

unesp UNIVERSIDADE ESTADUAL PAULISTA

“JÚLIO DE MESQUITA FILHO”

CAMPUS DE GUARATINGUETÁ

ALEXANDER KAMEYAMA

**ESTUDO DA TECNOLOGIA DE ACESSO WI-FI E SUAS APLICAÇÕES EM
AMBIENTES INDOOR E OUTDOOR**

Guaratinguetá

2013

ALEXANDER KAMEYAMA

ESTUDO DA TECNOLOGIA DE ACESSO WI-FI E SUAS APLICAÇÕES EM
AMBIENTES INDOOR E OUTDOOR

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Elétrica da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Elétrica.

Orientador: Prof. Dr. José Feliciano Adami

Guaratinguetá

2013

K15e	Kameyama, Alexander Estudo da Tecnologia de Acesso Wi-Fi e suas aplicações em Ambientes Indoor e Outdoor / Alexander Kameyama – Guaratinguetá : [s.n], 2013. 153 f : il. Bibliografia: f. 110-112 Trabalho de Graduação em Engenharia Elétrica – Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2013. Orientador: Prof. Dr. José Feliciano Adami 1. Sistemas de comunicação sem fio 2. LANs sem fio I. Título CDU 681.3.06
------	---

**ESTUDO DA TECNOLOGIA WI-FI E SUAS APLICAÇÕES EM AMBIENTES
INDOOR E OUTDOOR**

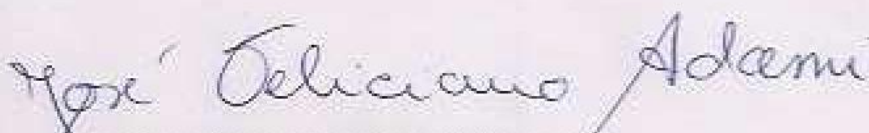
ALEXANDER KAMEYAMA

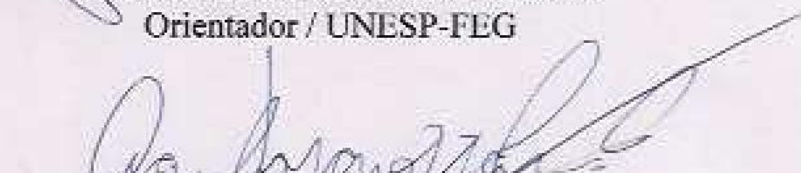
**ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO
COMO PARTE DO REQUISITO PARA A OBTENÇÃO DO
DIPLOMA DE GRADUADO EM ENGENHARIA ELÉTRICA**

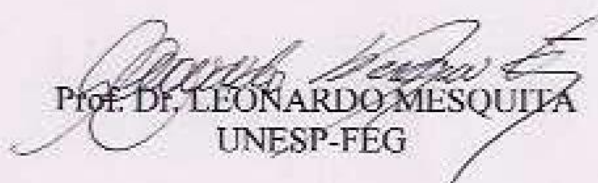
**APROVADO EM SUA FORMA FINAL PELO CONSELHO DE
CURSO DE GRADUAÇÃO EM ENGENHARIA ELÉTRICA**

Prof. Dr. LEONARDO MESQUITA
Coordenador

BANCA EXAMINADORA:


Prof. Dr. JOSÉ FELICIANO ADAMI
Orientador / UNESP-FEG


Prof. Dr. AGNELO MAROTTA CASSULA
UNESP-FEG


Prof. Dr. LEONARDO MESQUITA
UNESP-FEG

Dezembro de 2013

DADOS CURRICULARES

ALEXANDER KAMEYAMA

NASCIMENTO	16.06.1990 – SÃO PAULO / SP
FILIAÇÃO	Jackson Naoki Kameyama Elizabeth Mitiko Watanabe Kameyama
2008/2013	Curso de Graduação em Engenharia Elétrica Universidade Estadual Paulista – Faculdade de Engenharia de Guaratinguetá

de modo especial, aos meus pais Jackson Naoki Kameyama e Elizabeth Mitiko Watanabe Kameyama, que sempre me apoiaram nesta jornada.

AGRADECIMENTOS

Agradeço aos meus pais, *Jackson e Elizabeth*, que sempre me apoiaram e não mediram esforços para colaborar com tudo o que foi necessário para que eu pudesse completar esta etapa da minha vida,

ao meu orientador *Prof. Dr. José Feliciano Adami* que me incentivou e auxiliou na elaboração deste trabalho,

a minha namorada *Paloma* pelo carinho e apoio durante todos esses anos,

aos meus amigos, pelas experiências vividas, momentos de alegria e auxílio nos estudos.

KAMEYAMA, A. Estudo da tecnologia de acesso Wi-Fi e suas aplicações em ambientes indoor e outdoor. 2013. 153 pg. Trabalho de Graduação (Graduação em Engenharia Elétrica) – Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, Guaratinguetá, 2013.

RESUMO

A comunicação sem fio, hoje, é um recurso que já se tornou imprescindível para muitas pessoas no mundo inteiro. Através deste recurso é possível tornar o processo de comunicação muito mais eficiente, fazendo com que as pessoas tenham acesso a informações de maneira muito mais rápida independentemente de onde estejam.

A constante evolução das tecnologias de comunicação permite o desenvolvimento de novas aplicações e serviços antes inimagináveis. Esta nova gama de possibilidades permite uma maior mobilidade e eficiência por parte dos usuários finais e auxilia as provedoras de serviços e operadoras de telefonia móvel a complementarem a qualidade de serviços oferecidos por elas.

Este trabalho de graduação apresenta os princípios da comunicação sem fio e a tecnologia Wi-Fi, bem como suas aplicações mais atuais, abordando desde os conceitos básicos de redes de computadores até os procedimentos de planejamento de uma rede sem fio, passando por conceitos de rádio frequência, antenas, padrões, órgãos reguladores, equipamentos de redes de computadores, protocolos e monitoramento da rede.

