FACULDADE PATOS DE MINAS
CURSO DE ENGENHARIA ELÉTRICA

IVAN ROSA DO AMARAL

REDES SEM FIO
PADRÃO IEEE802.11AC

PATOS DE MINAS
2017

IVAN ROSA DO AMARAL

REDES SEM FIO
PADRÃO IEEE802.11AC

Trabalho de Conclusão de Curso apresentado à Faculdade Patos de Minas como requisito para obtenção do grau de Bacharel em Engenharia Elétrica.

Orientador: Prof.º Me. Rafael Augusto da Silva.

PATOS DE MINAS
2017

Candidato:
IVAN ROSA DO AMARAL

Título: REDES SEM FIO PADRÃO IEEE802.11AC

Trabalho de Conclusão de Curso apresentado à Faculdade Patos de Minas como requisito para obtenção do grau de Bacharel em Engenharia Elétrica – FACULDADE PATOS DE MINAS

Data: 08 de Novembro de 2017

_____
Prof.º.
Orientador

_____

Prof.º.
Examinador

_____

Prof.º.
Examinador

Aprovado ( ) Reprovado ( )

AGRADECIMENTOS

Agradeço a Deus pela vida, pela saúde e sabedoria que permitiram a minha caminhada até aqui, aos meus pais pelo incentivo e apoio, a minha esposa e filhos que abriram mão de vários momentos em minha companhia colaborando para meus estudos. Agradeço também aos professores que contribuíram com sua dedicação e empenho nos ensinamentos, ao coordenador do curso Professor Me. Guilherme Fernandes por procurar sempre as melhores soluções para os problemas, que foram vários durante o curso e ao meu orientador Professor Me. Rafael Augusto da Silva pela prontidão em aceitar a minha orientação, pela ajuda e esclarecimentos, e a todos que de alguma forma contribuíram para a realização desse trabalho.

AMARAL, Ivan Rosa do. **REDES SEM FIO PADRÃO IEEE802.11AC.** 2017. 67 f. TCC (Graduação) - Curso de Engenharia Elétrica, Engenharia, FPM - Faculdade Patos de Minas, Patos de Minas, 2017.

Ivan Rosa do Amaral[1]

Rafael Augusto da Silva[2]

RESUMO

Este trabalho tem por finalidade a comparação entre o novo padrão IEEE 802.11ac com as normas anteriores e às redes cabeadas, também conhecido como VHT (*Very High Throughput*), aprovado em dezembro de 2013. Muitas características das versões anteriores, sobretudo IEEE 802.11n, se mantiveram na nova versão, mas os principais ganhos em camada física possibilitam transmissões com alta taxa de dados, alcançando quase 7 Gbps em sua máxima capacidade de operação (largura de banda de 160 MHz, modulação 256-QAM com taxa de código 5=6, oito fluxos espaciais e intervalo de guarda curto entre símbolos OFDM). Para demostrar na prática a comparação entre as tecnologias foi elaborado um projeto de modernização da rede sem fio atual da Faculdade Patos de Minas (FPM) Campus JK. Com a implementação desse projeto, os usuários que utilizam aparelhos que suportam o 802.11n irão notar uma enorme melhora na velocidade da conexão, e os problemas de acessos simultâneos serão resolvidos com a utilização de pontos de acesso e rede *mesh.* Já os usuários com aparelhos que possuem o 802.11ac ficarão ainda mais satisfeitos, devido ao fato que a velocidade da conexão com o ponto de acesso utilizado ser mais que o dobro à do 802.11n.

Palavras-chave: IEEE 802.11ac. *Throughput*. Pontos de Acesso.

[1] Graduando Engenharia Elétrica- FPM, 2017. ivanramaral@hotmail.com

[2] Prof. Me. Rafael Augusto da Silva

ABSTRACT

This work aims to compare the new standard IEEE 802.11ac with the previous standards and the wired networks, also known as VHT (Very High Throughput), approved in December 2013. Many of the features of previous versions, especially IEEE 802.11n, but the main gains in physical layer enable high data rate transmissions, reaching almost 7 Gbps at maximum operating capacity (160 MHz bandwidth, 256-QAM modulation with code rate 5 = 6, eight spatial flows and short guard interval between OFDM symbols). In order to demonstrate in practice, the comparison between technologies, a project was developed to modernize the current wireless network of Faculdade Patos de Minas campus of Av JK. With the implementation of this project, users using devices that support 802.11n will notice a huge improvement in the speed of the connection, and the problems of simultaneous access will be solved with the use of access points and mesh network. Users with devices with 802.11ac were even more satisfied, because the speed of the connection to the access point used was more than double that of 802.11n.

Keywords: *IEEE 802.11ac. Throughput. Access Points.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES E SIGLAS

IEEE - Institute of Electrical and Electronics Engineers

AP - Acess Point

BSS - Basic Service Set

CAA - Clear Channel Assessment

DBPSK - Differential Binary Phase Shift Keying

DCI - Digital Cinema Initiatives

DQPSK - Differential Quadrature Phase Shift Keying

DS - Distribuition System

DSSS - Direct Sequence Spread Spectrum

ESS - Extended Service Set

FHSS - Frequency Hopping Spread Spectrum

GFSK - Gaussian Frequency Shift Keying

HEVC - High Efficiency Video Coding

MAC - Media Access Control

MOS - Mean Option Score

MSE - Mean Square Error

PSNR - Peak Signal to Noise Ratio

QoE - Qualidade de Experiencia

QoS - Qualidade de Serviço

SMPTE - Society of Motion Picture and Television Engineers

IP - Internet Protocol

TCP - Transmission Control Protocol

UHD - Ultra High Definition

UHD - Ultra High Definition

WLAN - Wireless Local Area Network

DSSS - Direct Sequence Spread Spectrum

FHSS - Frequency Hopping Spread Spectrum

IBSS - Independent Basic Service Set

MAC - Medium Access Control

MIMO – Multiple Input Multiple Output

MU-MIMO – Multiuser MIMO

MPDU - MAC Protocol Data Unit

MDSU - MAC Service Data Unit

A-MPDU - Aggregated MAC Protocol Data Unit

A-MSDU - Aggregate MAC Service Data Unit

OFDM - Orthogonal Frequency Division Multiplexing

PHY - Physical Layer

PLCP - Physical Layer Convergence Protocol

PMD - Physical Medium Dependent

SAP - Service Access Point

STA - Station

Wi-Fi - Wireless Fidelity

WLAN - Wireless Local Area Networks

CRC –Cicle Redundance Check.

CSMA/CA –Carrier Sense Multiple Access Cillision Avoidance.

CTS –Clear toc Send.

DES–Data encryption Standard.

DFWMAC –Distributed Foundation Wireless Media Access Control.

DHCP –Dynamic Host Configuration Protocol.

DoS –Denial of Service.

EAP –Extensible Authentication Protocol.

TSL–Transport Layer Security.

ESS –Extend Service Set.

GHz –Gigahertz.

IBSS –Independent Basic Service Set.

ICMP –Internet Control Message Protocol.

SUMÁRIO

1 INTRODUÇÃO

O IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) surgiu nos Estados Unidos em 1963 a partir da junção do IRE (Instituto de Engenheiros de Rádio) e do AIEE (Instituto Americano de Engenheiros Elétricos), atualmente é considerada a organização profissional com maior número de sócios no mundo, sedo uma instituição profissional sem fins lucrativos, com objetivo de gerar conhecimento na área da engenharia elétrica, eletrônica e computação (1).

No que diz respeito ao padrão de redes sem fio o IEEE iniciou seu desenvolvimento no ano de 1997, quando foi desenvolvido o padrão IEEE802.11 "*legacy*", que determinou os protocolos a serem usados para transmissão de dados, no início as conexões trafegavam com taxas de transmissão entre 1 e 2 Mbps e frequências entre 2,4 GHz e 2,4835 GHz. Com utilização de técnicas desenvolvidas a taxa de transmissão de dados era um pouco menor porem diminuía as interferências e a perda de pacote, além de transmitir múltiplos canais. Em 1999, a *Wireless Ethernet Compatibility Aliance* (WECA) passou a comandar o setor e hoje recebeu o nome Wi-Fi Alliance, o padrão inicial foi mudado em quase toda sua totalidade e houve um aumento na sua área de cobertura, e serviu como base para uma das tecnologias mais importantes da atualidade (2).

O protocolo 802.11 é um sistema de transmissão de dados via rádio, entre equipamentos eletrônicos em uma área com um raio de algumas dezenas de metros (3).

Esse protocolo foi planejado inicialmente como uma rede LAN (Local Área Network) sem fio em contrapartida à rede cabeada oferecendo taxa de transferência perto de 50Mbp/s com uma ótima segurança, ele foi e continua sendo uma alternativa em substituição ás redes cabeadas e com baixo custo, porem houve uma enorme evolução durante os últimos 20 anos e com o protocolo 802.11 não foi diferente (3).

As famílias do protocolo 802.11 têm vários pontos em comum como descrito a abaixo:

Permite criação de LAN sem fio a baixo custo em residências e pequenos escritórios;

Usa uma tecnologia miniaturizada que é quase imperceptível para o usuário;

Sua configuração não necessita de especialistas podendo ser facilmente realizada pelo usuário;

Quase não requer manutenção;

Possui um bom nível de segurança para utilização em residências e escritórios de pequeno porte, porém ainda com algumas vulnerabilidades;

É aceito em vários tipos de equipamentos e sistemas operacionais (3).

O IEEE802.11ac é um padrão que proporciona alta taxa de transmissão de dados em no mínimo 500 Mbp/s podendo chegar a vários Gbp/s, de acordo com o dispositivo na banda de 5 GHz (3).

Essa norma oferece velocidades muito maiores em relação à norma anterior. Resultados alcançados a partir de um canal de rádio mais amplo com até 8 fluxos espaciais MIMO (do inglês*: multiple-input multiple-output*), e uma sofisticada modulação (256 QAM), que na realidade proporcionam um throughput (taxa de transferência) de até dez vezes mais que a 801.11n, baseando-se em tecnologias bem simples que realmente funcionam. Porem a modulação em 256 QAM necessita de um ambiente de rádio que normalmente será pouco encontrado na prática (3).

A finalidade do IEEE 802.11ac contempla:

Alcance mínimo na taxa de transferência de 500 Mbp/s, apenas com modulação maior e mais competente para canais de rádio;

Aumento dos canais para 80 MHz até 160 MHz, em contra partida dos 40 MHz máxima largura para o 802.11n;

Sendo obrigatório suporte à canais com largura de banda de 80 MHz e para canais de 160 MHz fica facultativo, devido dificuldade de conseguir dois canais em 80 MHz que são adjacentes (apenas 8 canais de 20 MHz não são sujeitos da DFS (seleção dinâmica de frequência, do inglês *DynamicFrequency Selection*), podendo um canal de 160 MHz ser composto de dois canais não adjacentes em 80 MHz;

Obrigatório suporte para nova modulação em 265 QAM, com duas taxas de codificação 3/4 e 5/6, podendo optar para estes modos (vs. 64 QAM, taxa 5/6 no 801.11n em sua performance total);

Aumento na performance de no mínimo 1 Gbps e máxima performance de 6,9 Gbp/s com o MIMO (3).

Partiu-se da seguinte problemática, é viável a utilização das redes sem fio para altas taxas de transmissão de dados 802.11ac em substituição às normas anteriores e às redes cabeadas?

Sendo assim, objetivou-se buscar conhecimentos necessários para mostrar as vantagens e desvantagens que a norma do IEEE a 802.11ac tem em relação as normas anteriores e às redes cabeadas, mostrando a relação custo benefício de sua utilização em comparação à norma anterior IEEE802.11n e às redes cabeadas, especificamente objetivou-se:

1- Mostrar as vantagens e desvantagens da nova norma IEEE 802.11ac;

2 - Fazer comparação com normas anteriores e com redes cabeadas;

3 - Analisar se sua aplicação é economicamente viável.

4 - Verificar o tempo de retorno dos recursos investidos em sua implantação.

Justificou-se a escolha desse tema por perceber que o padrão IEEE 802.11 ac é uma tecnologia recente, foi lançado em 2013, porem o seu desenvolvimento se confirmou no início do ano 2015 onde ainda era uma tecnologia pouco utilizada. Como a necessidade dos consumidores por alta taxas de transmissão de dados cresce a cada dia, o novo padrão vem ganhado espaço no mercado, pois oferece soluções com altas taxas de transmissão de dados em redes sem fio.

Entretanto, há parâmetros e restrições que devem ser estudados, assim como precisa-se saber qual o momento adequado para migrar uma rede sem fio, para outro protocolo, ou para decidir quanto ao uso de redes cabeadas.

Para que os investimentos em novos equipamentos sejam plausíveis é preciso avaliar todos os fatores que influenciam na escolha correta, no caso das redes wireless um dos principais fatores e a performance e o nível de segurança da informação que os equipamentos utilizam em contrapartida às redes cabeadas.

Com os resultados obtidos nessa pesquisa espera-se que os clientes, sejam eles (coorporativos, domésticos ou acadêmicos), possam analisar as limitações e vantagens que a novo protocolo IEEE 802.11ac proporciona em suas redes sem fio, resultando em uma contribuição relevante para o meio acadêmico e para sociedade.

2 A PILHA DE PROTOCOLOS 802.11

Os padrões 802.11 fazem parte dos padrões IEEE, por exemplo, a camada 802.11 LLC (Controle de Enlace Lógico) é derivado da camada 802.2. Quando um usuário abre o navegador em seu computador, este navegador que pertence aos aplicativos de usuário terra, usa uma pilha de protocolo que é entregue com mais frequência com o sistema operacional. Ao fazer chamadas para esta pilha de protocolos, o navegador é capaz de trocar informações com um computador remoto. Um exemplo de pilha consiste no protocolo TCP / IP que permite a troca de informações em redes de natureza diferente, fragmentando informações em pacotes, que são enviadas por um sistema de mensagens independente das redes às quais os terminais estão conectados (4).

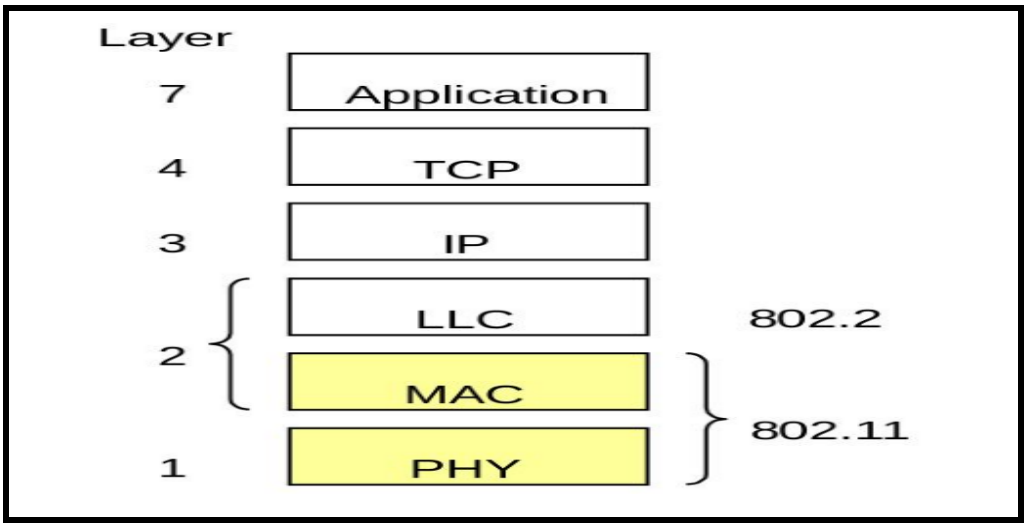
Por exemplo, em uma LAN IEEE, a camada IP usa serviços Ethernet. Quando o computador se comunica em 802.11, essa pilha usa os serviços de um driver de dispositivo que converterá esses dados em sinais de rádio (4).

