sua antecessor 802.11ac, com a nova tecnologia é possível transmitir 7GB de dados por segundo, com freqüências de 2.4 Ghz e 5Ghz, as altas taxas de velocidade dar-se a um bom desempenho do sistema de modulação projetado com base em sistemas ponto a ponto onde permite transmitir por múltiplos dispositivos de forma simultânea sem terem interferências entre si. Muitos especialistas acham que o padrão recém lançado não veio a substituir completamente seu antecessor, que esse padrão ainda apresenta dificuldades de penetra o sinal através das barreiras do ambiente, a tecnologia ainda apresenta grandes dificuldades de propagação de sinal quando tem obstáculos em seu caminho e que devido a muitos dizem que esta solução só funciona bem em fechados, onde a quantidade de paredes e obstáculos seja menor. Em nota o diretor da Samsung Kim Chang Yong disse: "*A empresa superou com sucesso essas barreiras para a comercialização da tecnologia de banda com ondas 60GHz*" essa informação foi dada segunda a mesma, com base no que a empresa alega ter criado antenas de alta cobertura, possuindo tecnologia "*beam-forming*" que consiste em detectar os dispositivos que necessitam de um sinal, enviando assim aos mesmos um sinal focado, direcionado para os aparelhos, diferentemente das tecnologias antigas que enviavam sinais de forma aleatória e em todas as direções, com o *beam-forming* todo sinal propagado recebera um sinal em contra partida, fechando uma comunicação ponto a ponto, conforme a figura 11 abaixo.

Figura 11, fonte: https://www.google.com.br/search?q=sinal+beam-forming&biw=1366&bih=612&source=lnms&tbm=isch&sa=X&ved=0ahUKEwivlY7qm_TLAhWIEpAKHW2ZCcAQ_AUIBigB#imgrc=tZQFH6wiVqxLBM%3A

Mal conseguimos aproveitar os recursos do padrão 802.11ad, o mundo das tecnologias nos trás mais uma evolução para as redes sem fio. Mais um protocolo para as comunicações, que esta prevista para ser lançada em 2019, trata-se do "futuro" do novo **padrão 802.11ax**.

O futuro padrão terá como atrativo fornecer uma conexão com velocidade superior 4 vezes mais que o padrão 802.11ac considerado por muitos o mais difundido da atualidade, essa tecnologia atingirá picos de 10GB em bandas de freqüência de 5Ghjz. A empresa mais por dento desse futuro meio de acesso é a *HUAWEI* , a empresa coreana diz que a nova tecnologia contará com spectros inteligentes, resumem-se em freqüências que são geradas a partir de ondas magnéticas, e também contará com uma grande coordenação de interfaces super competentes, o padrão não mostrará tanta diferenças assim para o usuário final com exceção da sua grande velocidade. A novidade em questão de velocidade será como uma luva para empresas que utilizam Voip (Voz sobre IP) e tecnologias semelhantes, empresas que trabalham como edição de vídeos onde requerem uma quantidade de streaming elevado terá maiores benefícios, vídeos com resolução máxima serão facilmente transmitidos e Assistidos em tempo real.

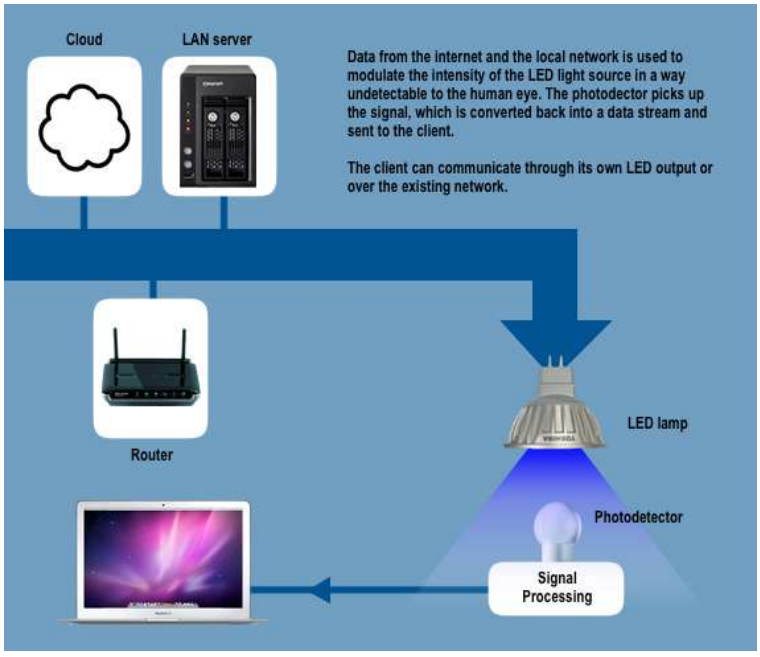
A expectativa é de que no fim de 2018 começando 2019 já possamos encontrar equipamentos com essa novidade no comércio, daqui pra lá ficaremos na torcida para que as operadoras de telefonia também evoluam de forma simultânea com tamanha velocidade, independente do critério que o padrão utilizará para conseguir altas taxas de transmissão, isso não se sabe, mais uma coisa é certa, em comparação direta com o padrão anterior, é visivelmente superior em matéria de eficiência.