PALAVRAS-CHAVE: Wi-Fi, 802.11, Site Survey, Offload, RF.

KAMEYAMA, A. Wi-Fi Access Technology study and its application in indoor and outdoor environments. 2013. 153 pg. Graduate Work (Graduation in Electrical Engineering) – Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, Guaratinguetá, 2013.

ABSTRACT

Wireless communications is a feature that has become indispensable for many people in the whole world. Through this feature, communication process can become much more efficient, allowing people to access information much more quickly wherever they are.

The constant evolution of communication technologies allows the development of new unthinkable applications and services. This new range of possibilities brings greater mobility and efficiency for final users and also helps service providers and carriers to improve the quality of services offered by them.

This study presents the principles of wireless communication and the Wi-Fi technology as well as its most modern applications, covering from the basics of computer networks to the procedures of planning a wireless network, concepts of radio frequency, antennas, patterns, regulatory agencies, network equipment, protocols and network monitoring.

KEYWORDS: Wi-Fi, 802.11, Site Survey, Offload, RF.

LISTA DE FIGURAS

Figura 1 - Posse de dispositivos por adultos americanos	25
Figura 2 - Logo Wi-Fi <i>Certified</i>	28
Figura 3 - Espectro Eletromagnético	29
Figura 4 - Canais da banda de 2,4 GHz.....	31
Figura 5 - Modulação AM.....	33
Figura 6 – Modulação FM.....	33
Figura 7 - Saltos de canal com FHSS	35
Figura 8 - Transmissão de sequência de chip	37
Figura 9 - Resistência a interferência	38
<i>Figura 10 - Phase Shift Keying</i>	39
Figura 11 - Diagrama de Constelações BPSK.....	40
Figura 12 - Diagrama de Constelações QPSK.....	41
Figura 13 - Códigos Comeplementares	44
Figura 14 - Subportadora e Sinal OFDM	48
Figura 15 - Duração do símbolo OFDM	49
Figura 16 - Diagrama de Constelações 16 QAM	51
Figura 17 - Diagrama de Constelações 64 QAM	52
Figura 18 - <i>Decision Tree</i>	55
Figura 19 - <i>Decision Tree</i> para decodificação.....	57
Figura 20 - <i>Independent Basic Service Set</i>	67
Figura 21 - Representação de um <i>Access Point</i> em uma topologia.....	68
Figura 22 - <i>Basic Service Area (BSA)</i>	68
Figura 23 - <i>Extended Service Set (ESS)</i>	68
Figura 24 - Exemplo de topologia de uma rede coporativa.....	70
Figura 25 - Modelos de <i>Access Points</i>	72
Figura 26 - Modelos de controladoras <i>wireless</i>	74
Figura 27 - Tela de gerenciamento de uma WLC	75
Figura 28 - Planta do 6º Andar.....	76
Figura 29 - Planta do 7º Andar.....	77

Figura 30 - Valores de atenuação padrão do <i>Air Magnet</i>	78
Figura 31 - Predição do 6º andar	79
Figura 32 - Predição do 7º andar	80
Figura 33 - Cisco <i>Access Point</i> 3502	81
Figura 34 - Interferência de canais	82
Figura 35 - Padrão de radiação de sinal	83
Figura 36 - Configuração do AP no <i>Air Magnet</i>	84
Figura 37 - Propagação do sinal em 2,4 GHz e 5,0 GHz	85
Figura 38 - Barra de sinal em dBm	86
Figura 39 - Sinal do AP com corte em -67 dBm em 2,4 GHz e 5,0 GHz	87
Figura 40 - Propagação do sinal com dois <i>Access Points</i> e corte em -67 dBm	89
Figura 41 - Propagação do sinal do 7º andar em 5,0 GHz e corte em -67 dBm	90
Figura 42 - Propagação do sinal do 7º andar em 5,0 GHz com três APs	91
Figura 43 - Propagação do sinal entre andares	92
Figura 44 - Data rate em relação a distância	93
Figura 45 - Simulação da altura de instalação com um tripé	95
Figura 46 - Propagação do sinal do AP 1 do 7º andar em 5,0 GHz e corte em -67 dBm	95
Figura 47 - Propagação do sinal do AP 2 do 7º andar em 5,0 GHz e corte em -67 dBm	96
Figura 48 - Propagação do sinal do AP 3 do 7º andar em 5,0 GHz e corte em -67 dBm	96
Figura 49 - Combinação de sinais no 7º andar em 5,0 GHz e corte em -67 dBm	97
Figura 50 - <i>Access Point</i> instalado no teto	98
Figura 51 - Topologia do projeto	100
Figura 52 - Quantidade de chipsets Wi-Fi vendidos nos últimos anos	103
Figura 53 - <i>Survey outdoor</i> realizado com o <i>Air Magnet</i>	104
Figura 54 - Previsão de tráfego de dados pelo Wi-Fi	108
Figura 55 - Evolução dos data rates dos padrões Wi-Fi	109
Figura 56 - Topologia em barramento	114
Figura 57 - Topologia em anel	115
Figura 58 - Topologia em estrela	115
Figura 59 - Topologia <i>Mesh</i>	116
Figura 60 - <i>Metropolitan Area Network</i>	117

Figura 61 - <i>Wide Area Network</i>	118
Figura 62 - Processo de Encapsulamento do Modelo OSI.....	127
Figura 63 - Processo de Desencapsulamento do Modelo OSI.....	128
Figura 64 - Composição de um endereço IP.....	130
Figura 65 - Classificação dos Endereços IP	131
Figura 66 - Modelos de roteadores	132
Figura 67 - Representação de um Roteador em uma Topologia	133
Figura 68 - Número de Hosts Disponíveis	136
Figura 69 - <i>Unicast, Broadcast e Multicast</i>	137
Figura 70 - Topologia em estrela com um Hub.....	139
Figura 71 - Switches	140
Figura 72 - Representação de um Switch em uma topologia	141
Figura 73 - Composição do endereço MAC.....	142
Figura 74 - Cenário de Comunicação host-to-host.....	144
Figura 75 - Passo 1 da Comunicação host-to-host	145
Figura 76 - Passo 2 da Comunicação host-to-host	146
Figura 77 - <i>ARP Request</i>	147
Figura 78 - <i>ARP Request</i> Continuação.....	147
Figura 79 - <i>ARP Reply</i>	148
Figura 80 - <i>ARP Reply</i> Continuação	149
Figura 81 - Enviando o dado	150
Figura 82 - Conexão em estrela com um switch	151
Figura 83 - Host em outra rede.....	152
Figura 84 - Conexão com vários roteadores.....	153