O driver de dispositivo envia comandos e dados para o dispositivo, onde geralmente há uma camada LLC (Controle de Enlace Lógico) / MAC (Controle de Acesso ao Meio) e PHY (Camada Física). Ao receber informações do rádio de mídia o fluxo de informações vai do dispositivo, para o driver de dispositivo, para a pilha TcP (Protocolo de Controle de Transmissão) / IP (Protocolo de Internet) e de lá, para o aplicativo (4).

Existem três camadas em 802.11 múltiplas redes de acolhimento:

- LLC (Controle de Enlace Lógico) acesso a recursos 802.xx, esta camada permite o tratamento de diferentes solicitações concorrentes para acessar um recurso físico (3).
- MAC (controle de acesso à mídia) permite que vários terminais se comuniquem através de uma única mídia. Existe, portanto, um sistema de endereçamento interno à camada MAC admitindo que cada terminal envie mensagens para o endereço de outro terminal. A camada MAC gerencia a contenção para acessar (3).
- PHY fornece a transformação da informação digital em sinais de rádio e vice-versa (3). A figura 1 apresenta a pilha de protocolos do padrão 802.11 (3).
-

Figura 1 - Pilha de protocolos



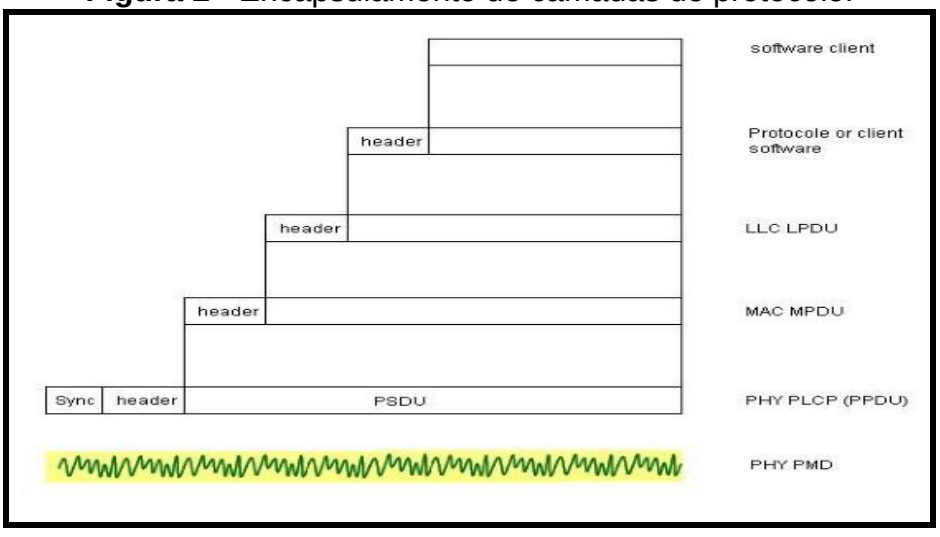
Fonte: (3)

As normas estipulam um tipo de "*frame*" para a transmissão de dados, bem como a gestão e o controlo do hardware de rádio. Como veremos em detalhes mais adiante, os quadros são divididos em seções (5).

Cada frame consiste aproximadamente em um cabeçalho, a carga útil e a sequência de verificação de quadros (FCS) (5).

Alguns quadros podem não conter dados úteis, mas sinalização, como RTS / CTS / ACK. As três camadas gerenciam diferentes questões e, portanto, cada uma adiciona informações ao pacote a partir da camada superior (5). A figura 2 apresenta o encapsulamento de camadas de protocolos do padrão 802.11.

Figura 2 - Encapsulamento de camadas de protocolo.



Fonte: (5)

Os padrões IEEE 802.11 são formados em três camadas (5):

1) Camada de enlace de dados LLC:

- 802.11e: QoS;
- 802.11f: protocolo de ponto de acesso interurbano;
- 802.11i: segurança (5).

2) A camada de acesso de mídia MAC:

- 802.3 (5)

3) Camada física PHY:

- Infravermelho: atualmente apenas para o padrão antigo 802.11;
- FHSS: Unicamente para o padrão obsoleto 802.11;
- DSSS: Para o padrão ultrapassado 802.11b;
- OFDM: Padrões 802.11a e 802.11n E 802.11ac;
- As bandas de frequência que se seguem são utilizadas nas várias emissões de frequências de 2,4 GHz (IEEE 802.11b, 802. 11g e 802.11n), 5 GHz (IEEE 802.11a, 802.11n e 802.11ac);
- Muito alta WLAN 60 GHz (IEEE 802.11ad);
- Espaços em branco (.11af, bandas diferentes, especialmente em torno de 800 MHz). (5)

2.1 Padrão 802.11n

O padrão 802.11n foi uma evolução do padrão 802.11a, e oferece muitas e importantes melhorias na subcamada MAC e na camada física (PHY), como descrito a seguir (6):

2.1.1 MIMO (*Multi-Input, Multi-Output*)

O MIMO disponibiliza vários benefícios como aumento na velocidade sem aumentar no consumo de espectro, com a utilização da multiplexagem espacial (SM), que fraciona os dados e transmite separadamente ao longo de canais espaciais paralelos em um tempo muito menor para transmiti-los em série. O 802.11n sem o SM transmite até 150Mbps e com o SM de 300 a 450 Mbps, se tanto

o transmissor quanto o receptor tiverem no mínimo três antenas e cadeia de RF em conjunto (7).

Devido a *multipath*, terá maior confiança, onde um AP com quatro antenas recebe o sinal de um cliente quatro vezes ao mesmo tempo, ou seja, quatro copias, cada sinal é distorcido (construtiva ou destrutivamente) de quatro formas diferentes diminuindo a possibilidade das quatro copias sofrerem distorção destrutiva ao mesmo tempo. Portanto, o equalizador MIMO dentro do receptor poderá reunir todos os sinais copiados e combina-los, garantindo maior confiança, com taxas de dados mais exatas e com menor número de tentativas. O que não ocorre em um AP com menos antenas, devido ao aumento do número de fluxos espaciais em relação ao número de antenas de recepção (7).

Possibilidade de maior veracidade no *downlink*, pois no 802.11n está disponível o *beamforming* (que traz grandes vantagens), como a codificação de blocos de tempo espacial e a diversidade de atrasos cíclicos. Porém quando se refere a técnicas que visam assistência ao cliente existem algumas incompatibilidades por isso *beamforming* e pouco utilizado (8).

O *beamforming* têm sua importância justificada devido à fragilidade dos dispositivos com baixo número de antenas, para desvanecimento destrutivo.

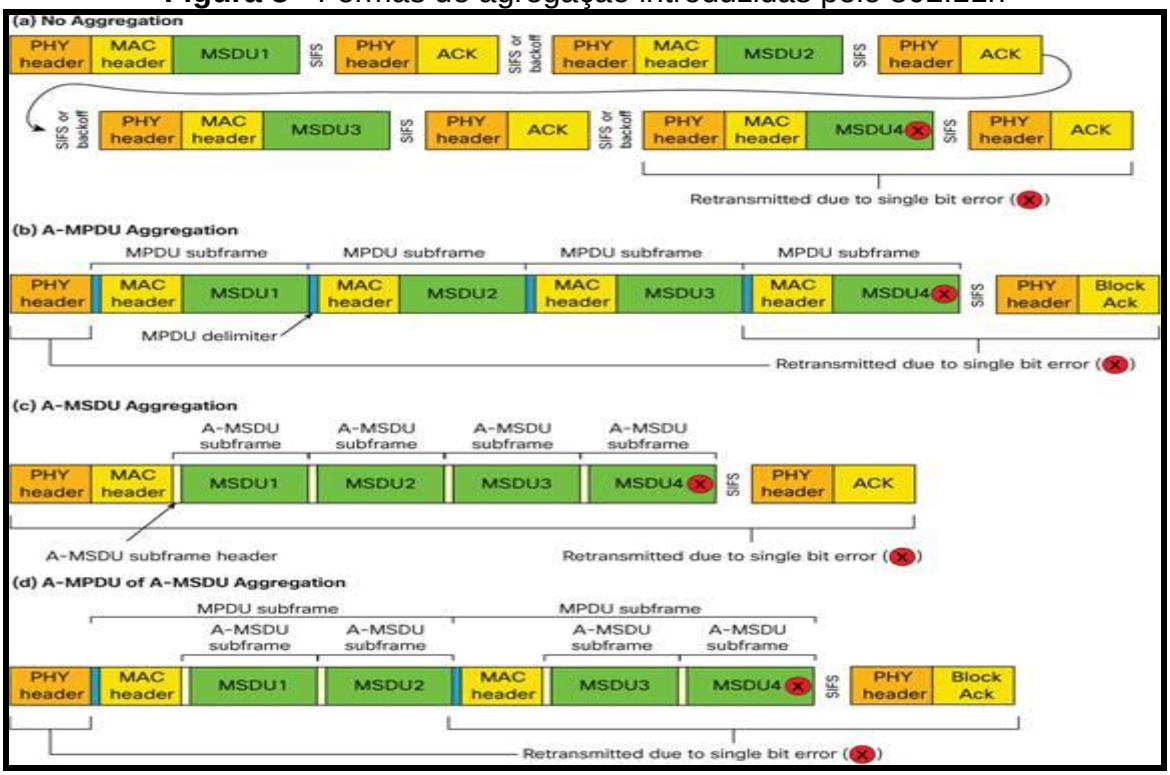
Na ligação de canais como a largura de banda do canal é duplicada de 20 para 40MHz, pode-se transportar o dobro de dados ao mesmo tempo em uma única transmissão. O que na realidade o ganho é um pouco mais que o dobro, pois pode-se usar a banda de guarda entre os dois canais tradicionais de 20MHz (8).

2.1.2 Agregação

Haja vista que o PHY é como o motor de um veiculo que gera muita potencia, o MAC é como o sistema de transmissão do veiculo, que se reponsabiliza por entregar com eficiencia a potencia para as rodas (9).

No 802.11a, cada quadro de dados vem com carga exessiva, tais como o preâmbulo para a trama, muitas vezes uma trama de confirmação, bem com os intervalos de tempo entre e ao entorno dessas transmissões. Quando o tamanho dos dados fica menor do que essa carga exessiva, acelerar a carga de dados não aumenta a velocidade efetiva. O MAC está desperdiçando potência(4). A figura 3, a seguir nos mostra as formas de agregação introduzidas pelo protocolo 802.11n (9).

Figura 3 - Formas de agregação introduzidas pelo 802.11n



Fonte: (9)

Já no 802.11n, utiliza-se duas técnicas de agregação denominada A-MSDU (*Aggregated MAC Service Data Unit*) e A-MPDU (*Aggregated MAC Protocol Data Unit*), que também podem ser mescladas, como em "A-MPDU de A-MSDU". Com agregação, os dados são asociados em uma única unidade que é transmitida com um preâmbulo e identificada em uma transmissão. Um MSDU mescla MSDUs (por exemplo, LLC + IP + TCP + dados) na parte superior da rota de transmissão MAC, portanto um MSDU individual em um A-MSDU falta um cabeçalho / rodapé MAC, como um número de seqüência ou seqüência de verificação de quadros . O que é bom para a eficicácia e ainda fazer ensaios, no nível individual de MSDU é impossível. Em paralelo, A-MPDU associa MPDUs na parte inferior do MAC, então cada MPDU em um MDPU contém seu próprio cabeçalho MAC. O resultado não é tão bom , prinicipalmente para MSDUs curtas, portanto se um pacote não conseguir trafegar pelo link sem fio, por exemplo, com um único erro de bit isolado, os outros MDPUs ainda podem ser recebidos sem erros sendo necessário repetir somente o pacate com erros. Como é mostrado na Figura 1.(9).

2.1.3 Acesso de canal para 40 MHz

Uma das principais razões para o sucesso do 802.11n é a simplicidade de se instalar um AP (*Acess Point*) ou usar um cliente, mesmo estando proximo a outros aparelhos 801.11 e todos funcionam. Isso origina de um objetivo de design do MAC em que o acesso ao canal seja suficientemente eficiente e imparcial para todos, sem levar em conta a quantidade de dispositivos, distância entre AP, capacidade do dispositivo e etc..., como por exemplo (seu pacote é tão importante quanto o meu pacote). Ver a finalidade de eficiência na gama de técnicas de MAC para diminuir as colisões, como senso de portadora física (não transmite se preceber muita energia) e senso de portadora virtual (não transmitir enquanto alguém disser que eles estariam transmitindo ou recebendo). Nota-se o objetivo de justiça em que cada dispositivo, que é, permitir transmitir somente depois de obedecer os mesmos critérios de detecção de portadora e restrição de colisão (10).

Porém o canal de 40MHz mostra desafios reais quanto a prevenção de choques e quanto a igualdade, uma vez que é impossível manter um senso de portadora físico exato e um senso de portadora virtual em dois subcanais de 20 MHz ao mesmo tempo. Ao invez disso, um canal "primário" de 20 MHz é definido com as condições normais de carga no sentido da portadora e na prevenção de choques, aumentado por um sentido de portadora físico degradado no canal "secundário" de 20 MHz (10).

Quando um dispositivo quer transmitir, ele ordena o acesso ao canal da maneira comum, tudo no subcanal primário de 20 MHz. Tambem, imediatamente antes do dispositivo poder transmitir um pacote de 40 MHz, o dispositivo verifica o estado físico de detecção da portadora do canal secundário durante uma curto prazo para garantir-se de que o canal secundário está também desocupado. Se estiver nítido, o pacote de 20 MHz é enviado, se não, o dispositivo pode transmitir um pacote de 20 MHz no canal primário ou recuar novamente, então confirma novamente se os 40 MHz completos estão livres(10).

Nota-se que este esquema simples é suficientemente justo, e a primeira opção é suficientemente eficaz. Mesmo assim, em algumas topologias, os dispositivos no canal secundário de 20 MHz são injustiçados em relação aos dispositivos de 40 MHz e, assim, 802.11n primeiramente tem regras de seleção de

canais adicionais para tentar evitar esse cenário. Essas regras operam muito bem, haja visto o grande número de canais de 40 MHz acessa em 5 GHz (10).

O 802.11n estava evidente na comunidade de padrões por seu moroso progresso. Havia três motivos:

- O processo que 802.11n aderiu para escolher a proposta vencedora, incitou limitações.
- 802.11n era muito valorizado, num cenário em que muitos especialistas queriam mesclar com sua tecnologia. A evolução ficou barrada por muito tempo atraves da contenção, e foram uitilizados vários metodos opcionais, e levou-se em longo periodo para filtrar todos os modos opcionais.
- O emprego de sistemas 802.11 a 2.4 GHz usando larguras de canal de 40 MHz na proximidade de sistemas 802.15 (como Bluetooth) levantou preocupações entre partes da comunidade 802.15(11).

No entanto o formato PDU 802.11a não possui uma recomendação de largura de banda, 802.11ac tem que usar algumas artimanhas para manter a compatibilidade com versões anteriores. A recomendação de largura de banda é codificada na sequência de codificação, bem como o bit individual / de grupo no endereço MAC do transmissor na formação RTS (Estratégia em tempo real)é transformado de "individual" para "grupo" (11).

Esta última modificação será perceptivel em traços de sniffer. Apenas um único bit é necessário para separar o número de símbolos OFDM (*Orthogonal Frequency Division Multiplexing*) reais presentes se a transmissão em vez usa o intervalo de guarda curto e os símbolos OFDM são realmente 3,6 microssegundos de comprimento. Se o fator de aceleração cair abaixo da unidade, o AP usa SU-MIMO (usuários únicos *Multi-Input, Multi-Output*) em vez disso. Ou seja, o aparelho verifica o sentido da portadora e, se o canal está ocupado, espera-se até que o mesmo desocupe, e aleatoriamente recua um número de slots e espera enquanto ele conta esses slots (11).