Os estudos tecnológicos não param de crescer, em um futuro ainda mais distante e promissor a forma de conexões sem fio irá mudar radicalmente, estudiosos e especialistas prometem conexões 100 vezes mais rápidas que as atuais, isso dar-se a maneira como o meio de acesso irá se definir, estamos falando da ainda distante mais real conexões ***Li-FI (Light Fidelity – Fidelidade da luz*),** tecnologia que passará a usar ondas de luzes para transmissão empregando diodos emissores de luz o popularmente conhecido LED.

Apesar de trabalha de forma semelhante a Wifi da atualidade, a Li-fi utilizará métodos de modulação semelhantes aos raios infra vermelhos, as lâmpadas de LED terão o papel de semicondutores e a saída óptica poderão ser moduladas em velocidades capazes de serem detectados em dispositivos fotodetectores e convertidas de volta para a corrente elétrica, convencionalmente usadas em residências.

Essa nova tecnológica trará uma segurança mas elevada do que a wifi, e não possuirá interferências com outros sistemas, onde poderiam serem usados a bordo de um avião, sem causar nenhum dano aos sistema que estarão sendo pelo piloto no ato de um vôo. A novidade permitirá que as lâmpadas tenham não somente a função de garantir a conectividade mais tenha a função de iluminar, em teste de laboratórios a Li-fi atingiram estrondosamente velocidades de até 22GB por segundo, em outros testes feitos em uma única lâmpada e LED, consegui-se manter conexão com a internet para quatro computadores com velocidades alcançadas de 150 Mbps para cada um dele. Imaginamos se uma única lâmpada consegue tais façanhas, imagina só um grupo de lâmpadas e seus impactos de velocidade causariam.

Com essa tecnologia no mercado, é bem previsto que futuros dispositivos venham de fabrica com detectores de fotossínteses estabelecendo por exemplo conexão com um poste de luz em vi publica, que por sinal tem tecnologia Li-fi disponibilizando assim conexões com os aparelhos e dando-nos velocidades surpreendentes de acesso e download.



Método de funcionamento Li-Fi, ***Figura 12****, fonte*:
https://www.google.com.br/search?q=lifi&biw=1366&bih=612&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjc5ND42PbLAhVIFpAKHZC1B6UQ_AUICCgD#imgrc=WdSSFk6HbTzpeM%3A

O seu funcionamento resume-se em dois estados: Lâmpada acessa e apagada, a transmissão será feita de forma rápida e imperceptível ligando ou desligando a luz, a mesma será

registrada por um foto sensor, que será responsável por identificar o estado da luz (Acesa e apagada) caso a mesma esteja acesa ela terá a inteira função de transformar a luz em informações e transmitir para seu dispositivo nele associado.

Entretanto, a tecnologia pelo fato de usar lâmpadas, as mesmas não conseguirão ultrapassar paredes o que limitará seu uso em alguns ambientes fechados, em compensação, como a transmissão de dados será feita pela luz, à amplitude de lugares que isso pode abrangi é inimaginável. Muitos testes estão sendo feitos para melhoria desta inovação, a principio os valores das lâmpadas não serão baratas, mas com o crescimento de utilitários deva mudar isso, e seu valor pode passar a ser mais acessível para as pessoas.