LISTA DE TABELAS

Tabela 1 - Canais e frequências da banda 2,4 GHz	31
Tabela 2 - Representação de bits com modulação QPSK	41
Tabela 3 - Padrão 802.11	42
Tabela 4 - Padrão 802.11b.....	46
Tabela 5 - Comparação entre técnicas de modulação.....	53
Tabela 6 - Taxa de Transmissão 802.11g	59
Tabela 7 - Padrão 802.11g.....	59
Tabela 8 - Utilização das frequências de 5,0 GHz	60
Tabela 9 - Atribuições do AP e WLC.....	73
Tabela 10 - Potências disponíveis para o AP Cisco 3502	81
Tabela 11 - Quantidade de portas de switch necessárias.....	99
Tabela 12 - Camadas do Modelo OSI	119
Tabela 13 - Exemplo de Endereços IP.....	134

LISTA DE ABREVIATURAS E SIGLAS

AM	Amplitude Modulation
AP	Access Point
ARP	Address Resolution Protocol
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Basic Service Set
CCK	Complementary Code Keying
CD	Collision Detection
CSMA	Carrier Sense Multiple Access
DRS	Dynamic Rate Shifting
DSSS	Direct Sequence Spread Spectrum
ESS	Extender Service Set
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FFT	Transformada Rápida de Fourier
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
LAN	Local Area Network
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Transformada Inversa Rápida de Fourier
IP	Internet Protocol
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization
ISP	Internet Service Provider
MAC	Media Access Control
MAN	Metropolitan Area Network

MIMO	Multiple Input Multiple Output
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OUI	Organizational Unique Identifier
POE	Power over Ethernet
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
SHF	Super High Frequency
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UDP	User Datagram Protocol
UHF	Ultra High Frequency
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WLC	Wireless Lan Controller

SUMÁRIO

1 INTRODUÇÃO	17
2 UM BREVE HISTÓRICO DOS SISTEMAS DE COMUNICAÇÃO	19
2.1 A INTERNET	21
3 FUNDAMENTOS DE REDES SEM FIO	23
4 AGÊNCIAS REGULADORAS	27
4.1 IEEE	27
4.2 WI-FI ALLIANCE	28
4.3 FCC, ETSI, ANATEL	28
5 PRINCÍPIOS DE RF	29
5.1 MODULAÇÃO E PADRÕES IEEE	32
5.1.1 O padrão original IEEE 802.11	34
5.1.1.1 FHSS – Frequency Hopping Spread Spectrum	34
5.1.1.2 DSSS – Direct Sequence Spread Spectrum	36
5.1.1.3 PSK e BPSK	39
5.1.1.4 QPSK	41
5.1.2 IEEE 802.11b	42
5.1.2.1 CCK – <i>Complementary Code Keying</i>	43
5.1.3 IEEE 802.11g	46
5.1.3.1 OFDM – <i>Orthogonal Frequency-Division Multiplexing</i>	47
5.1.3.2 QAM – Quadrature Amplitude Modulation	50
5.1.4 IEEE 802.11a	59
5.1.5 IEEE 802.11n	61
5.1.5.1 MIMO – Multiple Input Multiple Output	62

5.1.5.2 Compatibilidade com padrões anteriores	63
5.1.6 IEEE 802.11ac	64
6 TOPOLOGIAS E TERMINOLOGIA	66
7 EQUIPAMENTOS	71
7.1 ACCESS POINTS	71
7.2 CONTROLADORAS	72
8 PLANEJAMENTO, PROJETO LÓGICO E MELHORES PRÁTICAS	76
8.1 OBJETIVOS	76
8.2 PREDIÇÃO	78
8.3 SITE SURVEY	94
8.4 SITE SURVEY PÓS INSTALAÇÃO	98
8.5 TOPOLOGIA LÓGICA	98
9 APLICAÇÕES ATUAIS E APOSTAS PARA O FUTURO	101
9.1 3G/4G OFFLOAD	101
9.1.1 Femtocélulas	102
9.1.2 Wi-Fi	103
9.2 MOBILE CONCIERGE E ANALYTICS	105
10 CONCLUSÕES	107
REFERÊNCIAS	110
APÊNDICE A 1 - REDES DE COMPUTADORES	113
APÊNDICE A 1.1 - MODELO OSI	119
APÊNDICE A 1.1.1 - CAMADA DE APLICAÇÃO	120
APÊNDICE A 1.1.2 - CAMADA DE APRESENTAÇÃO	121
APÊNDICE A 1.1.3 - CAMADA DE SESSÃO	122

APÊNDICE A 1.1.4 - CAMADA DE TRANSPORTE	123
APÊNDICE A 1.1.5 - CAMADA DE REDE	124
APÊNDICE A 1.1.6 - CAMADA DE ENLACE.....	125
APÊNDICE A 1.1.7 - CAMADA FÍSICA	126
APÊNDICE A 1.2 - ENCAPSULAMENTO E DESENCAPSULAMENTO	127
APÊNDICE A 1.3 - IP	130
APÊNDICE A 1.4 - ETHERNET	137
APÊNDICE A 1.5 - ENTREGA DE PACOTES HOST A HOST	144

1 INTRODUÇÃO

Com o passar dos últimos anos, milhares de dispositivos móveis foram lançados no mercado. Estes aparelhos se tornam cada vez mais modernos, capazes de executar aplicações cada vez mais robustas de maneira extremamente rápida. Essa rápida evolução de dispositivos eletrônicos e móveis faz com que novas necessidades e desafios apareçam de forma constante nesse mundo tecnológico. Pessoas querem informações de maneira cada vez mais rápida, a qualquer hora e a qualquer lugar.