Após o termino da implementação do 802.11n em 2009, o 802.11ac surgiu com melhorias nas técnicas MIMO, disponibilizando um faixa de freqênca de até 160MHz e até 8 fluxos de dados. Tais tecnicas possibilitaram atingir um trafego na rede acima à 1 Gbit/s (11). A evoluçao do padrão 802.11 e mostrado na tabela 1.

Tabela 1 – Evolução do padrão IEEE 802.11

Protocolo IEEE 802.11	Publicação	Frequência (GHz)	Banda (MHz)	Vazão (Mbits/s)	Canais MIMO	Modulação	Alcance (m)
1997	junho de 1997	2.4	22	1 ou 2	-	DSSS, FHSS	100
a	setembro de 1999	5	20	até 54	-	OFDM	120
b	Setembro de 1999	2.4	22	Até 11	-	DSSS	140
g	Junho de 2003	2.4	20	até 54	-	OFDM, DSSS	140
n	Outubro de 2009	2.4, 5	20, 40	Até 150	4	OFDM	140
ac	Dezembro de 2013	5	20, 40, 80, 160	Até 780	8	OFDM	115

Fonte: (11)

2.2 – Padrão 802.11ac

O padrão IEEE 802.11ac, foi formado pela equipe do IEEE no fim de 2008 e foi confirmado em dezembro de 2013 com progressos nas camadas física e MAC. Atuando exclusivamente na faixa de 5 GHz, IEEE 802.11ac garante compatibilidade com as versões anteriores IEEE 802.11a (5 GHz) e IEEE 802.11n que operam com a na mesma faixa de frequência (12).

As principais inovações, especialmente em camada física, ressaltadas no padrão 802.11ac são:

- Para comunicação utiliza Larguras de banda de 80 MHz e 160 MHz;
- Suporta até 8 fluxos espaciais empregando MIMO;
- Emprego de modulação 256-QAM.
- Multiusuários com MIMO, através de acesso múltiplo por separação no espaço SDMA (12).

Aqui está o que *Wi-Fi* Alliance sugere como soluções para chips baseados em 802.11ac:

Os recursos obrigatórios na Fase 1 são(3):

- Operação de 5GHz (2,4 GHz está excluído);
- Canais de 20, 40 e 80MHz;

- 1 fluxo espacial, mais 2 fluxos espaciais para aparelhos não-móveis, porque menos canal de informação de estado de diálogo em estações fixas;
- Mcs o-7 (BPsK, r 1/2 a 64-QAM, r 5/6);
- VHT A-MPDU delimitador para RX e TX para MPDU simples;
- A-MPDU na recepção;
- A-MPDU em transmissão;
- Clear Channel Assessment (CCA) em canal secundário;
- CTS com sinalização de largura de banda em resposta a RTS com sinalização de largura de banda (3).

As características opcionais na Fase 1:

- 2 ou 3 fluidos espaciais cliente;
- Mobile Access Points com 2 fluxos espaciais AP;
- 3 stream espacial para pontos de acesso fixos;
- Modulação em (256-QAM, 3/4 e r 5/6);
- Intervalo de guarda Curta (GI);
- AP STBC na transmissão 2x1 (melhorando SNR através da utilização de múltiplos caminhos);
- STA STBC na recepção 2x1;
- Recepção A-MPDU de A-MSDU;
- RTS com sinalização de sinalização de banda;
- *Transmit beamforming* (TxBF);
- Codificação LDPC (Low Density Parity Check). (3)

Características da Fase 2:

- *Stream* para cliente e AP;
- MU-MIMO;
- TXOP;
- Compartilhamento VHT TXOP;
- Economia de energia. (3)

No 802.11ac tem possibilidade de usar mais fluxos MIMO, no máximo 8, o que nos leva a pressupor que há 8 antenas disponíveis. Além disso emprega o *Multi-*

User MIMO (MU-MIMO), possibilitando a criação de várias seções geográficas dentro de uma célula que permitido pelo SDMA (do inglês: *Space Division Access*). Com a utilização do MU-MIMO é possível que várias estações possam transmitir simultaneamente com seu AP (do inglês: Access Point), ou seja, ponto de acesso (13).

O MU-MIMO é uma evolução do MIMO que se faz necessário o uso de vários conjuntos de antenas, bem como ter compatibilidade com a versão anterior e coexistência com aparelhos 802.11a, 802,11n, na banda de 5GHz, o que significa encapsular a introdução de VHT (*Very High Throughput*), em um quadro 802.11a. Similarmente aos produtos 802.11, os produtos 802,11ac surgiram no mercado bem antes da norma se lançada oficialmente(13).

Em comparação com o 802.11n, o projeto do MIMO para o 802.11ac é bem mais simples, não só o design, mas levando em conta o padrão em si, a sua capacidade se recuperar perante interferência ou ruído, levou apenas a um aumento no *throughput* incrementado sobre a geração anterior a 802.11n (13).

O que explica a simplicidade do MIMO no 802.11ac em relação a 802.11n é devido considerar que do lado do 802.11n o número de McS (do inglês: *Modulation and Coding Scheme*) “Esquema de Modulação e Codificação” (são 77, incluindo 32 que são considerados como realmente necessários e apenas 8 que são obrigatórios para uma estação) e pelo outro lado os 8 McS do 802.11ac, que entre eles 6 já existiam no 802.11n. Desse jeito, como os chipsets IEEE 801.11n ficaram disponíveis no mercado em maio de 2007 foi criado pelos integrantes do IEEE 802.11 uma nova equipe de estudo que recebeu o nome de “VHT” ou “muito alta velocidade” visando elevar a taxa de transferência do IEEE 802.11 (13).

Devido às dificuldades de alocação um canal de 160 MHz contínuo (há disponibilidade de dois na faixa de 5 GHz), o padrão permite que dois canais de 80 MHz incontínuos sejam empregados em uma transmissão que, ao todo, solicita 160 MHz de largura de banda (14).

O padrão também demanda a possibilidade de transmissão com múltiplos usuários. Um sistema MU-MIMO aceita que um AP transmita dados para vários usuário simultaneamente através de *beamforming*, método de múltiplas antenas com reutilização espacial (14).

A Tabela 2 mostra similaridades e diferenças entre o padrão 802.11ac em relação ao padrão antecessor, o IEEE 802.11n. Duas das considerações

descartadas no 802.11ac são MCS (Esquema de modulação e codificação) diferentes e o formato de preâmbulo *Greenfield* (14).

Quadro 1 - Comparação entre os padrões 802.11n e 802.11ac

	IEEE 802.11n	**IEEE 802.11ac**
MIMO	Sim	Sim
Largura de banda do canal (MHz)	20 e 40	20, 40 e 80 obrigatórios 160 e 80 + 80 opcionais
Código LDPC	Opcional	Opcional
STBC	Opcional	Opcional
Intervalo de guarda curto	Opcional	Opcional
Multiusuários	Não	Opcional
Fluxos espaciais	Até 4	Até 8
Modulação	BPSK, QPSK 16-QAM e 64-QAN	BPSK, QPSK, 16-QAM 64-QAM e 256-QAM (opcional
MCS desiguais	Opcional	Não
Faixa de operação (GHz)	Opcional	Não
Preâmbulo *Greenfield*	Opcional	Não

Fonte: (14)

Introduzido na versão IEEE 802.11n, MCS desiguais são empregados com dois, três ou quatro direções espaciais, taxa de código iguais, entretanto com modulações diferentes (15).

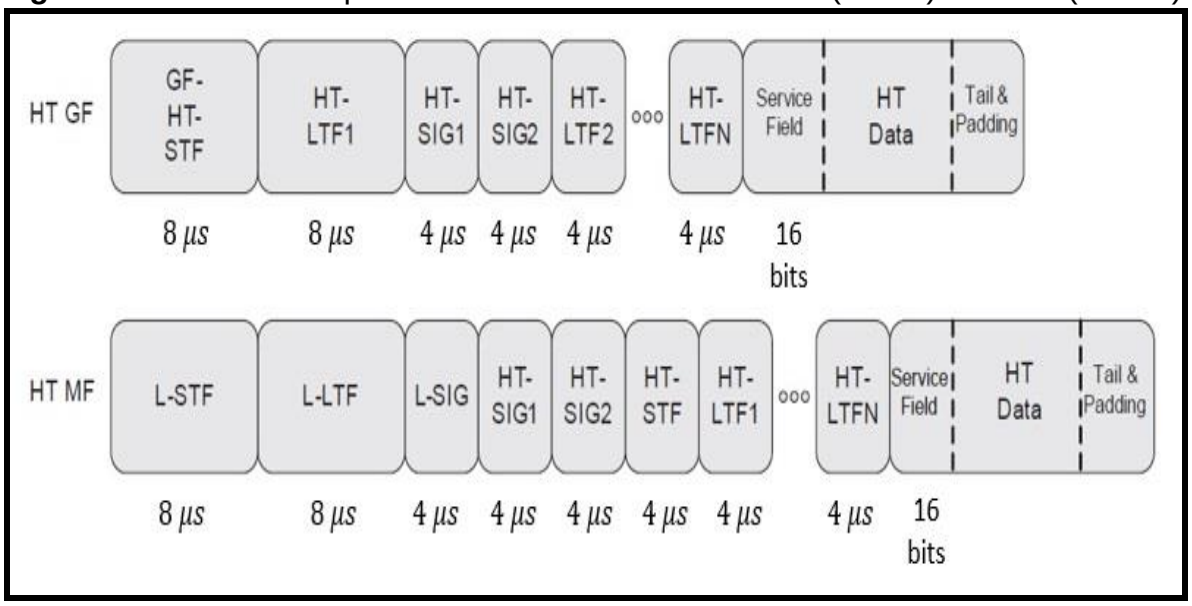
São empregados em conjunto com *beamforming* quando cada fluxo está sujeito a canais com SNR's diferentes. Como exemplo, MCS 38 emprega taxa de código 3=4 e dois fluxos espaciais, um modulado em 64-QAM e outro em 16-QAM; logo MCS 74 emprega novamente taxa de código 3=4 e quatro fluxos espaciais, dois com modulação 64-QAM e dois modulados em 16-QAM. Para simplificar do padrão IEEE 802.11ac, MCS diferentes foram banidos do novo padrão (15).

Já no padrão IEEE 802.11n foi proposto o preâmbulo *Greenfield* para diminuir a quantidade de *overhead* por meio da redução dos campos do preâmbulo e atuar

principalmente na faixa de 5 GHz, devido ao baixo progresso do IEEE 802.11a nessa faixa de frequência em várias partes do mundo (15).

Entretanto, com o progresso das WLANs, sua utilização para redes em larga escala é evitado justamente por não fornecer compatibilidade com outros dispositivos IEEE 802.11 que empregam o formato de preâmbulo *Mixed*. Por essa causa e fatores com relação a alocação de canais na camada MAC, no período de desenvolvimento do IEEE 802.11ac seu conceito não foi adotado. A figura 4 nos mostra os dois formatos de quadros para o IEEE 802.11n. (15)

Figura 4 -Formatos de quadros IEEE 802.11n: *Greenfield* (acima) e *Mixed* (abaixo).

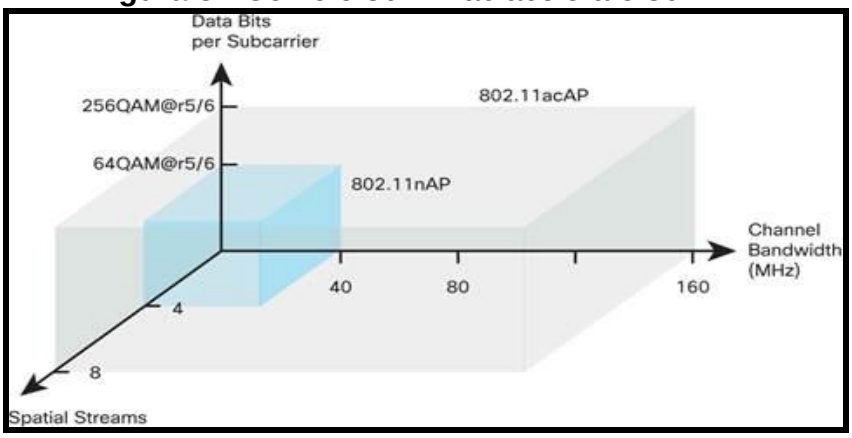


Fonte: (15)

2.3 Aumento dos Canais

A princípio com o uso de canais de rádio maiores, ocorre o aumento do *Throughput*. Como mostrado na figura 6, a largura dos canais foi aumentada para 80 MHz e em alguns casos para 160 MHz contra 40 MHz no máximo em 802.11n em 2.4GHz. Suporte para canais de 80 MHz é obrigatório em 802.11ac. O suporte de canal de 160 MHz é facultativo. Um canal de 160 MHz pode até ser composto de dois canais não contíguos a 80 MHz. Isto é devido à dificuldade em encontrar dois canais de 80 MHz contíguos. (16)

Figura 5 - Como o 802.11ac acelera o 802.11n



Fonte: (16)

O *Throughput* em redes sem fio depende de três fatores: largura de banda do canal, densidade da constelação e número de fluxos espaciais. O 802.11ac explora os limites de cada um deles, como mostrado na Figura 5 (16).

A velocidade da camada física de 802.11ac é calculada de acordo com o Quadro 2. Por exemplo, uma transmissão de 80 MHz enviada a 256QAM com três fluxos espaciais e um espaço de guarda curto proporciona 234 × 3 × 5/6 × 8 bits / 3,6 microssegundos = 1300 Mbps (4).

Quadro 2 - *Calculando a Velocidade de 802.11n e 802.11ac*

PPHY	**Largura de banda (como número de subportadores de dados)**	**número de Fluxos espaciais**	**Bits de dados por subportadora**	**Tempo por símbolo OFDM**	Taxa de dados PHY (bps)
802.11n or 802.11ac	56 (20 MHz)	4	Até 5/6 × $\log_2(64) = 5$	3.6 microssegundos (intervalo de guarda curto)	
	56 (20 MHz)			4 microssegundos (intervalo de guarda longo)	
8802.11 ac only	234 (80MHz)	8	Até 5/6 × $\log_2(256) \approx 6.67$		
	2 × 234 (160 MHz)				

Fonte: (16)

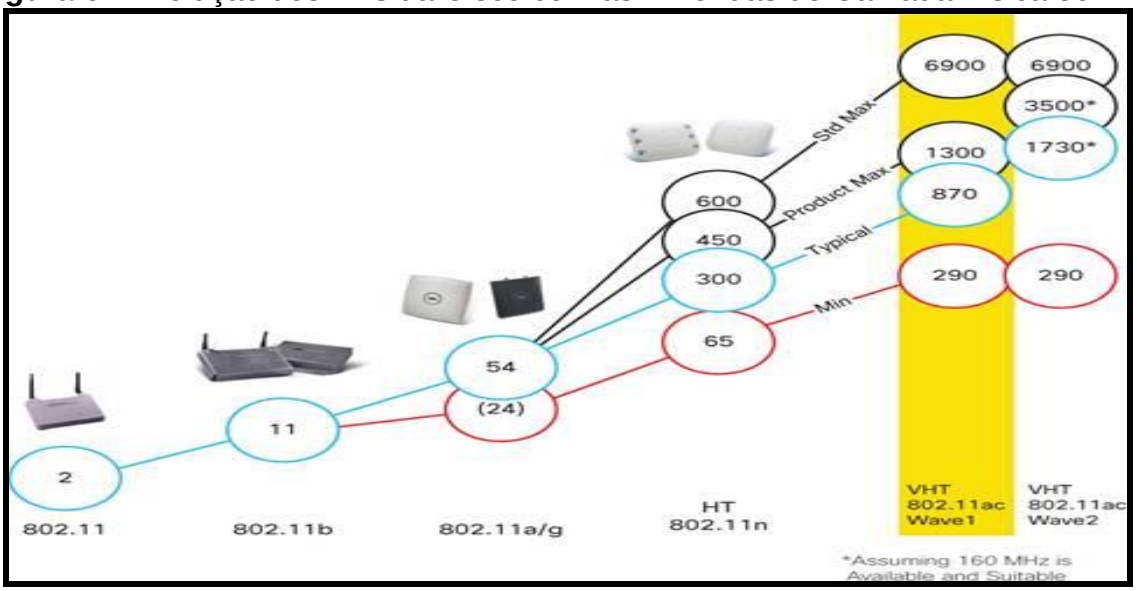
Podemos notar que ao aumentar a largura de banda do canal para 80 MHz a velocidade e elevada em 2,16 vezes, e 160 MHz proporciona uma duplicação. Em contrapartida ele exige mais espectro, e cada vez que estamos dividindo o mesmo poder de transmissão sobre duas vezes mais subportadoras, então a velocidade é duplicada, mas a faixa para essa velocidade duplicada é levemente reduzida (para uma vitória global (16).