CONSIDERAÇÕES FINAIS

O propósito das redes sem fio é de fato dar aos seus usuários mobilidade, segurança e principalmente velocidade ao acesso as informações, em vista ao inicio das redes comparando ao que ela representa e é hoje a evolução é constante. As conexões sem fio revolucionaram a telefonia no mundo e causando um impacto profundo nas redes de computadores.

Percebemos que toda tecnologia independente de seu tempo de criação ou uso, irão ter vulnerabilidades, o termo usado em segurança da informação é: “Não há segurança 100%”, concordo plenamente com a frase, mais devemos reconhecer todo esforço, tempo e dedicação dos especialista e estudiosos por a cada ano disponibilizarem inovações de segurança para este tipo de acesso, lançando assim de forma seqüenciada novidades e mais novidades no que desrespeito a segurança dos dados, Protocolos de autenticação, criptografia de dados, mecanismos de gerenciamento e segurança todas as inovações citadas aqui tem o objetivo de desmitificar o ditado popular “Redes sem fio, não é segura”, posso garantir é sim segura, desde que seja muito bem executada e configurada.

Concluo que para este trabalho a evolução é visivelmente perceptível, a tecnologia com toda outra ainda possui suas desvantagens mais que o numero de vantagens e ainda maior, cito algumas delas:

- Crescimento progressivo
- Flexibilidade de instalação
- Redução de custos
- Flexibilidade no ambiente de trabalho
- Configuração rápida e simples da rede
- Maiores velocidades de conexões a cada dia
- Agilidade em todas de decisões
- Baixo custo de Implementação

As vantagens são inúmeras, seus pontos fracos antigamente muito questionados pelas grandes corporações, como segurança e velocidade, problemas nos quais eram relevantes hoje em dia já não são tanto assim, a segurança e a velocidade cresceram e ainda crescem de forma simultânea, por exemplo, referindo-se a velocidade o padrão 802.11ax trás picos de velocidade de 10GB, quanto as projeções futuras para conexões sem fio através de lâmpadas LED´s a Li-Fi, trará velocidades extraordinários, os desenvolvedores garantindo 100 vezes mais rapidez comparando as atuais, podendo chegar a picos de 20GB por segundos. Quanto à segurança de dados vimos também o quanto à evolução de autenticação teve seus caminhos morfológicos para nos dar mais segurança, que podemos ter um servidor Radius para gerenciar todas autenticações e junto com ele usarmos o protocolo WPA2 enterprise, no qual ambos juntos funcionam muito bem, partindo do principio em que diz Tenenbaum: "***Qualquer um que utilize uma chave de segurança com nível elevado, pode ter certeza que ninguém conseguirá decifrar pacotes***" e de fato isso é verdade, dados criptografados requerem muito tempo para serem descobertos (interceptados), e como os protocolos de autenticação hoje utilizam recursos de renovação de conexão, ou seja, para cada conexão estabelecida ao ponto de acesso, há um tempo para essa conexão, após esse tempo o Acess Point – AP, irá fazer toda renegociação com dispositivo na tentativa de renovar a sua chave de acesso, tempo bem menor comparado a que um cracker precisaria utilizar para interceptar pacotes, ou usar técnicas para decifrar as chaves de acesso compartilhadas, praticamente pelo tempo seria inviável esse método de invasão.

Acredito que o propósito das redes sem fio como muitos dizem não é substituir as redes cabeadas, com todo esse estudo posso dizer que as redes cabeadas são ainda as mais requisitadas e que as redes wifi o que antes era motivo de muita preocupação como segurança e velocidade, hoje já não são mais o maior desafio dessas redes ainda são os obstáculos físicos Paredes, montanhas, interferências essas no momento são as maiores preocupações dos analistas, que mesmo com toda sofisticação e rapidez que a tecnologia futura trará a Li-Fi, virá com limitações quando deparados com obstáculos. Portanto devemos respeitar o crescimento dessas redes, aproveitar seus variados recursos que elas nos traz.

A amplitude de dispositivos e o meio de acesso é uma realidade e nos proporciona recursos muito interessantes, que podemos sim investir nessa tecnologia acreditar bastante que só temos a ganhar com isso, viabilizar esse meio de acesso cobrindo, padronizando grande parte do mundo com as conexões sem fio, nós daria muito mais interatividade, produtividade e principalmente acesso aos dados com muito mais rapidez, pontos fundamentais onde a concorrência no mundo é muito grande.