Essa dependência de informações, independentemente do lugar em que um pessoa esteja, já se tornou inerente a muitos usuários da internet nos tempos de hoje. Atualmente, não existe mais a necessidade de utilizar a internet no computador conectado a um cabo de rede proveniente do modem do provedor de internet. Isso é possível através da tecnologia Wi-Fi, que permite que as informações sejam transmitidas através do ar, ao invés de cabos. Além disso, pessoas também podem acessar a internet em locais públicos, estabelecimentos comerciais, etc, sem a utilização de cabos.

Para tornar possível um usuário acessar conteúdos da internet sem a utilização de cabos entre seu computador ou smartphone e um modem, é necessária uma complexa rede de equipamentos, protocolos e conceitos de telecomunicações, bem como tecnologias de segurança da informação e ferramentas de monitoramento.

Assim como os dispositivos móveis se tornam mais robustos e as necessidades das pessoas se tornam cada vez mais exigentes, os equipamentos que tornam a comunicação sem fio possível também evoluem. Aplicações antes inimagináveis aparecem a cada dia com o objetivo de tornar a vida das pessoas cada vez melhores possibilitando a elas realizarem atividades de maneira mais eficiente e produtiva.

O capítulo dois descreve um pouco a trajetória dos artefatos de comunicações desde os sumérios até as técnicas de modulação, amplamente utilizadas atualmente.

O capítulo três apresenta uma breve descrição da internet e seu surgimento.

O capítulo quatro aborda o conceito de redes sem fio e os motivos pelos quais este tipo de comunicação está se tornando cada vez mais importante para o dia a dia da população.

O capítulo cinco apresenta algumas das agências que regem as regras de utilização de algumas das tecnologias de transmissão sem fio. Entre elas estão o IEEE, a Wi-Fi Alliance e Anatel, agência reguladora de telecomunicações do Brasil.

O capítulo seis trata em detalhes as principais técnicas de transmissão sem fio de dados. Ele aborda tecnologias de rádio frequência e as mais modernas técnicas de modulação. Além disso, os padrões 802.11 estabelecidos pelo IEEE para o Wi-Fi também são explicados.

No capítulo sete, são apresentadas as principais topologias e termos técnicos encontrados neste segmento de tecnologia.

O capítulo oito apresenta os principais equipamentos que compõem um projeto de rede Wi-Fi, entre eles *Access Points* e controladoras.

O capítulo nove apresenta um projeto real de planejamento de uma rede Wi-Fi desde as premissas iniciais até a montagem da topologia final. Neste processo estão inclusos as etapas de predição via *software*, *site survey*, e pós *site survey*, todas explicadas detalhadamente.

O capítulo dez apresenta as principais aplicações das redes Wi-Fi presentes no mundo inteiro, em adição ao caso abordado no capítulo nove. Além disto, este capítulo mostra quais são as principais apostas das grandes empresas para esta área bastante promissora.

2 UM BREVE HISTÓRICO DOS SISTEMAS DE COMUNICAÇÃO

Hoje muitas pessoas não são capazes de imaginar a vida sem smartphones com acesso a internet e notebooks que podem acessar a internet de qualquer parte de casa ou de um escritório. Porém, toda essa facilidade e mobilidade se dá graças a grande e constante evolução dos setores de TIC (Tecnologia da Informação e Comunicação) e Telecomunicações.

A constante busca pela facilidade e rapidez da comunicação não é de hoje. Os sumérios, considerada a civilização mais antiga da humanidade, criaram o sistema cuneiforme de escrita, que foi utilizada por toda a Mesopotâmia e alguns povos vizinhos. Acredita-se que este seja o primeiro sistema de escrita já criado, antecedendo os hieróglifos egípcios em aproximadamente 75 anos.

Na medida em que as civilizações foram passando a ocupar territórios cada vez mais extensos, as distâncias entre os povos aumentavam. Surgiu então a necessidade de criação de meios de comunicação mais eficientes, que pudessem transmitir mensagens a distâncias maiores. Surgiram assim as mensagens por sinal de fumaça, pombo-correio, bandeiras, tochas e mensageiros.

Em 1838 foi inventado o telégrafo, por Samuel Finley Breese Morse, americano, nascido em 1791. O telégrafo representou uma significativa evolução dos meios de comunicação à distância e sua criação se deve também a diversos experimentos e descobertas de cientistas e físicos. Tudo começou com William Watson que demonstrou, em 1747, que a corrente elétrica podia ser transmitida a uma distância considerável através de um fio metálico entre um emissor e um receptor. A partir dessa invenção, diversos pesquisadores descobriram inúmeras possibilidades e aplicações para correntes elétricas. Hans Christian Oersted descobriu que uma agulha magnética se defletia mediante a passagem de corrente elétrica por um fio suficientemente próximo, e que além disso, a deflexão variava de lado de acordo com o sentido da corrente. Pierre Simon Laplace e André Marie Ampère utilizaram a corrente elétrica em pequenos magnetos instalados nas extremidades da recepção de 26 fios para representar letras do alfabeto. Entretanto, foi o telégrafo de Morse que se popularizou e começou a ser utilizado por indústrias, governos e militares. Seu sistema se destacava pela presença de apenas um fio. A comunicação era possível através de um código de sua autoria que era constituído por pontos, traços e intervalos, com base na presença ou ausência de impulsos elétricos.