Saindo de 64QAM para 256QAM também ajuda, por outro 8/6 = 1,33 vezes mais rápido. Estando mais próximos, os pontos de constelação são mais sensíveis ao ruído, de modo que em 256QAM ajuda mais em alcance reduzido onde 64QAM já é confiável. Ainda assim, 256QAM não requer mais espectro ou mais antenas do que 64QAM (16).

A velocidade depende número de fluxos espaciais. Mais fluxos espaciais demandam mais antenas, conectores de RF e cadeias de RF no transmissor e no receptor. As antenas devem ser afastadas um terço de um comprimento de onda (3/4 polegadas) ou mais, e as cadeias de RF a mais consomem energia adicional. O que leva muitos dispositivos móveis a limitar o número de antenas para um, dois ou três (16).

Em conjunto, estes três aumentos de velocidade são expressivos. Conforme mostrado na Figura 6 e no Quadro 3, o protocolo 802.11ac requer no mínimo 4,4 vezes mais veloz que o protocolo 802.11n correspondente e os produtos Wave 1 da camada média e alta são quase 3 vezes mais rápidos, atingindo taxas de dados PHY de 1,3 Gbps. O ganho real será uma função da eficácia do MAC (raramente melhor que 70%) e das capacidades dos dispositivos em cada terminação do link (16).

Figura 6 - Evolução dos APs da Cisco com as Emendas de Camada Física 802.11.



Fonte: (16)

Quadro 3 - Taxas de dados importantes de 802.11a, 802.11n, and 802.11ac.

Configuração Nominal	**Largura de Banda (MHz)**	**Número de fluxos espaciais**	**Tamanho e Taxa da Constelação**	**Intervalo de guarda**	**Taxa de dados PHY (Mbps)**	**Taxa de transferência (Mbps) ***
802.11a						
Todos	20	1	64QAMr3/4	Longa	4	24
802.11n						
Alteração min.	20	1	64QAMr5/6	Longa	5	46
Produto low-end (2,4 GHz apenas+)	20	1	64QAMr5/6	Curta	2	51
Produto intermediário	40	2	64QAMr5/6	Curta	00	210
Produto máximo	40	3	64QAMr5/6	Curta	50	320
Alteração máxima	40	4	64QAMr5/6	Curta	00	420

Configuração Nominal	Largura de Banda (MHz)	Número de fluxos espaciais	Tamanho e Taxa da Constelação	Intervalo de guarda	Taxa de dados PHY (Mbps)	Taxa de transferência (Mbps) *
802.11ac 80 MHz						
Alteração min.	80	1	64QAMr5/6	Longa	93	210
Produto low-end (2,4 GHz apenas +)	80	1	256QAMr5/6	Curta	33	300
Produto intermediário	80	2	256QAMr5/6	Curta	67	610
Produto máximo	80	3	256QAMr5/6	Curta	300	910
Alteração máxima	80	8	256QAMr5/6	Curta	470	2400
802.11ac 160 MHz						
Produto low-end	160	1	256QAMr5/6	Curta	67	610
Produto intermediário	160	2	256QAMr5/6	Curta	730	1200
Produto high-end	160	3	256QAMr5/6	Curta	600	1800
Produto ultra-high-end	160	4	256QAMr5/6	Curta	470	2400
Alteração máxima	160	8	256QAMr5/6	Curta	930	4900
* Assumindo 70 por cento eficiente MAC, exceto para 802.11a, que carece de agregação, mas supondo que 40 MHz não está disponível devido à presença de outros APs.						

Fonte: (16)

Realmente, haverá apenas três ou quatro canais verdadeiramente com ausência de interferência em 802.11ac dependendo de onde é usado e nem todos os canais são iguais na potência permitida ou existência de DFS e, sendo assim, a banda de 5 GHz tende a saturar tão rápido quanto a banda de 2,4 GHz. (16).

2.4 Projeção para o Futuro

2.4.1 Norma 802.11ad

Na atualidade o IEEE já desenvolve uma nova norma para usuários mais avançados que irá oferecer maiores velocidades, menos interferências e alcance maior (17).

O padrão 802.11ad afirma oferecer velocidades na ordem dos Gb/s. Para isso, está emprega uma largura de banda por volta de 2 GHz na banda de frequências dos 60 GHz (17).

Para usuários doméstico, poderá atingir 1,3 Gb/s, sendo o limite teórico desta norma perto dos 7 Gb/s (17).

Apesar do 802.11ad trazer grandes atrativos no aumento da velocidade, a 802.11ac deverá ser a rede a predominar o comércio nestes próximos anos e a norma 802.11ad será mais direcionada aos usuários avançados e empresas (17).

3 Segurança em Redes Wireless

As WLANs, assim como, qualquer outro sistema, não são suficientemente seguras desde seu surgimento. É necessário ter certos cuidados e realizar configurações para uma WLAN ser avaliada como suficientemente segura (18).

A comunicação feita por meio de ondas de rádio ou infravermelho como portadoras do sinal, caso outra estação esteja sintonizada na faixa de frequências da transmissão recebe as informações transmitidas. Para que uma segurança um mínima exista em uma WLAN, são indispensáveis, assim, dois componentes (18):

- Meio de determinação de quem ou o que pode utilizar a WLAN – esse solicitação é atendido pelos mecanismos de **autenticação** para controlar o acesso da LAN;
- Meio que fornece **privacidade** para informações wireless – esse solicitação é realizada pelos algoritmos de criptografia (18).

3.1 O Algoritmo WEP (*Wired Equivalent Privacy*)

Trata-se de um algoritmo de criptografia usado por um processo de autenticação de chave compartilhada com a finalidade de autenticar usuários e criptografar dados somente sobre o segmento *wireless*. Ele envolve os seguintes serviços básicos de segurança:

- **Autenticação –** seu função é tentar garantir que apenas clientes que pertençam à rede poderão acessá-la por meio da comprovação e avaliação de suas identificações.
- **Privacidade –** para garantir a privacidade dos dados que trafegam na rede, isto é, verifica se os dados só poderão ser acessados por clientes que tiverem permissão.
- **Integridade –** para assegurar que os dados transmitidos não sejam alterados no caminho de ida e volta entre os usuários e os pontos de acesso (19).

A seguir, esses itens são detalhados.

3.1.1 Autenticação

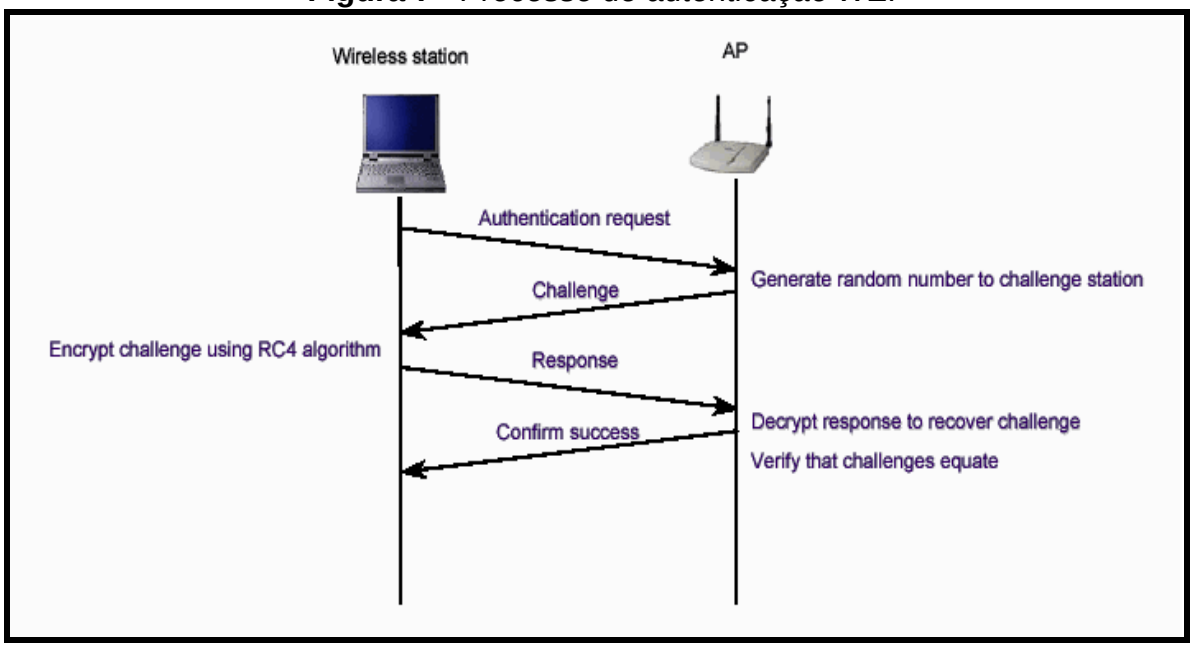
O WEP oferece autenticação em dois tipos: chave dividida (*shared key*) e sistema aberto (*open system)*. Em um sistema acessível a autenticação é a seleção de fábrica devendo ser evitado, pois trabalha somente como mecanismo de identificação, (20).

Se o mecanismo de criptografia estiver desabilitado, qualquer aparelho poderá acessar o ponto de acesso e, em seguida, à rede. Com a criptografia habilitada se o usuário não tiver posse de uma chave secreta, o usuário não terá sucesso ao transmitir nem receber mensagens por meio do ponto de acesso, mesmo que a estação esteja autenticada (20).

A autenticação com base em chave compartilhada utiliza a método de *challenge-response (*20).

O ponto de acesso não é autenticado neste mecanismo, somente na estação. Conforme a figura 7, o aparelho sem fio está requerendo ao AP sua autenticação. Então um número aleatório e gerado no AP que o despacha para o aparelho. Utilizando o algoritmo RC4 o aparelho recebe esse número, criptografa-o e o devolve. O AP descriptografa a resposta e a confronta com o número enviado. Caso a checagem for verdadeira, o AP envia para o aparelho uma mensagem confirmando que a autenticação foi realizada com sucesso (20). A figura 7 esquematiza os métodos de autenticação das WLANs 802.11.

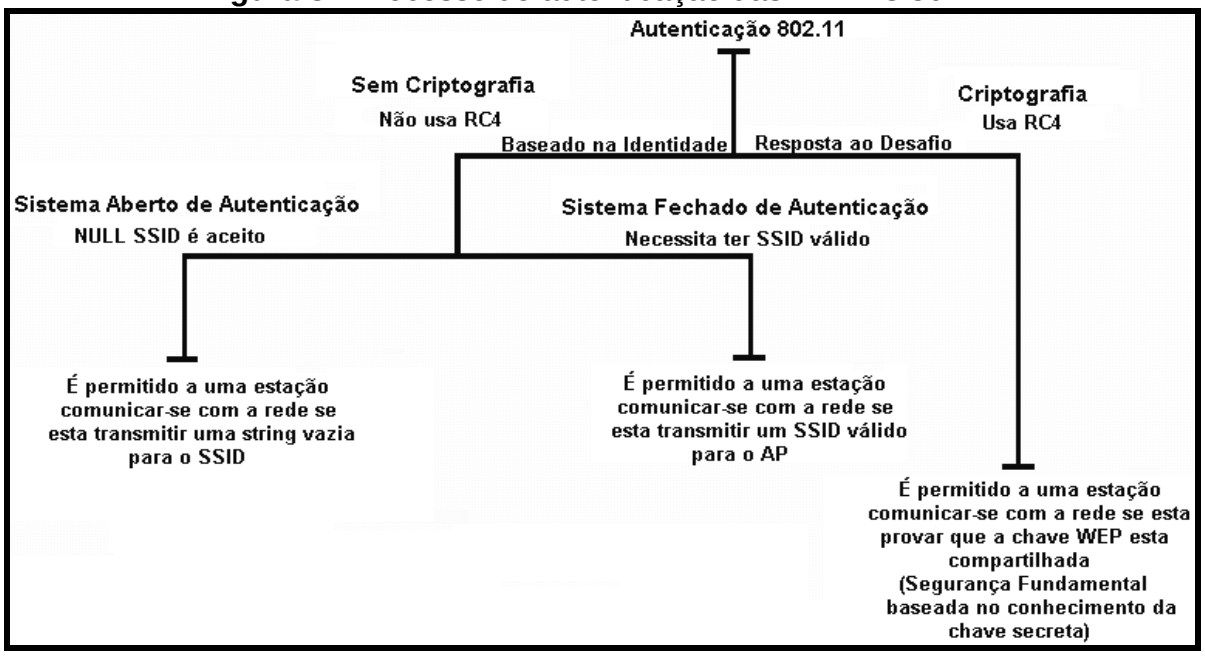
Figura 7 - *Processo de autenticação WEP*



Fonte: (20)

Um problema grave deste esquema de autenticação é que o técnica de *challenge-response* é sensível a invasores. Sendo possível interceptar tanto o texto cifrado quanto o texto original, a chave criptográfica pode ser derivada com facilidade (20).

Figura 8 - Processo de autenticação das WLANs 802.11.



Fonte: (20)

3.1.2 Privacidade

É opcional aderir à Privacidade. Quando opta-se por habilitá-la, emprega-se métodos de criptografia, baseadas no algoritmo RC4, para originar uma pseudo-sequência de dados aleatório. Através deste método, o WEP pode evitar a exposição dos dados no período da transmissão pela rede sem fio (18).

Torna-se indispensável que os participantes tenham de posse a mesma chave criptográfica para que seja possível a codificação e decodificação dos quadros, (18).

Entretanto, o padrão IEEE 802.11, não explicita como deve ser a repartição das chaves e, na realidade, a maior parte das instalações usam a mesma chave para todos os aparelhos. Isso acarreta enormes problemas à segurança dessas instalações, haja visto que a chave é dividida com vários usuários, atrapalhando a

sustentação do segredo. Na tentativa de minimizar o problema alguns administradores de rede não revelam a chave secreta ao usuário final, realizando eles mesmos a configuração dos equipamentos (18).

Como as chaves continuam armazenadas nos equipamentos remotos esse método, portanto, não apresenta a solução. O compartilhamento de uma mesma chave por vários clientes também elevam as possibilidades de colisão do vetor de inicialização, detalhados a seguir. Proporcionalmente ao o número de usuários cresce a possibilidade de uma colisão aleatória (18).