REFERÊNCIAS

- **Livro:** Hacker Friendly LLC, Redes sem fio no Mundo em Desenvolvimento, 2008, *http://hackerfriendly.com*
- **Livro:** KUROSE|ROSS., Redes de computadores e a internet, uma abordagem top-down 3°, 5° e 6° Edição.
- **Livro:** Adam Engst e Fleishman, Redes Sem fio, guia prático para Windows e MAcintosh / 2° edição,
- **Livro:** Theodore S. Rappaport. Comunicações sem fio, princípios e praticas / 2° edição.
- **Livro:** Tenenbaum | Wetherall, Redes de computadores / 5° edição.

- **Artigo:** Estudo do Crescimento das Redes Wireless802.11 – 2.4 GHz em Ambiente Urbano –Caso Rio Claro-SP.
- **Artigo:** A tecnologia WiFi 802.11ac consegue oferecer velocidade gigabit para as empresas?
- **Artigo:** A Tecnologia do Futuro Wi-Fi (*Wireless Fidelity*).
- **Artigo:** Estudo comparativo entre redes sem fio e redes cabeadas.
- **Artigo:**Implementação de uma rede sem fio: Estudo de caso na plataforma Windows.
- **Artigo:** Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w.
- **Artigo:** O novo padrão 802.11ac e as redes corporativas.
- **Artigo:** Evolução da Segurança em Redes Sem Fio.

- **Link:** http://www.tecmundo.com.br/wi-fi/23964-wi-fi-802-11ac-as-redes-sem-fio-de-alta-velocidade-vem-ai.htm
- **Link:** http://www.profissionaisti.com.br/2014/09/um-pouco-sobre-redes-sem-fio-wireless/
- **Link:** http://liktecnologia.com.br/index.php/estudo-da-cisco-preve-aumento-de-quase-10-vezes-no-trafego-global-de-dados-moveis-nos-proximos-cinco-anos/
- **Link:** http://www.telesintese.com.br/em-cinco-anos-maior-parte-dos-dados-vai-transitar-por-wifi/
- **Link:** http://www.tecmundo.com.br/internet/58366-wifi-802-11-ax-nova-geracao-conexoes-fio.htm
- **Link:** http://ghztecnologia.blogspot.com.br/2010/12/como-surgio-tecnologia-wireless.html
- **Link:** http://www.infowester.com/wifi.php
- **Link:** http://www.teleco.com.br/tutoriais/tutorialredeswlanII/pagina_2.asp
- **Link:** **http:**//www.gta.ufrj.br/grad/01_2/802-mac/
- **Link:** **http**://www.cisco.com/c/dam/r/pt/br/internet-of-everything-ioe/assets/pdfs/c45_729588_01_802_11ac_customer_use_cases_aag_v1a_ptbr.pdf
- **Link:** http://www.techtudo.com.br/artigos/noticia/2012/02/entenda-wep-e-wpa-protocolos-de-seguranca-de-rede-wi-fi.html

- **Link:** http://www.gta.ufrj.br/grad/08_1/ieee802-11/wep.html
- **Link:** http://docplayer.com.br/655356-Seguranga-em-redes-wireless-estudo-comparativo-entre-os-protocolos-wep-e-wpa-para-implementacao-de-seguranca-em-empresas-e-residencias.html
- **Link:** http://pt.slideshare.net/lauraaguiarmeneses/tcc-mobilidade-corporativa-e-o-estudo-de-casos-mltiplos-de-seus-servios-em-travel-management-companies
- **Link:** http://www.ebah.com.br/content/ABAAAgU8kAE/redes-sem-fio-grandes-empresas
- **Link:** http://gizmodo.uol.com.br/qualcomm-wilocity/
- **Link:** http://escreveassim.com.br/2011/07/13/wigig-wifi-7-gbps/
- **Link:**http://www.bbc.com/portuguese/noticias/2015/11/151126_tecnologia_internet_lifi_hb
- **Link**:http://www.techtudo.com.br/noticias/noticia/2014/09/entenda-o-que-e-li-fi-internet-luz-que-pode-substituir-o-wi-fi.html
- **Link:** https://tecnoblog.net/102223/li-fi-conexao-lampadas