Em 1876, através de experimentos realizados por Alexander Graham Bell e seu assistente Thomas Augustus Watson, foi criado o telefone. Bell desenvolveu o que designou de telégrafo harmônico, um mecanismo capaz de receber várias mensagens telegráficas em código morse simultaneamente. Alexander Bell desejava ir ainda mais longe. Ele queria fazer com que a corrente elétrica variasse de intensidade da mesma maneira que o ar ao emitir um som. Dessa maneira, poderia transmitir falas por meio da eletricidade, dando início ao desenvolvimento do telefone.

A história da comunicação sem fio se iniciou em meados de 1861, quando o físico e matemático britânico, James Clerk Maxwell deu forma à uma teoria do eletromagnetismo que uniu eletricidade, ótica e magnetismo, surgindo assim as Equações de Maxwell, que juntou a Lei de Ampère, Lei de Gauss e a Lei de Indução de Faraday. Essa teoria descreve as bases teóricas da propagação de ondas eletromagnéticas. Dessa forma pesquisadores começaram a considerar a transmissão de informação para um lugar remoto por meio da propagação eletromagnética. Heinrich Hertz, físico alemão, nascido em 1857, realizou diversos experimentos utilizando as teses previamente desenvolvidas por Maxwell. Ele conseguiu demonstrar que as ondas viajam em linhas retas e que elas podiam ser refletidas por uma folha de metal. Hertz realizou experimentos conseguindo transmitir entre dois condutores a uma distância de 1,5 metros. Guglielmo Marconi, em 1896, conseguiu a façanha de transmitir por telégrafo sem fio um sinal entre duas cidades distantes 52 km uma da outra.

Em 1921, foi implantado, pelo Departamento Policial de Detroit, o primeiro sistema rádio-telefônico móvel que operava na faixa de frequências de 2 MHz. Devida a essa faixa de baixa frequência, a taxa de transmissão e a qualidade do sinal eram baixas.

Edwin Howard Armstrong inventou a modulação FM (Frequency Modulation) em 1933. A modulação por frequência é a codificação de uma informação em uma onda portadora através da variação da frequência. Através desse invento, foi possível melhorar significativamente a qualidade das transmissões por ondas eletromagnéticas. A partir desse momento, diversas tecnologias envolvendo modulação foram desenvolvidas e melhoradas, permitindo a criação de, por exemplo, o sistema de telefonia móvel que muitos utilizam hoje em dia. Através desses conceitos de ondas eletromagnéticas, modulação, faixas de frequências, entre outros, foi possível a transmissão de não apenas voz, mas também dados, sem a utilização de fios.

2.1 A INTERNET

A internet é um conjunto imenso de diversas redes de comunicação do mundo inteiro compostas por diversos equipamentos e computadores conectados em uma rede mundial. Através da internet pode-se obter acesso a uma infinidade de informações disponíveis quase que instantaneamente de diversos lugares do planeta.

Atualmente, as pessoas utilizam a internet para se comunicar, enviar emails, realizar os mais diversos tipos de pesquisas, efetuar compras, baixar conteúdos como filmes, documentos, músicas e imagens, entre outros.

A primeira rede mundial de comunicação é o que veio a se tornar futuramente o que se conhece hoje como Internet, foi criada no meio militar, assim como diversas outras tecnologias. Chamada de ARPANet (*Advanced Research Projects Agency Network*), a primeira rede operacional de computadores à base de comutação por pacotes fazia parte do departamento de defesa dos Estados Unidos da América. Desenvolvida pela ARPA (*Advanced Research and Projects Agency*), esta rede tinha como objetivo interligar as bases militares e os departamentos de pesquisa norte americano.

No Brasil, a internet se iniciou em instituições acadêmicas e instituições de pesquisas. Em 1988, a FAPESP (Fundação de Amparo à pesquisa do Estado de São Paulo) estabeleceu uma conexão com um laboratório em Chicago, nos EUA. Neste mesmo ano, o LNCC (Laboratório Nacional de Computação Científica) estabeleceu uma conexão com a universidade de Maryland através da Bitnet (*Because it's time network*). Em 1989 a Universidade Federal do Rio de Janeiro também consegue se conectar com uma universidade nos EUA, desta vez a Universidade da Califórnia.

Em 1992, o Instituto Brasileiro de Análises Sociais e Econômicas assinou um convênio com a Associação para o Progresso das Comunicações liberando o uso da Internet para ONGs. Em 1993 ocorreu a primeira conexão a 64 Kbps estabelecida entre São Paulo e Porto Alegre.

Em 1995 os ministérios das Comunicações e da Ciência e Tecnologia criaram o provedor de acesso privado à Internet liberando a operação comercial no Brasil. Após isso, assinaturas de acesso a rede começaram a ser vendidas por estes provedores.

No início, a velocidade de acesso a Internet era de 4kbps, onze vezes mais lenta do que a velha conexão discada. Naquela época, conexão por fibra nem era cogitada. Atualmente, as taxas de transmissão podem atingir até 40 Gbps.

3 FUNDAMENTOS DE REDES SEM FIO

Com o passar do anos e a evolução da internet, as aplicações se tornaram mais robustas e os usuários mais exigentes. As empresas buscam melhorar a cada dia sua eficiência e produtividade, oferecendo meios tecnológicos ao seus funcionários cada vez mais modernos, para que eles possam exercer suas funções da maneira mais eficiente possível.

Hoje, muitas empresas já possuem suas redes de comunicação, fornecendo acesso a internet aos seus funcionários dentro do escritório, e algumas também fornecem acesso a rede sem a utilização de cabos. Fornecer acesso wireless para seus empregados significa mobilidade, produtividade e eficiência. Um determinado funcionário pode querer levantar de sua mesa no escritório e se dirigir a uma sala de reunião para apresentação de um determinado trabalho. Com a rede wireless, ele pode se conectar a internet e ter acesso aos recursos da rede cabeada (servidores de arquivos, impressoras, intranet, etc) de qualquer lugar do escritório, independentemente da existência de um cabo de rede disponível e seu comprimento. Essa mesma empresa, pode ainda adicionar de maneira muito rápida um novo dispositivo na rede, sem ter que alterar alguma estrutura física.