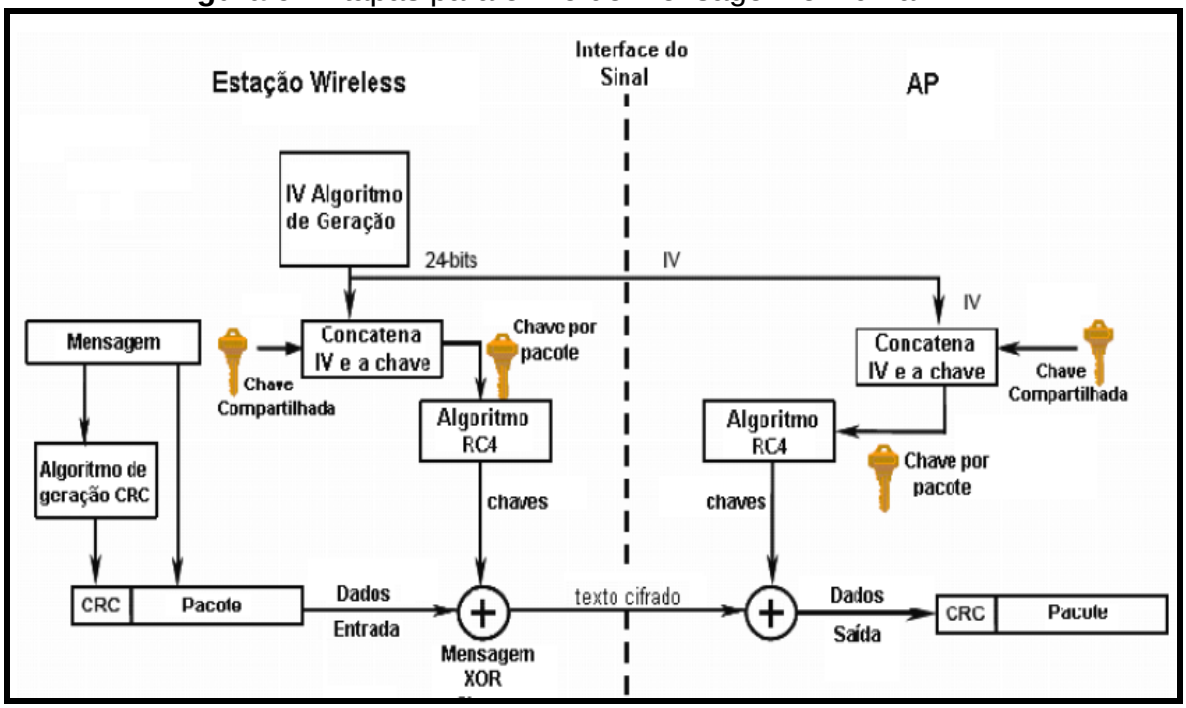
Além do mais, tendo em vista que a troca de chaves solicita que cada usuário reconfigure o seu aparelho, se torna cada vez mais frequente as atualizações dos drivers controladores dos cartões de rede (NIC – Cartão de Interface de Rede).

Na realidade, a troca levará meses ou anos para ser realizada, fornecendo aos invasores mais tempo para avaliar o tráfego (18).

Para uma mensagem ser enviada se faz necessário seguir os passos abaixo:

- A equipamento transmissor encadeia a sua chave secreta (*shared key*), de 40 a 104 bits, a um vetor de inicialização (IV) de 24 bits;
- O resultado utilizado como entrada para o algoritmo gerador de números pseudoaleatórios (PRNG) estabelecido pelo RC4;
- O PRNG cria uma sequência de bits de tamanho idêntico ao quadro MAC contendo seu CRC (*Cyclic Redundancy Check*);
- É realizada uma operação binária XOR entre a sequência de PRNG e o quadro MAC gerando o texto cifrado;
- O quadro cifrado é transmitido em conjunto com o IV;
- O processo inverso e feito pelo receptor (18).
- A seguir na figura 9 são mostradas as etapas descritas acima.

Figura 9 - Etapas para envio de mensagem em uma WLAN



Fonte: (18)

Quase sempre, o ampliação do tamanho da chave criptográfica eleva o grau de segurança (18).

Em algumas pesquisas é apontado que chaves com tamanho maior que 80 bits, torne praticamente impossível e a quebra do código. A maioria das WLANs, contudo, possui chaves criptográficas de no máximo 40 bits (18).

O vetor de acionamento inicial IV no WEP tem 24 bits e, como é muito pequeno, apresenta um problema da WEP. Em último caso, esse IV é modificado a cada pacote transmitido, inicializando em zero e chegando ao valor limite de 224-1. Sendo assim, como que a chave criptográfica k é igual para usuários que estão conectados ao mesmo tempo, o par (k, IV) é reproduzido assim que o IV é reproduzido. Essa reprodução de sequência não é desejada, pois abre possibilidade a invasões e por consequência o descobrimento de pacotes por ocasionais intrusos (18).

3.1.3 Integridade

Para garantir a integridade dos dados transmitidos entre clientes e APs, o padrão IEEE 802.11 especifica um serviço de segurança que utiliza um CRC-32

(*Cyclic Redundancy Check*) simples. Esse artifício nega qualquer mensagem que durante a transmissão tenha sido alterada (19).

O CRC é calculado em cada pacote a ser transmitido. Utilizando uma chave RC4 para originar o texto cifrado da mensagem, a integridade do pacote é criptografada. Portanto no receptor, é efetuada a descriptografia, assim, na mensagem recebida o CRC é recalculado. A mensagem original do CRC e confrontada com CRC calculado. Havendo divergência, a mensagem que teve sua integridade violada será indicada ao receptor, que por sua vez, irá descartá-la (19).

O CRC-32, entretanto, é uma função linear que não possui chave. Essa característica faz com que o protocolo fique sujeito a dois tipos de invasores danosos e indesejáveis (19).

Eventuais mensagens capturadas e modificadas no meio do caminho sem serem descobertas pelo receptor final. Isso ocorre devido à linearidade da função detectora de falhas e, pelo motivo da função não haver uma chave(19).

Encontrar uma sequência confidencial RC4 e, na sequência, autenticar-se na rede e inserir mensagens clandestinas na mesma (19).

3.2 Outros algoritmos

Tendo em vista os problemas detectados no WEP, ao passar do tempo, foram sugeridas melhorias no sistema de segurança das WLANs, que resultou em vários soluções acessíveis para os usuários. Algumas dessas soluções e suas principais características são detalhados a seguir (21).

3.2.1 WEP2 (*Wired Equivalent Privacy version 2*)

No ano de 2004, o IEEE propôs uma nova versão da WEP. É fundamentada no algoritmo RC4, empregando um vetor de inicialização de 12 bits, o que o faz mais robusta, porém ainda sensível aos ataques (21).

3.2.2 WPA (*Wi-Fi Protected Access*)

WPA fornece encriptação através do TKIP (*Temporary Key Integrity Protocol*) adotando o algoritmo RC4. Ele é originado do protocolo 802.1X com melhoria nas

vulnerabilidades da WEP promovendo avanços como a construção e distribuição de chave por pacote, um código de integridade de mensagens e um vetor de inicialização mais robusto. O único ponto negativo se dá pelo fato que é possível que o hardware não suporte o WAP (21).

3.2.3 WPA2 (*Wi-Fi Protected Access version 2*)

Baseado no padrão 802.1i, WPA2 foi lançado em 2004 e emprega um técnica mais reforçada de encriptação (AES – *Advanced Encryption Standard*). O AES aceita chaves de 128 bits, 192 bits e 256 bits. Tem compatibilidade com WPA e cada sessão utiliza um novo jogo de chaves (21).

3.2.4 SSID (*Service Set Identifier*)

Emprega uma palavra-passe aceitando uma rede sem fio de ser dividida em redes diferentes com um único identificador. Buscando acesso a uma das redes, o computador cliente deve ser configurado com a SSID da rede almejada. A seleção de SSID, contudo, não é reconhecido como um técnica segura de impedir acesso sem autorização à uma WLAN, uma vez que o SSID é publicado em texto puro em cada beacon que o AP despacha pela rede. Ficando fácil identificar o SSID de uma rede utilizando um *sniffer* (22).

3.2.5 MAC (Media Access Control) *address filtering*

Pode ser acrescentada ao AP uma lista de endereços MAC pertencentes a computadores clientes, tendo somente estes o acesso liberado. É realizado a comparação entre os endereços da lista para permissão ou não permissão com o endereço MAC quando o cliente realiza um pedido, (22).

Apesar dos filtros MAC serem uma ótimo medida de proteger a rede contra acesso não permitidos, eles continuam tendo sensibilidade a ataques conforme descrito a seguir:

- Extravio do PC *Card* que fica no filtro MAC do AP;
- Adotar um *sniffer* na WLAN e em seguida copiar um endereço MAC, fingindo-se passar pelo cliente clonado;

Para redes menores e domésticas com poucos clientes os Filtros MAC são excelentes. Utilizar WEP e filtros MAC garantem uma solução de segurança satisfatória para esses lugares, já que é pouco plausível que um invasor empregue esforços para copiar ou clonar um endereço MAC ou em experimentos de quebrar a chave WEP para obter acesso a um dispositivo de um cliente doméstico (22).

3.2.6 VPN (*Virtual Private Network) Link*

Talvez a forma de segurança mais garantida seria configurar uma conexão VPN na rede sem fio. VPNs usam AES e são as favoritas por gerentes de empresas (22).

3.2.7 802.1X

Com o 802.1X a etapa de autenticação é realizada por um servidor RADIUS no qual as credenciais do cliente são conferidas com o servidor. Quando um cliente tenta o primeiro acesso, ele precisa fornecer o nome de usuário e a senha. Em seguida é realizado a comparação com o servidor RADIUS e o acesso é garantido de acordo com o resultado (23).

Cada usuário possui uma senha única e para oferecer maior segurança ela mudada com frequência. Quando combinado com o protocolo de autenticação extensível (EAP), o 802.1x proporciona um ambiente suficientemente seguro e flexível tomando como base vários projetos de autenticação empregados nos dias de hoje (23).

Utilizado na transação do método de autenticação o EAP é um protocolo que determina as características do técnica de autenticação abrangendo:

- Requerimento de credencias aos usuário como senhas, certificados, etc;
- Utilização de protocolos (MD5, TLS, GSM, OTP, etc);
- Geração de chave e autenticação mutua com suporte agregado (23).

O técnica de uma autenticação 802.1x-EAP ocorre da seguinte forma:

1º. Solicitação de associação com o AP pelo cliente;

2º. Recebimento de resposta da solicitação de associação feita pelo AP com uma solicitação de identidade EAP;

3º. O AP recebe uma resposta da identidade EAP do usuário;

4º. É enviada ao servidor de autenticação uma identidade EAP do usuário;

5º. Uma solicitação de autorização ao AP e feita pelo servidor de autenticação;

6º. Encaminhamento do pedido de autorização ao cliente e realizada pelo AP;

7º. E enviada uma resposta de autorização EAP do cliente para o AP;

8º. O servidor de autenticação recebe uma resposta de autorização EAP do AP;

9º. O AP recebe do servidor de autenticação uma mensagem EAP de autorização concedida;

10º. O cliente recebe a mensagem do AP, mudando o status da porta em modo EMCAMINHADO (23).

4 Redes Mesh

Ao oposto da rede sem fio tradicional, uma rede *mesh* não é constituída apenas de um único acess point conectado à rede de banda larga. Ao oposto, ela é feita de nós que atuam em conjunto para distribuir um único sinal de internet em múltiplos pontos de um mesmo ambiente. Na maioria dos casos, os nós trabalham como roteadores e repetidores de alta eficácia (24).

O que ocorre devido o sinal de internet em uma rede *mesh* não se perder ao se distanciar do roteador principal. De fato, a intenção é que uma conexão *Wi-Fi* nesse modo fique ainda mais rápida com o acréscimo de novos nós – unidades independentes do Google *Wi-Fi* ou roteadores *OnHub*, por exemplo (24).

Os pontos de acesso que constituem uma rede *mesh* não são roteadores nem repetidores comuns, pois necessitam ser municiados com um aplicativo especial. De acordo com a necessidade do usuário o sistema é indispensável para controlar a repartição da conexão na rede. Ainda que os nós sejam feitos para estender-se o alcance da conexão no espaço interno, o *troungput* pode ser direcionado para uma tarefa específica, de acordo com a necessidade (24).

Assim, um computador que realiza streaming de filme pode receber preferência, e simultaneamente os dispositivos móveis sofrem com ausência de sinal ao serem mudados de posição. Na prática, que dizer que, uma rede *mesh* pode proporcionar conexão estável em qualquer parte do recinto dentro do seu raio de abrangência, mesmo que o usuário se mova com frequência (24).

4.1 Facilidade de uso

Redes *mesh* são simples de se administrar, pois o software que acompanha cada nó possui o dever de se associar ao restante da infraestrutura automaticamente. A compatibilidade entre as unidades depende do fabricante, mas, em contrapartida, não é necessário um administrador de rede para desenvolver o desempenho da conexão (24).

4.2 Relação Custo benefício

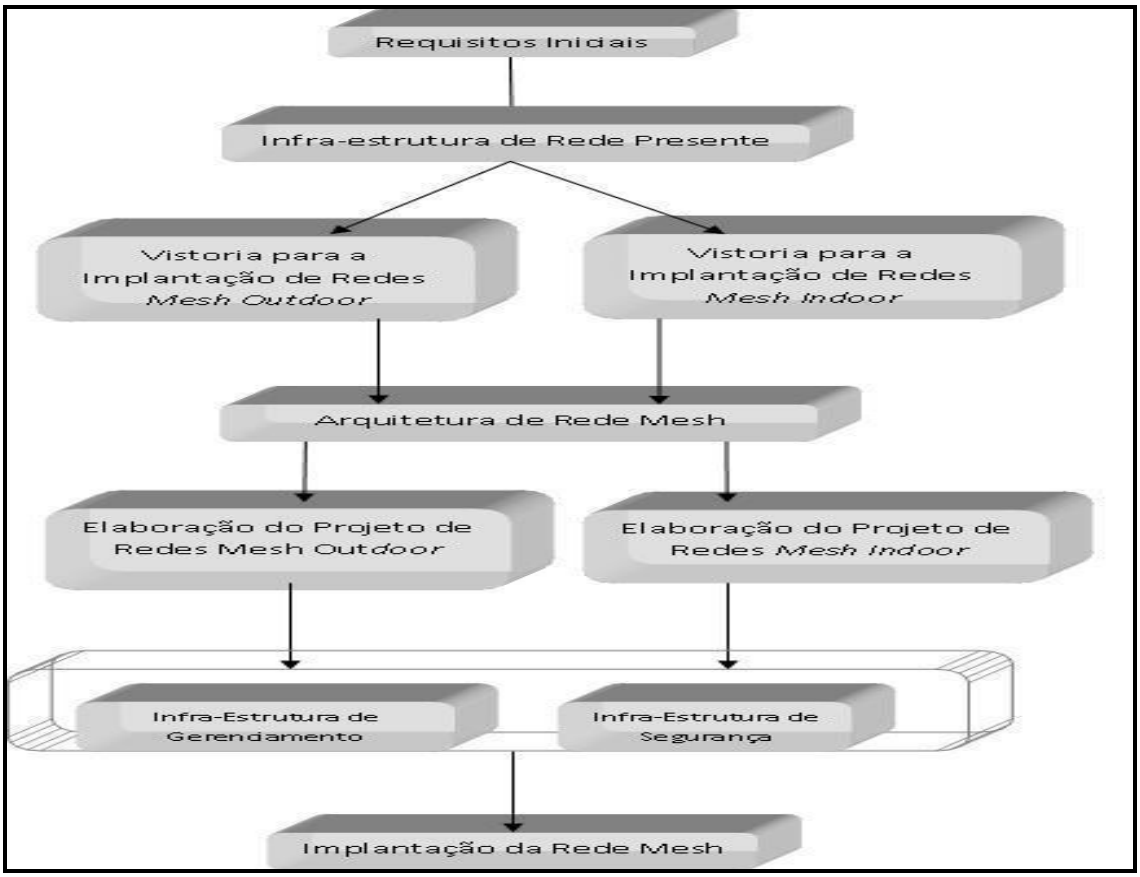
Em redes sem fio comuns, é necessário investir em roteadores mais potentes ou em repetidores, que podem prover baixa eficiência, para cobrir áreas maiores. Já em redes *mesh*, o custo da infraestrutura tem escalabilidade mais maleável. Para cobertura em ambientes mais amplos, basta acrescentar mais nós a uma mesma rede (24).