As redes cabeadas necessitam de uma infraestrutura física adequada para passagem de cabos nas paredes e furos para passagem para outros cômodos. Além disso, o manuseio ou manutenção incorreta de cabos, pode levar a problemas e até indisponibilidade da rede. Assim, as redes sem fio se tornam de mais fácil instalação se comparadas as redes cabeadas, além de ser possível hospedar uma LAN sem fio em locais onde o cabeamento não pode ser realizado. Alguns exemplos são: edifícios, casas ou escritórios antigos, parques, praças, ruas, pátios, bares, lanchonetes, restaurantes, shoppings, aeroportos, galpões, escolas, universidades e outros locais ao ar livre.

Uma das principais preocupações com uma rede wireless antigamente era a segurança, ou seja, assegurar que uma determinada informação está sendo transmitida de forma segura pelo ar. Nos últimos anos, a segurança fornecida não só por equipamentos da infraestrutura da rede sem fio, mas como também por outros equipamentos da rede, melhorou de forma extremamente significativa e resultou na forte adoção das tecnologias de rede sem fio.

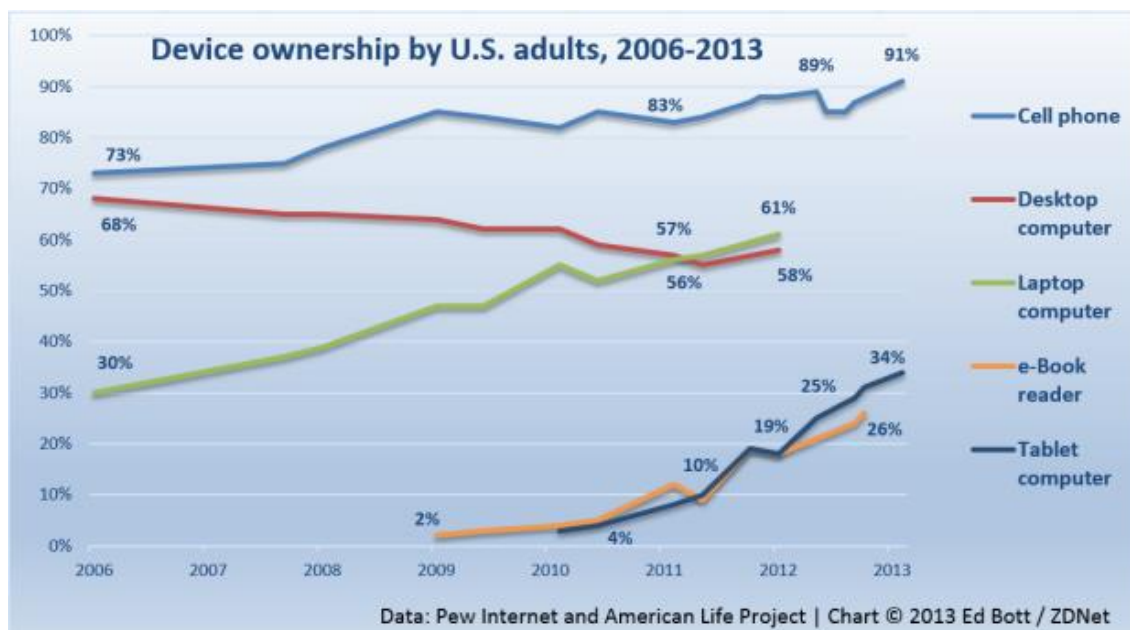
Atualmente, cada vez mais empresas adotam essa tecnologia para aumentar a produtividade e a mobilidade de seus funcionários dentro de uma empresa. Além disso, outras estão adotando políticas mais liberais para acesso à rede, como utilizar seus celulares ou tablets próprios para acesso à rede corporativa e a internet da empresa. Isso se deve a grande popularização desses dispositivos que já vem preparados para acesso sem fio.

Pesquisas realizadas recentemente mostram que a presença de internet sem fio grátis em um determinado estabelecimento pode aumentar consideravelmente a quantidade de clientes e o seu tempo de permanência, e consequentemente aumentar os lucros do estabelecimento comercial. Os restaurantes, as lojas e os bares estão fortemente adotando essa tecnologia para atrair cada vez mais clientes. Os hospitais, as escolas, e os aeroportos também tem adotado de forma bastante significativa o uso de redes sem fio para disponibilizar acesso à internet.

Uma aplicação bastante interessante e que envolve grandes investimentos é a utilização de redes sem fio por operadoras para disponibilizar internet nas ruas, da mesma maneira que é disponibilizado por um estabelecimento comercial. Essa é uma abordagem bastante complexa, que envolve longos estudos e altos investimentos.

A produtividade não está mais restrito ao local de trabalho fixo ou um determinado período do dia. Agora, pessoas esperam estar conectadas a qualquer hora e em qualquer lugar, do escritório, do aeroporto ou até em casa. Há algum tempo atrás, funcionários quando viajam ficavam restritos de acesso à internet. Hoje, eles podem acessar a internet, checar *emails*, baixar e subir arquivos e até participar de conferências em seus celulares, *notebooks* ou *tablets*. O forte crescimento das vendas e utilização desses equipamentos, principalmente *smartphones* e *tablet*, estimula ainda mais a criação de novas redes sem fio e o desenvolvimento e melhorias das que já existem. A Figura 1 ajuda a ilustrar o comportamento do consumidor nos últimos anos mostrando que os tablets e smartphones se tornaram itens de muito desejo dos adultos dos Estados Unidos.

Figura 1 - Posse de dispositivos por adultos americanos



Fonte: (IDG Now, 2013)

Esse aumento expressivo nas vendas de tablet, notebook e smartphones ajudaram muito a mudar o cenário das tecnologias sem fio atualmente. A projeção é que cada vez menos desktops sejam vendidos e os dispositivos móveis tomem conta do mercado, fazendo com que mais infraestrutura de acesso à internet sem fio seja construída e mais tecnologias sejam desenvolvidas para suprir toda essa demanda.

São muitas as aplicações, desde as mais básicas até as mais complexas e caras. Além disso, existem diversas vantagens e é um investimento que pode trazer grandes retornos financeiros. Porém, para que tudo isso funcione de maneira adequada, é necessário entender como o conceito de rádio frequência funciona, além de tomar conhecimento de quais são os equipamentos e infraestrutura necessária para colocar em funcionamento uma rede sem fio de qualidade.

Uma rede cabeada, vista anteriormente, é chamada de LAN (*Local Area Network*). Em uma rede sem fio, chamada de WLAN (*Wireless Local Area Network*), a maior diferença para uma LAN é a forma de conexão, que ao invés de cabos é feita por radiofrequência.

Da mesma maneira que os equipamentos de uma rede cabeada possibilita a interoperabilidade com outros equipamentos de outros fabricantes, os equipamentos para

implementar uma WLAN também devem funcionar em conjunto. Para isso, em 1999, algumas empresas, como Nokia, 3com, Symbol Technologies e Lucent Technologies, se uniram para formar um grupo de pesquisas chamado WECA (*Wireless Ethernet Compatibility Alliance*), que tinha como objetivo desenvolver soluções de redes sem fio utilizando os mesmo padrões. Em 2003, esse grupo passou a se chamar Wi-Fi Alliance, o que deu origem ao nome Wi-Fi, que é conhecido mundialmente.

4 AGÊNCIAS REGULADORAS

Muitas pessoas se beneficiam da disponibilidade de acesso à internet sem fio ao viajar para outras partes do mundo. Sem órgãos regulatórios para assegurar o uso correto e a interoperabilidade de equipamentos, é muito provável que as pessoas não conseguiriam se conectar em diferentes lugares. Para assegurar que algumas regras referentes ao uso da radiofrequência sejam impostas e obedecidas, diversas organizações de cada país e comitês globais monitoram padrões e o uso dessa tecnologia.

Cada país possui seu conjunto de regulamentos que determina qual tipo de sinal (forma e potência) que pode ser enviado em cada parte do espectro de frequência global. É comum que vários países realizem acordos e agrupem suas regras em apenas um regulamento global. Nos Estados Unidos e alguns outros países da América, o FCC (*Federal Communications Commission*) determina quais frequências e potências podem ser utilizadas. A Europa e alguns outros países, como México e Israel, seguem as especificações do *European Telecommunication Standards Institute* (ETSI). No Japão, as regras são definidas pelo Ministro das Comunicações.

4.1 IEEE

O *Institute of Electrical and Electronic Engineers* (IEEE) é uma organização profissional global que desenvolve e documenta padrões relacionados as áreas de elétrica, computação e engenharia. Em 1980, o comitê de comunicação do IEEE definiu e criou diversas áreas de estudo de comunicação por redes de computadores, que foram divididos em grupos de trabalho, começando pelo número 802. O IEEE 802 se refere a uma família de padrões do IEEE que trata de redes locais (LAN – *Local Area Networks*) e redes metropolitanas (MAN-*Metropolitan Area Networks*). Os serviços e protocolos especificados pelo IEEE 802 definem uma padronização para LANs e MANs referentes as suas camadas um e dois (Física e Enlace) do modelo OSI. O décimo primeiro grupo dessa categoria, 802.11, foi criado em 1990 para analisar as aplicações e os cenários nos quais as redes sem fio eram usadas. O 802.11 é um grupo aberto, composto por engenheiros de diferentes companhias que trabalham em conjunto para criar padrões melhores do que qualquer solução proprietária.

4.2 WI-FI ALLIANCE

A Wi-Fi Alliance é uma associação global sem fins lucrativos que é dedicada a promover o crescimento e a aceitação das WLANs. Um dos seus principais objetivos é assegurar a interoperabilidade de dispositivos que utilizam os padrões 802.11 oferecidos por diferentes fabricantes. Em 2000, por iniciativa desse grupo, iniciou-se um programa chamado Wi-Fi CERTIFIED. Este programa fornece uma certificação para cada produto com a tecnologia Wi-Fi como prova de interoperabilidade e excelência na experiência de uso. Esse certificado fornece uma segurança por parte do consumidores na hora da compra, já que assegura que um determinado produto irá funcionar com outro que também possui o certificado. A Wi-Fi Alliance já certificou mais de 15000 produtos e hoje possui mais de 550 empresas membros dessa associação. A Figura 2 mostra o logo do certificado emitido pela associação:

Figura 2 - Logo Wi-Fi *Certified*



Fonte: (wi-fi.org, 2013)

4.3 FCC, ETSI, ANATEL

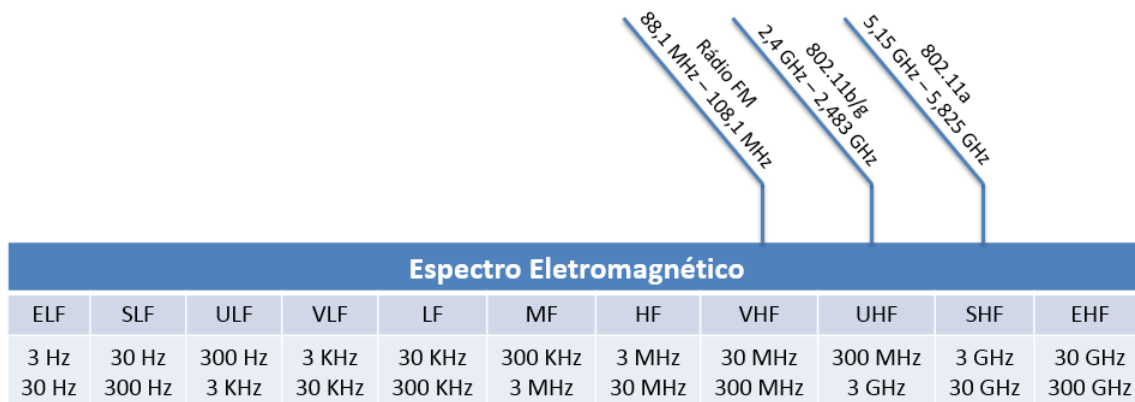
O FCC, ETSI e Anatel são exemplos de agências reguladoras do Estados Unidos, Europa e Brasil respectivamente. São estas agências que determinam quais frequências e potências de transmissão que podem ser utilizadas. Além disso, estas agências definem regras como canais disponíveis, conectores de antenas e ganhos de antenas, bem como promovem a homologação de novos equipamentos.