4.3 Metodologia para Implantação de redes sem fio.

Se faz necessário alguns cuidados com o planejamento na fase de implantação, para garantir a qualidade de uma rede, pois neste momento é estudado o espaço físico onde a rede será localizada, quais o equipamentos serão adotados, a que tipo de interferência ela está exporta e quais os finalidades desejadas com a implementação desta rede (25).

A metodologia indicada para esse projeto acontece em sete etapas que seguem uma ordem cronológica pré-estabelecida, conforme o fluxograma da Figura 10.

Figura 10 - Fluxograma para implantação redes mesh



Fonte: (24)

4.3.1 Requisitos Iniciais

De início é muito importante realizar contato com o cliente, buscando compreende todos os objetivos que se pretende alcançar com a implantação da rede *mesh*, analisando quais objetivos são almejados com a implantação e o porquê da escolha da tecnologia. (25)

Para otimização dessa etapa, poderá ser elaborado um questionário vidando obter detalhes técnicos da escalabilidade da rede (disposta para crescimento), tolerância a falhas, desempenho esperado da rede, nível de segurança, quais os aplicativos distribuídos que serão empregados, entre outros. Assim corpo técnico terá as principais características que a rede precisa para atender as necessidades do cliente e minucia características que comprometerão diretamente no desenvolvimento do projeto (25).

4.3.2 Infraestrutura de Rede Presente

A segunda etapa trata da análise da infraestrutura de rede atual no espaço em que a rede *mesh* será implantada, verificando se há alguma tecnologia de comunicação existente, se a mesma é cabeada ou sem fio e se será conectada com a nova rede ou se serão redes individuais, analisando neste último caso, assuntos como interferência entre a rede existente e a nova rede (25).

Constatado uma rede cabeada ou sem fio no local de implementação da rede *mesh,* o gerente do projeto terá requerer junto ao cliente a documentação da mesma para aquisição de informações sobre a infraestrutura atual na rede, funcionalidades e aparelhamentos empregados para esse objetivo (25).

Além disso deve ser apurado a existência de um gateway para o acesso à Internet que caso não tenha, deve ser fornecido e conectado à rede *mesh* para ter o acesso à Internet. A conexão deste *gateway* à rede *mesh* realiza-se empregando normas internacionais de padronização de redes cabeadas, para não existir problemas de conexão (25).

4.3.3 Vistoria para a Implantação de Redes *Mesh*

Nesta etapa tem objetivo de uma análise criteriosa do ambiente onde será implantada a nova rede, subdividindo-se em dois domínios: um abordando da inspeção do ambiente indoor, e o outro do ambiente outdoor. A solução para esta etapa da metodologia consistir em um documento contendo as especificações de ambos, podendo conter detalhes como alturas de prédios, que poderão ser os futuros pontos de acesso *mesh* num ambiente outdoor, tipo de vegetação deste ambiente, que pode influenciar no sinal wireless entre outros. No ambiente indoor as especificações abordam o material que é construído as paredes do recinto, aparelhos elétricos e eletrônicos, móveis e qualquer tipo de artefato presentes no recinto que possam de alguma forma interferir no sinal (24).

4.3.4 Elaboração da Arquitetura da Rede *Mesh*

É indispensável decidir o processo para acesso para a última milha da rede, onde o *backbone wireless* da rede receberá requisições de clientes *wireless*, se receberá exigências de uma rede cabeada existente, se existirá outros clientes *wireless* como celulares e PDAs, e neste último caso, introduzir a instalação de servidores intermediários de borda para o acesso destas diferentes tecnologias (24).

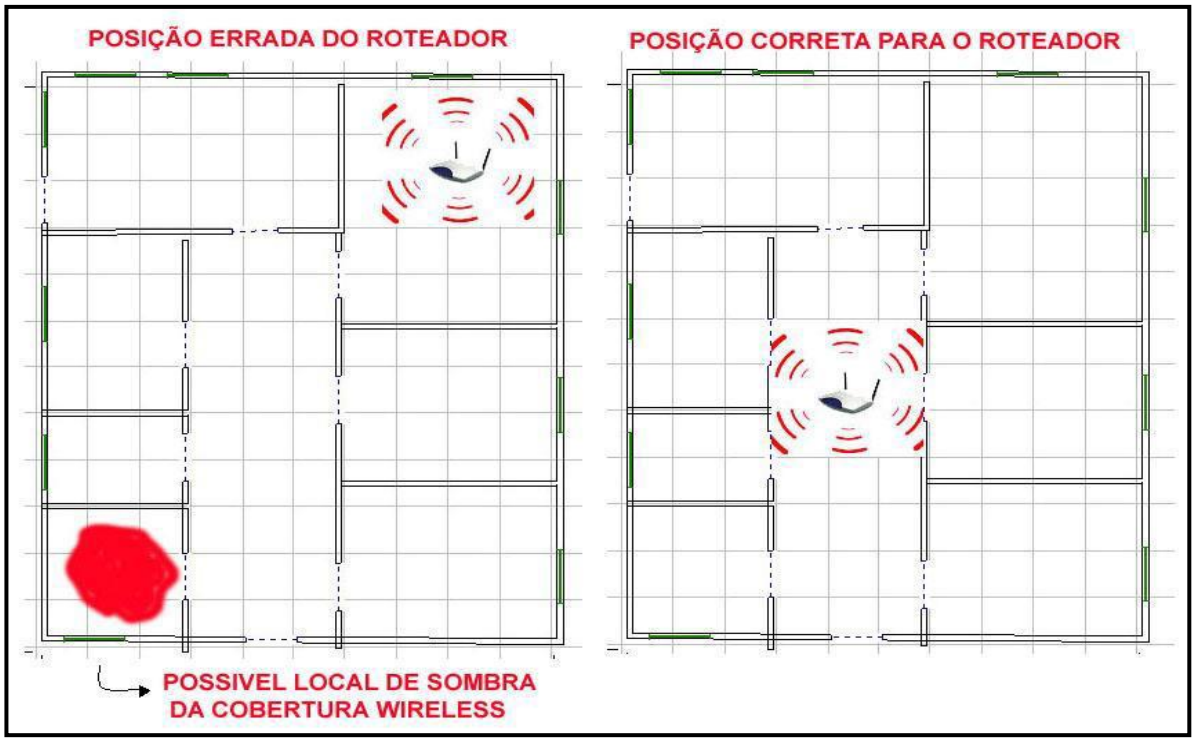
4.3.5 Projeto de Redes *Mesh Indoor e Outdoor*

Para o projeto Indoor, os roteadores *mesh* precisam ser distribuídos de forma análoga no prédio para que o sinal se propague uniformemente em todo o recinto. Inicialmente é fixado provisoriamente o roteador *mesh* piloto da rede *indoor.* O seu local pode ser provisório, pois poderá ser realocado visando de se adaptar as características do ambiente e das interferências que o mesmo pode apresentar ao sinal da rede (25).

O local de instalação deste roteador poderá ser em um corredor próximo ao centro físico do prédio, preferencialmente em lugares altos, para um maior alcance da rede e suavizem a quantidade de barreiras, segundo o exemplo da planta baixa visto na Figura 11. Deve-se evitar vizinhanças com objetos metálicos e materiais elétricos que possam influenciar de forma negativa o sinal. A fórmula para calcular o sinal que chega efetivamente ao receptor é:

- Potência de transmissão + ganho da antena - perda de sinal + ganho da antena receptora (25).

Figura 11 – Posicionamento correto de um roteador



Fonte (25).

Para alocação dos próximos roteadores da rede, poderão ser empregados nesta etapa da metodologia, um *notebook* e um software *site survey (Netstumbler*). O *notebook* deverá ser programado para acessar o roteador *mesh* posicionado no passo acima e através do *software site survey* instalado no mesmo, realizar medições por todo o lugar identificando os pontos para a posicionamento dos outros roteados (26).

Os pontos onde for constatado baixa qualidade do sinal precisam ser apontados como prováveis novos pontos de acesso da rede. A avaliação deverá ser feita de dentro para fora da construção, fazendo com que o sinal se espalhe igualmente por todas as dependências do prédio e aumentando-se assim o raio de covertura da rede com qualidade aceitável. A tabela 5 nos mostra a atenuação em diferentes tipos de obstáculos prediais (26).

Tabela 2 - Atenuação em diferentes tipos de obstáculos prediais.

Material	Atenuação (dB)
Janela de vidro	2
Porta de madeira	3
Parede de gesso	3
Mármore	5
Parede de vidro	6
Parede de tijolo	8
Parede de concreto	10-15

Fonte: (24)

Para ambientes *Outdoor*, se faz necessário determinar os pontos onde serão instalados os roteadores *mesh*. Para esse tipo de espaço, a qualidade do sinal também é o fundamental aspecto para o posicionamento dos roteadores e antenas *mesh*. As altercações em relação ao indoor estão nas características do espaço e no tipo de interferências que ele pode provocar ao sinal da rede. Os roteadores *mesh* devem ser alocados em locais que tenham visadas diretas para os outros roteadores (26).

É imprescindível a definição de fatores como as áreas de acesso para a avaliação do número máximo de clientes que poderão se conectar à rede daquele ambiente, o que minimiza os perdas por uma eventual sobrecarga e aumenta ao máximo o performance da rede e a qualidade do sinal, já que uma grande número de acessos simultâneos a um mesmo roteador pode provocar sobrecarga pela banda dividida, interferindo na qualidade do sinal e inclusive do enlace(26).

Nesta etapa da metodologia é indispensável a definição dos estruturas de segurança que serão empregados na rede, com objetivo de evitar a interceptação de dados que trafegam na rede. Poderá existir a adição de segurança a nível de equipamento de rede ou em nível de aplicativos. Recomenda-se equipamentos que aceitem o padrão 802.11, dominando ou uma criptografia de chave WEP (*Wireless Encryption Protocol*), WPA (*Wi-Fi Protectes Access*) ou WPA2 para que possibilite existir comunicação criptografada (26).

Outros artifícios de segurança podem ser usados como: Filtro de Endereço MAC (*Media Access Point*), autenticação de usuário e senha com o *framework Wifidog e o RADIUS (Remote Authentication Dial-In User Service*) para configuração de diversos níveis de permissão de acesso. Enfim, elabora-se o projeto lógico da rede, com todas as especificações das distâncias, alturas, identificação e locais onde serão implantados os roteadores *mesh* (26).

4.3.6 Infraestrutura de Gerenciamento da Rede

Esta fase depende das necessidades do cliente e da análise dos resultados das fases anteriores. É indicado a utilização de um *software* que possa medir dados, como consumo de banda de rede, taxas de transmissão, etc. Também se faz necessário que o software gerenciador da rede, possa controlar o acesso à rede e também saiba diferenciar os perfis dos usuários por nível de acesso a alguns recursos da rede (24).

Este aplicativo pode ser proprietário ou livre, a escolha de uma solução irá resultar em custos com a compra de um *software* proprietário ou com a obtenção de mão de obra especializada para suporte ao aplicativo livre. O aplicativo deverá realizar o controle de erros, desempenho, segurança, configuração e usuários. O resultados desta fase implicará em uma documentação com um plano de testes de gerenciamento a ser realizado assim que o sistema for implantado (24).

4.3.7 Implantação da Rede *Mesh*

A implantação da rede *mesh* tem que seguir o projeto realizado nas etapas anteriores, em conjunto com o bom emprego do plano de segurança e de gerenciamento da rede se houver algum. A instalação dos pontos de acesso *mesh* no local de aplicação deve ser feita seguindo o projeto lógico da rede elaborado anteriormente, com atenção para a infraestrutura cabeada da rede. Cada roteador deve ser fixado no local definido usando uma caixa hermética como proteção, contra a ação da natureza nos espaço outdoor e protegendo contra prováveis choques e contatos em ambiente indoor (25).

É a exposição minuciosa concisa dos métodos, materiais, técnicas aplicadas e devem ser divulgados com a maior nitidez possível (25).

5 MATERIAIS E MÉTODOS

Adotando como base os dados apresentados nos capítulos anteriores, e com intuito de mostrar na pratica a aplicação, as vantagens e desvantagens do novo protocolo IEEE 802.11ac em relação a norma anterior e às redes cabeadas, para estudo de caso irei elaborar um projeto de atualização na rede sem fio no Campus da FPM (Faculdade Patos de Minas) na Avenida Juscelino Kubitschek, local em que realizo esse curso. Para elaboração desse projeto será seguido os 7 passos descritos no capítulo anterior.

Durante o período do curso, foi notado pelos alunos, professores e demais pessoas que frequentam o local uma qualidade muito baixa da rede sem fio nesse campus, onde é percebido que em vários momentos não é possível acessar a rede sem fio e quando se consegue o acesso nota-se baixa performance dos dispositivos conectados como lentidão e em muitas das vezes não consegue abrir páginas da web, vídeos, aplicativos com *wattsApp*, instagran, servidores de e-mail, etc.

Em conversa direta com professores, coordenador do curso e Técnico de TI, e vistoria no local foi levantado as seguintes informações:

- O link de dados de internet contratada para o campus da AV JK e de 50Mbps, rede cabeada da provedora Algar Telecom;
- Os Ap's existentes são 802.11 b / g do fabricante intelbras modelo WOG 212, os quais são indicados para ambientes residenciais, possuem capacidade e no máximo 20 acessos simultâneos, baixa taxa de transferência de dados (54 Mbps), fatores que afetam diretamente na qualidade do serviço da rede sem fio;
- O campus possui dois Ap's em cada pavimento, o que é insuficiente devido a quantidade de pessoas que utilizam a conexão com a rede sem fio nos pavimentos exceder o limite de acesso simultâneo dos Ap's.
- Foi definido que o projeto será executo levando em conta principalmente a capacidade de alunos por sala e a lotação máxima em ambiente de acesso comum como a praça de alimentação, salas de reuniões e convenções, etc;
- Foi realizado a medição de sinal em todo o campus e verificado que existe vários pontos de sombra e que serão cobertos pela nova rede *mesh*;

- Os laboratórios de informática, salas da administração continuaram com as redes cabeadas existente, devido necessidade de nível de segurança da informação mais elevado (servidor de *firewall*) que a rede sem fio não provê, mais também serão cobertas com as redes sem fio para fornecer sinal aos dispositivos móveis entre outros;
- Os alunos, professores e demais usuários, necessitam de uma rede sem fio mais robusta, que possa atender melhor às necessidades e fornecer conexão em alta performance e com um nível de segurança satisfatório;
- Será mantido toda a infraestrutura existente e realizado adequações para implantação da nova rede sem fio.

O roteador escolhido para implementação foi o *Unif AC mesh 802.11Ac plug & play mesh*, por serem ideais para utilização em campus Estudantis e empresas de pequeno porte e por ter um bom custo benefício, também por suportar tanto usuários na faixa de 2,4 GHz como na faixa de 5 GHz (802.11 a/b/g/n/ac), tem um alcance limitado a 180m e potência de 22 dbm e taxa de transferência de até 300 Mbps para usuários conectados na faixa de 2,4 GHz 802.11n com ganho de antena de 3 dbi, e de até 867 Mbps para usuários trafegando na faixa de 5 GHz 802.11AC com ganho de antena de 4dbi, e suporta 250 acessos simultâneos , cada AP custa por volta de 490,00 que em comparação com um similar que suporta apenas 802.11 a/g/n tem seu valor de mercado por volta de 480,00. A figura 12 abaixo nos mostra as especificações técnicas do roteador utilizado nesse projeto.

Figura 12 - *Data sheet roteador UAP-AC-M*.

UAP-AC-M Specifications

UAP-AC-M	
Dimensions	353 x 46 x 34.4 mm (13.9 x 1.81 x 1.35")
Weight	152 g (5.36 oz) with Antennas
Networking Interface	(1) 10/100/1000 Ethernet Port
Buttons	Reset
Power Method	24V Passive PoE (Pairs 4, 5+; 7, 8 Return); 802.3af Alternative A (Pairs 1, 2+; 3, 6 Return) (Supported Voltage Range: 44 to 57VDC)
Power Supply	24V, 0.5A Gigabit PoE Adapter*
Power Save	Supported
Maximum Power Consumption	8.5W
Maximum TX Power 2.4 GHz 5 GHz	 20 dBm 20 dBm
Antennas 2.4 GHz 5 GHz	(2) External Dual-Band Omni Antennas 3 dBi 4 dBi
Wi-Fi Standards	802.11 a/b/g/n/ac
Wireless Security	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
BSSID	Up to Four per Radio
Mounting	Wall/Pole/Fast-Mount (Kits Included)
Operating Temperature	-30 to 70° C (-22 to 158° F)
Operating Humidity	5 to 95% Noncondensing
Certifications	CE, FCC, IC

* Only the single-pack of the UAP-AC-M includes a PoE adapter.

Advanced Traffic Management	
VLAN	802.1Q
Advanced QoS	Per-User Rate Limiting
Guest Traffic Isolation	Supported
WMM	Voice, Video, Best Effort, and Background
Concurrent Clients	250+

Supported Data Rates (Mbps)	
Standard	Data Rates
802.11ac	6.5 Mbps to 867 Mbps (MCS0 - MCS9 NSS1/2, VHT 20/40/80)
802.11n	6.5 Mbps to 300 Mbps (MCS0 - MCS15, HT 20/40)
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	1, 2, 5.5, 11 Mbps

Fonte: (27)

A distribuição dos roteadores foi realizada levando em consideração a atenuação das paredes de tijolos (8 dB) e a quantidade total de usuários que cada ambiente suporta. Para esse projeto será considerado que entre 50% da capacidade total de usuários podem se conectar ao mesmo tempo à rede sem fio (28), na figura 13 (projeto do pavimento térreo) podemos perceber que o alcance do sinal dos Ap's se sobrepoem, isso ocorre devido ao elevado numero de usuários, que demandam um múmero maior de AP's. Sendo assim, se faz necessário um bom planejamento de reuso de frequência, com intuito de minimizar as interferências entre os AP's, tal planejamento não é, entretanto, o objetivo deste trabalho. O quadro 4 abaixo nos mostra o número máximo de canais por faixa de frequência.

Quadro 4 - Número Máximo de Canais por Faixa de Frequências

FAIXA DE FREQUÊNCIAS (MHz)	NÚMERO DE CANAIS	
	20MHz	40MHz
2400 - 2483	3 (3)	1
5150 - 5350	8 (8)	3
5470 - 5725	11 (8)	5 (3)
5725 - 5850	5 (4)	2

Fonte: (27)

No primeiro pavimento foi projetado 4 *Acess points*, para atender um total estimado de 1360 pessoas (capacidade total) que poderão ser alunos, professores, funcionários da instituição e visitantes. Para chega a um número de pessoas que acessam cada AP ao mesmo tempo basta dividir o total de pessoas por 4 aparelhos e depois dividir por 2 (50% de acesso simultâneo), chegando a uma estimativa de 182 pessoas para cada AP. Com base nessa estimativa foi designada uma margem para resguardar alguma eventualidade de concentração de pessoas em um determinado local de 68 pessoas, levando em consideração o *Datasheet* do AP utilizado, que suporta até 250 acessos simultâneos. Esse total de 1360 pessoas estão divididas da seguinte forma: 600 pessoas nas salas de aula do corredor principal, recepção e área externa em frente a recepção, 100 pessoas na praça de alimentação, 360 pessoas nas salas de aula do corredor secundário e 200 pessoas

nos 4 laboratórios, além de 200 pessoas na sala do auditório. Os AP’s serão então distribuídos como descrito a seguir:

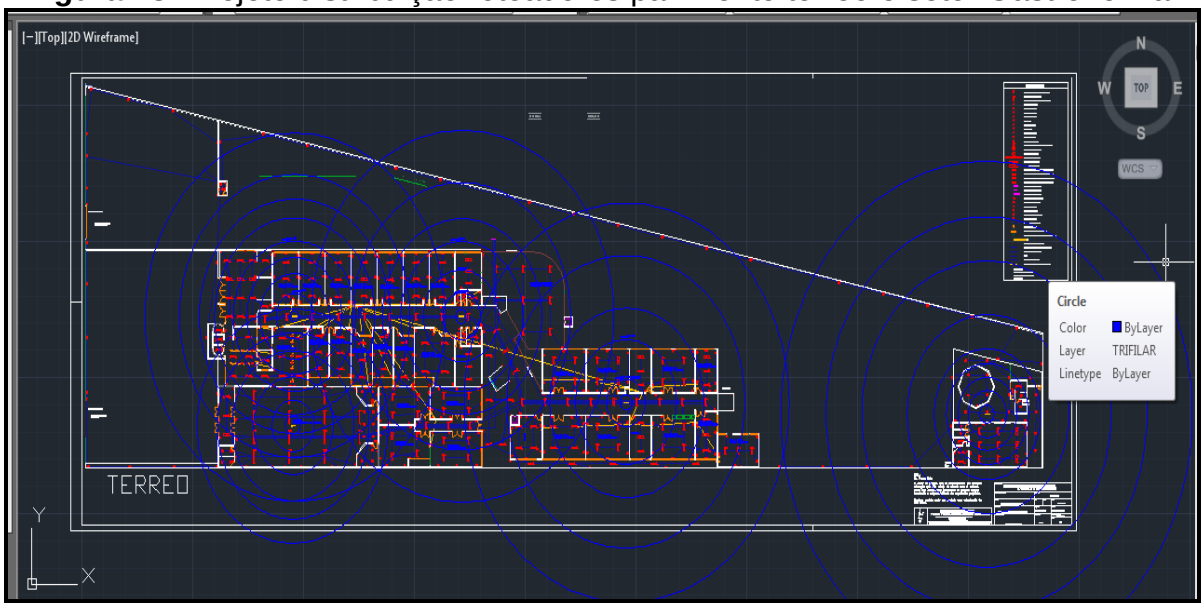
No corredor principal serão instalados 2 AP’s fixos na eletrocalha a 2,5 metros de altura, um posicionado na entrada do corredor próximo à recepção, com objetivo de fornecer conexão aos usuários que se encontram nas proximidades da parte externa em frente à recepção e mais ou menos 50% dos alunos nas salas de aula do corredor principal. Outro no fim do corredor principal, que irá atender a outra metade dos alunos nas salas de aula do corredor principal e às pessoas presentes na praça de alimentação.

Um terceiro roteador *wireless* tambem será instalado na eletrocalha à 2,5 metros de altura, e posicionado no centro do corredor secundário, para atender os alunos das salas de aula desse corredor e dos laboratórios.

O quarto AP será instalado na sala do auditório com capacidade para até 200 pessoas, em local a ser definido devido ao local encontrar-se em reforma. Na sala do auditório foi designado um roteador individual para o ambiente, porém como o ambiente é pouco utilizado, o mesmo irá ajudar na cobertura das salas paralelas.

Também foi planejado um roteador para atender ao setor do curso de Gastronomia, localizado nos fundos do terreno, por ser afastado dos AP’s planejados para o pavimento térreo - com as perdas causadas pelas paredes o mesmo se faz necessário. Como o setor do curso de Gastronomia tem capacidade para menos alunos (100 no total) o roteador poderá ser instalado em um abrigo na parte externa da alvenaria, para prover cobertura também na área externa entre o pavimento térreo e o setor do curso de culinária, a figura 13 nos mostra a distribuição dos roteadores *wireless* no pavimento térreo e setor do curso de Gastronomia.

Figura 13- Projeto distribuição roteadores pavimento térreo e setor Gastronomia.



Fonte: autoria própria.

Para o primeiro pavimento foi projetado 3 roteadores wireless, todos instalados na eletro calha existente a 2,5 metros de altura para atender um total estimado de 1060 pessoas divididas em 380 pessoas das salas administrativas e alunos das salas de aulas no corredor principal, mais 100 pessoas na biblioteca, mais 260 pessoas nas salas do corredor secundário e 320 pessoas nas 4 salas de aula com acesso por um pequeno corredor localizado em frente ao corredor secundário próximo às escadas. Para estimar o número de acessos simultâneos para cada AP a conta é similar a realizado para o primeiro pavimento (((1060 / 3) /2) =176,66), também com margem de segurança para o caso de agrupamento de pessoas em um mesmo local.

No corredor principal seram instalados 2 AP’s fi, um posicionado na entrada do corredor em frente às salas da ADM, com objetivo de fornecer conexão aos usuários que se encontram nas salas da adminstração e mais ou menos 50% dos alunos nas salas de aula do corredor principal. Outro no fim do corredor principal, que irá atender a outra metade dos alumos nas salas de aula do corredor principal e as pessoas presentes na biblioteca.

Na região central corredor secundário está projetado mais um roteador wireless, com objetivo de prover cobertura para os usuários das salas presentes nesse corredor e mais 4 salas corredor pequeno localizado em frente ao corredor

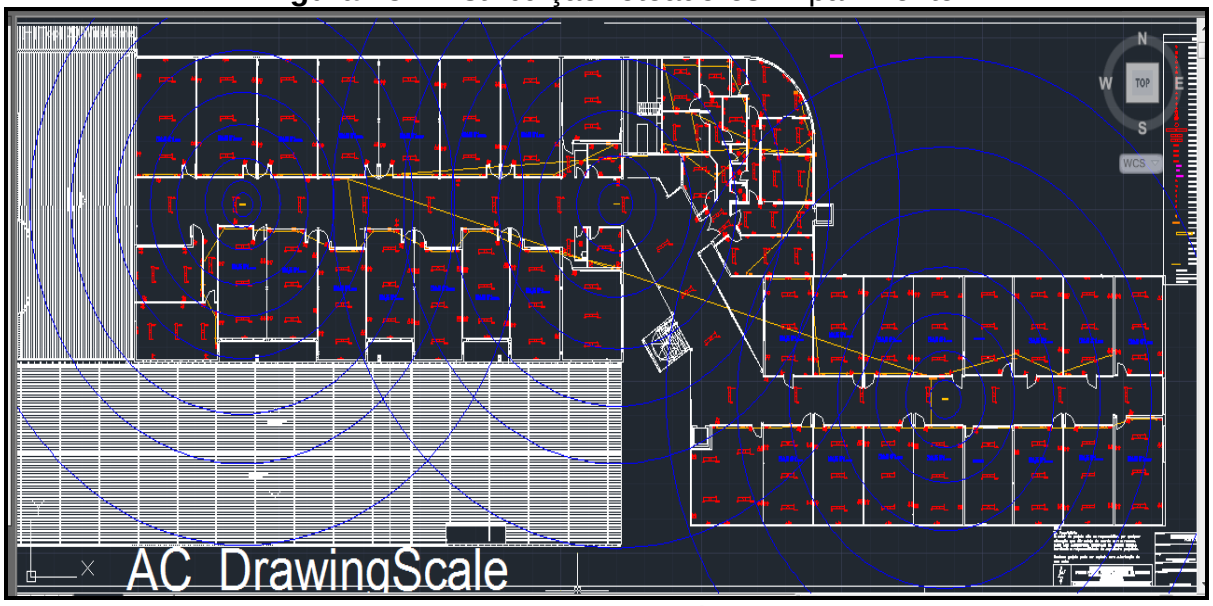
secundário próximo às escadas. A figura 14 nos mostra a distribuição dos roteadores no primeiro pavimento.

Figura 14 - Distribuição roteadores 1º pavimento.

Fonte: autoria própria.

No segundo pavimento também foi projetado 3 roteadores fixados na eletro calha a 2,5 metros de altura, com distribuição similar ao primeiro pavimento, para atender um total estimado de 1030 pessoas, para calcular o número de acessos simultâneos para cada AP basta realizar a conta feita para os demais pavimentos ((1030/3) /2 = 171). A figura 15 nos mostra a distribuição dos pontos de acesso no segundo pavimento.

Figura 15 - Distribuição roteadores 2º pavimento



Fonte: autoria própria.

6 RESULTADOS E DISCUSSÃO

Com a implementação do projeto apresentado anteriormente, os problemas referentes à conexão e acesso à rede serão resolvidos para acessos na faixa de 2,4 GHz com o 802.11n, além de acrescentar mais uma faixa de frequência a de 5GHz no 802.11ac que proporciona uma experiência ainda melhor aos usuários com aparelhos que suportam essa frequência no 802.11ac, proporcionado elevadas taxas de transferência, haja visto que a rede *wireless* existente é limitada a 54 Mbps e 20 acessos simultâneos no padrão 802.11 a/g, e que em contrapartida a nova rede suporta até 250 acessos simultâneos e taxas de transferência de 6.5 a 300 Mbps no padrão 802.11n e 6.5 a 867 Mbps no padrão 802.11 ac. Sem contar que a rede ficará robusta e com escalabilidade, suportando expansão e ficando preparada para o futuro, uma vez que a maioria dos aparelhos fabricados nos dias de hoje já contam com o protocolo 802.11ac e a tendência é que a cada dia que passa os protocolos antigos fiquem obsoletos com baixíssima ou nenhuma utilização.

Como nesse projeto optou-se pela implementação da rede *mesh*, o usuário irá perceber também que não haverá mais quedas na conexão ao se deslocar da área de cobertura de um AP para a área de outro AP, pois na rede *mesh* os AP's ou nós atuam em conjunto para distribuir um único sinal de internet em múltiplos pontos de um mesmo ambiente e em caso de uma ampliação no número de alunos basta inserir mais nós à rede.

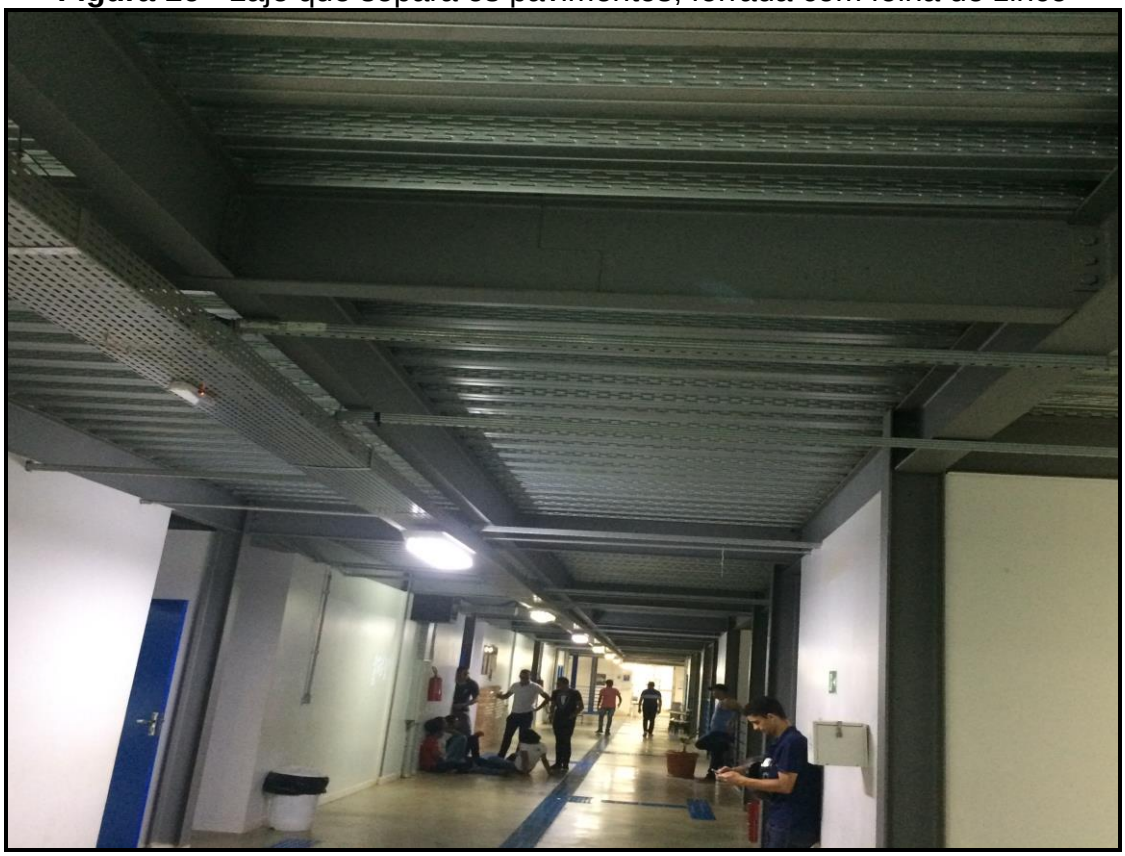
Vale ressaltar que a velocidade da conexão percebida pelos usuários depende diretamente do *link* de dados disponibilizado pela instituição para a rede sem fio e da quantidade de usuários que estão compartilhando o *link* ao mesmo tempo.

Não será necessário a substituição dos cabos ethernet da rede existente que são da categoria 6 (cat. 6) que suportam velocidades 10/100/1000 Mbps e são resistentes a interferência externa.

A infraestrutura da rede existente como os *racks* e roteadores poderão ser aproveitados, o que irá reduzir muito o investimento a ser feito; pelo menos um dos roteadores existentes deve possuir porta ethernet de1Gbps para que se possa explorar ao máximo as vantagens dos roteadores *Unif AC mesh 802.11Ac plug & play mesh.*

Também vale ressaltar que os roteadores dos pavimentos não irão causar interferência nos roteadores dos outros pavimentos devido à característica do roteador que propaga o sinal com menor intensidade na vertical e a característica construtiva da laje que separa os pavimentos que são de concreto e que toda laje é forrada por uma folha de zinco que reflete o sinal não permitindo a penetração do sinal. Como mostra a figura 16 a seguir.

Figura 16 - Laje que separa os pavimentos, forrada com folha de zinco



Fonte: (Autoria própria)

No que se refere a custo da implantação da rede, segue abaixo um quadro comparativo.

Quadro 5 - Custos com implantação redes wireless

	Valor de mercado (R$)			
Quantidade Material / aparelho	Rede atual AP 802.11 a/ g	Utilizando AP que suportam até 802.11n	Utilizando AP que suportam até 802.11ac	Total
06 unidades Intelbras WOG 212 12dbi	350,00	n/a	n/a	2100,00
11 unidades *Unif AC mesh 802.11n*	n/a	480,00	n/a	5280,00
11unidades *Unif AC mesh 802.11Ac*			490,00	5390,00
Cabos cat. 4 1caixa com 305 metros	1 x 150,00	n/a	n/a	150,00
Cabos cat. 6 caixa com 305 metros	n/a	1x 780,00	1 x 780	780,00
Conectores RJ 45 cat. 4/5 pct com 100 unidades	2 x 20			40,00
Conectores RJ 45 cat. 6 blindado, pct com 50 unidades	n/a	2 x 95,00	2 x 95	190,00
Custo com mão de obra para implantação rede atual	6 x 100			600,00

Custos com Mão de obra para IMP rede mesh 802.11n ou 802.11ac		11 x 100	1100,00
Custo total rede existente	2100 + 150 + 20 + 600		2870,00
Custo total com rede até 802.11n	5280 + 780 + 190 + 1100		7350,00
Custo total com rede até 802.11ac	5390 + 780 + 190 + 1100		7460,00

Fonte: (Autoria própria)

Os resultados obtidos no Quadro 5 nos mostram que os custos da rede existente são bem menores que os custos para a implementação da rede mesh. Também, nos leva à conclusão de que a rede atual foi mal planejada e não atende às necessidades dos usuários da rede na instituição e que a implantação desse projeto irá resolver os problemas existentes e garantir que em caso de novas demandas o investimento será pequeno, apenas aumentando o número de pontos de acesso à rede *mesh*.

7 CONSIDERAÇÕES FINAIS

Devido ao crescimento significativo na quantidade de usuários conectados a redes *wireless* com seus dispositivos móveis e à demanda por serviços que solicitam taxas de dados mais rápidas, grupos de tarefa buscam criar soluções que assegurem QoS (Qualidade de serviço), assim como, redes que aceitem cada vez múltiplos acessos. O padrão IEEE 802.11ac traz um aumento expressivo da taxa de transmissão de dados com canais mais amplos (até 160 MHz), modulação mais forte com quantidade maior de fluxos espaciais, o que solicita um disposição de antena máximo. Além disso, um único AP pode transmitir vários quadros a usuários diferentes ao mesmo tempo. MU-MIMO é praticado em conjunto com *beamforming*, que focaliza a potência da antena na direção do receptor e não influenciando nas transmissões paralelas.

7.1 Conclusão do Projeto

O presente trabalho tem como objetivo a análise de comparação entre o padrão IEEE 802.11ac com relação às normas anteriores e às redes cabeadas.

Para um melhor entendimento foi realizado um projeto de modernização na rede sem fio da FPM campus JK, que possui roteadores sem fio que utilizam o padrão 802.11a/g os quais são ideais para ambientes residências e não são indicados para locais com concentração de pessoas como escolas, faculdades e pequenas empresas.

A nova rede projetada além de garantir o acesso aos usuários com aparelhos que empregam os protocolos anteriores, fornecem acesso aos usuários das normas mais novas 802.11n e 802.11ac.

Os estudos apresentados nos mostram que com a implementação desse projeto os usuários que utilizam aparelhos com suporte para 802.11n vão sentir uma enorme melhora na velocidade da conexão, e os problemas de acessos simultâneos resolvidos com o emprego da rede mesh. Já os usuários com aparelhos com suporte para 802.11ac terão uma experiência ainda melhor, devido velocidade da conexão ser de mais que o dobro em comparação com o 802.11n no ponto de acesso projetado.

Sendo assim, conclui-se que a norma IEEE802.11ac traz grandes vantagens com relação às normas anteriores principalmente com relação a performance e como o custo de um AP 802.11n e quase o mesmo de um AP 802.11ac não se justifica a sua não utilização, uma vez que a tendência é de um aumento continuo na utilização de altas velocidades em conexões de dados pelos usuários das redes sem fio.

Com relação às redes cabeada as redes sem fio são muito viáveis em locais com alta densidade de pessoas, pois fornece conexão à internet com altas taxas de transferência e com um nível de segurança aceitável, gerando uma grande economia de cabos que por sua vez causam muita poluição visual, sem contar com a contribuição com a sustentabilidade uma vez que os cabos ethernet são fabricados com matéria prima mão renovável.

Já em ambientes como administração, escritórios, laboratórios, a utilização da rede sem fio se justifica somente para aparelhos móveis celulares, notebooks, tabletes (aparelhos de uso pessoal), mais quando se trata de aparelhos com acesso à rede interna ou coorporativa os níveis de segurança da rede sem fio não são confiáveis, tornando a sua utilização inviável, sendo necessário a utilização de rede cabeada com servidores de *firewall* mais robustos.

7.2 Trabalhos Futuros

Uma das principais inovações apresentadas com o padrão IEEE 802.11ac ainda não foi testada precisamente por solicitar múltiplos fluxos espaciais e técnica MU-MIMO. Todas as experiências foram realizadas com somente um usuário e um fluxo espacial.

Para um julgamento eficaz do padrão, torna-se necessário sua implementação em espaço físico real, com objetivo de comparar os resultados empíricos com os computacionais e confrontar as similaridades e oposições.

REFERÊNCIAS

1 - O QUE É IEEE. Disponível em: <http://sites.ieee.org/sb-ufrgs/o_que_e_ieee/>. Acesso em: 25 mar. 2017.

2 - WI-FI. Disponível em: <https://www.tecmundo.com.br/tecnologia/113811-10-tecnologias-completam-20-anos-vida-2017-video.htm>. Acesso em: 25 mar. 2017.

3 - **IEEE82.11AC:** an anlysis of the standard. Online: Copyrigt, 2013. 500 p.

4 - SYSTEMS, Cisco. **Autenticação do Multi-domínio do IEEE 802.1X no exemplo de configuração dos switch de configuração fixa da camada 3 do Cisco catalyst.** 2007. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/lan-switching/8021x/98523-8021x-cat-layer3.html>. Acesso em: 14 jun. 2017.

5 - FONSECA, Willian. **Wireless: diferenças entre as gerações b, g e n.** 2009. Disponível em: <https://www.tecmundo.com.br/internet/2764-wireless-diferencas-entre-as-geracoes-b-g-e-n.htm>. Acesso em: 15 jun. 2017.

6 - WIRELESS: What Is 802.11n?. What Is 802.11n?. 2017. 15:56. Disponível em: <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103>. Acesso em: 19 jun. 2017.

7 – LEOPEDRINI, Jonh. **O que é MIMO?** 2011. Disponível em: <http://www.telecomhall.com/br/o-que-e-mimo.aspx>. Acesso em: 28 jun. 2017.

8 - GEIER, Eric. **Conheça “beamforming”, a tecnologia que promete acelerar o Wi-Fi.** 2013. Disponível em: <http://pcworld.com.br/noticias/2013/11/21/conheca-201cbeamforming201d-a-tecnologia-que-promete-acelerar-o-wi-fi/>. Acesso em: 30 jun. 2017.

9 - BEVILACQUA, Argemiro. **Detcção e mitigação de anomalia na camada mac em redes IEEE 802.11.** 2015. Disponível em: <http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/handle/tede/561>. Acesso em: 20 jul. 2017.

10 - MAGNO, Ricardo; RICHARTE, Diogo; GONSALVES, Daniel. **Como Evoluiram as normas wi-fi IEEE 802.11.** 2013. Disponível em: <http://paginas.fe.up.pt/~projfeup/submit_13_14/uploads/relat_1MIEEC01_3.pdf>. Acesso em: 10 jul. 2017.

11 - DIGITAL, Palpite. **Wi-Fi 802.11 a/b/e/g/n/r/ac/ad. Afinal, o que significa isso?** 2017. Disponível em: <https://www.palpitedigital.com/wi-fi-802-11-abgnacad-afinal-que-significa-isso/>. Acesso em: 23 jun. 2017.

12 - KELLY, Viviane. **NEW IEEE 802.11ac™ SPECIFICATION DRIVEN BY EVOLVING MARKET NEED FOR HIGHER, MULTI-USER THROUGHPUT IN:** 2014 INTERNATIONAL CES, LAS VEGAS, USA, 7 January 2014. 2014. Disponível em: <http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html>. Acesso em: 05 jun. 2017.

13 - LOBO, Fernando. **O novo padrão 802.11ac e as redes corporativas.** 2014. Disponível em: <http://cio.com.br/tecnologia/2014/05/06/o-novo-padrao-802-11ac-e-as-redes-corporativas/>. Acesso em: 20 jun. 2017.

14 - MACHADO, Willian Lopes. **SIMULAÇÃO DA CAMADA FÍSICA DO PROTOCOLO IEEE 802.11AC UTILIZANDO A FERRAMENTA MATLAB.** 2015. Disponível em: <http://bdm.unb.br/bitstream/10483/15119/1/2015_WillianLopesMachado.pdf>. Acesso em: 20 jul. 2017.

15 - JORDÃO, Fábio. **Wi-Fi 802.11ac: as redes sem fio de alta velocidade vêm aí.** 2012. Disponível em: <https://www.tecmundo.com.br/wi-fi/23964-wi-fi-802-11ac-as-redes-sem-fio-de-alta-velocidade-vem-ai.htm>. Acesso em: 30 jul. 2017.

16 - SYSTEMS, Cisco. **802.11ac: The Fifth Generation of Wi-Fi Technical White Paper.** 2017. Disponível em: <https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html#_Toc383047840>. Acesso em: 17 set. 2017.

17 - BARION, Rogério. **IEEE 802.11 ad – o padrão Wi-Fi revoluciuonário:** O padrão IEEE 802.11 ad. 2016. Disponível em: <http://www.entelco.com.br/blog/ieee-802-11-ad-o-padrao-wi-fi-revoluciuonario/>. Acesso em: 21 ago. 2017.

18 - BORGES, Adriano Cesar Braga; AZEVEDO, Fabrício Gonçalves de; MARQUS, Fernando Matheus. **Problemas de segurança na internet enfrentados pelas redes sem fio.** 2010. Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2668/2623>. Acesso em: 14 ago. 2017.

19 - SERENO, José Humberto Laranjeira. **Tendencias de impletanção e segurança em redes wireless organizacionais.** 2015. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/10450/1/Dissertação MSIO JSereno - 130313008.pdf>. Acesso em: 05 jul. 2017.

20 - SERVICES, Airtel Telemidia. **Simple steps to secure your Wi-Fi Network.** 2008. Disponível em: <http://www.airtel.in/applications/genericlead/wifi/images/wifisecure.pdf>. Acesso em: 09 set. 2017.

21 - LASHKARI, Arash Habibi. **A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i).** 2009. Disponível em: <http://nslab.kaist.ac.kr/courses/2012/test/paperlist/2-7.pdf>. Acesso em: 26 set. 2017.

22 - ABOBA, B.; SIMON, D.. **Extensible Authentication Protocol (EAP) Key Management Framework.** 2008. Disponível em: <https://tools.ietf.org/html/rfc5247>. Acesso em: 03 out. 2017.

23 - IEEE Standard for Information technology. IEEE Standards: Part 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancement, 2004.

24 - ALVES, Paulo. **O que é rede mesh?** 2016. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/10/o-que-e-rede-mesh-conheca-tecnologia-que-melhora-o-wi-fi.html>. Acesso em: 09 out. 2017.

25 - AFFILIATES, Cisco And/or Its. **For high-density client environments in higher education.** 2017. Disponível em: <https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/cisco_wlan_design_guide.pdf>. Acesso em: 05 out. 2017.

26 - ROCHA, João Wilson Vieira. **Redes WLAN de Alta Velocidade II: Recomendações Aplicáveis.** 2016. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeswlanII/default.asp>. Acesso em: 07 out. 2017.

27 - TECHNOLOGY, High-performance Wide-area Wi-fi With Unifi ® Mesh. **802.11AC AP with Plug & Play Mesh.** 2017. Disponível em: <http://dl-origin.ubnt.com/datasheets/unifi/UniFi_AC_Mesh_DS.pdf>. Acesso em: 13 out. 2017.

28 - VAVER, Roberto Torres; SOUZA, Alexandre José Barbiere de. **ANALYSIS OF THE IEEE 802.11AC PROTOCOL USE IN HIGH DENSITY WLAN NETWORKS – CASE STUDY OF A STADIUM.** 2016. Disponível em: <https://www.researchgate.net/publication/305793770_Analysis_of_the_IEEE_80211ac_protocol_use_in_high_density_WLAN_networks_Case_Study_of_a_Stadium>. Acesso em: 19 out. 2017.

ANEXOS