5 PRINCÍPIOS DE RF

O conceito de wireless utiliza o ar como meio de transmissão, e para isso são utilizadas as ondas eletromagnéticas. Como toda onda, suas principais características são: frequência, amplitude e comprimento de onda.

Ao falar de ondas eletromagnéticas, deve-se ter em mente que para cada aplicação tem-se uma faixa de frequência que pode ser utilizada. O espectro eletromagnético da Figura 3 ilustra de forma clara as faixas de frequências e algumas de suas aplicações:

Figura 3 - Espectro Eletromagnético



Fonte: (Cisco, 2013)

Essa divisão é realizada pela existência de inúmeros serviços que podem utilizar sinais de rádio, e para evitar problemas, principalmente com interferências, é necessário que cada serviço opere de acordo com essas regras mediante aprovação. Existem, no entanto, algumas faixas de frequência que não necessitam de aprovação, ou algum tipo de licença: são as faixas ISM (*Industrial, Scientific and Medical*), que operam nas seguintes bandas: 900 MHz, 2,4 GHz e 5,0 GHz. As bandas de frequência ISM são bandas reservadas internacionalmente para o uso de rádio frequência para propósitos industriais, científicos e médicos. A tecnologia Wi-Fi para WLANs utiliza essas duas últimas frequências para transmissão de dados.

Uma vez que não existe a necessidade de uma licença para a utilização dessas faixas de frequência, nenhum usuário tem exclusividade sobre elas. Por exemplo: a banda de 2,4 GHz, além de ser utilizada para WLANs, também é utilizada por câmeras de vídeo sem fio, tecnologia

Bluetooth, fornos de microondas e telefones sem fio. Dessa maneira uma WLAN utilizando a banda de 2,4 GHz está sujeita a interferências desses dispositivos.

Como pode-se notar no espectro eletromagnético da Figura 3, as frequências utilizadas por WLANs estão dentro da faixa de UHF (*Ultra High Frequency*) e SHF (*Super High Frequency*). As bandas ISM englobam as seguintes frequências:

- 900 MHz: 902 a 928 MHz;
- 2,4 GHz: 2,400 a 2,483 MHz;
- 5,0 GHz: 5,150 a 5,350 GHz; 5,350 a 5,725 GHz; 5,725 a 5,825 GHz;

Dependendo dos órgãos reguladores de cada país, essas frequências podem sofrer algumas pequenas variações.

Cada banda de frequência está dividida em diversos canais. Um canal consiste em uma largura da banda que vai de uma frequência a outra, dentro da banda de frequência geral. As explicações das bandas ISM a seguir facilitam a compreensão do conceito de canais.

900MHz

A banda de 900 MHz começa em 902 MHz e vai até 928 MHz. Essa frequência é bastante familiar devido a existência de telefones sem fio que utilizavam essa banda de frequência antigamente.

2,4 GHz

A banda de frequência de 2,4 GHz é talvez a mais utilizada atualmente para WLANs. Essa banda é subdividida em diversos canais que vão desde 2,400 GHz até a frequência de 2,4835 GHz. Nos Estados Unidos e no Brasil existem 11 canais disponíveis, cada um com largura de 22 MHz, porém separados por somente 5 MHz, o que pode causar um grande problema de interferência. O canal 1 inicia na frequência 2,401 GHz e termina em 2,423 GHz e está centrado em 2,412 GHz. O canal 2, por estar 5 MHz distante do canal 1, inicia em 2,417 GHz, porém por ter 22 MHz de largura, inicia em 2,406 GHz e termina em 2,428 GHz. Assim, pode-se notar que existe uma sobreposição de frequências nos canais 1 e 2. Quando um dispositivo utiliza o canal 1 para transmitir e perto deste está localizado um outro dispositivo transmitindo no canal 2 da banda de

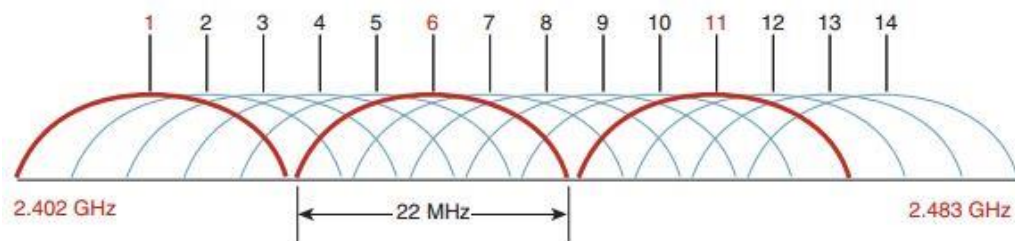
2,4 GHz, existe uma forte chance de haver degradação do sinal por interferência. Da mesma maneira, o canal 3 também interfere tanto no canal 1 quanto no canal 2, já que sua faixa de frequência se inicia em 2,411 GHz e termina em 2,433 GHz, sendo centrada em 2,422 GHz (5 MHz distante do canal 2). Dessa maneira, a única combinação de canais que não se sobrepõem são o 1, 6 e 11, como mostra a Tabela 1 abaixo:

Tabela 1 - Canais e frequências da banda 2,4 GHz

Canais e frequências da banda 2,4 GHz			
Canal	Início (GHz)	Frequência Central (GHz)	(Fim GHz)
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473

Sendo assim, pode-se desenhar o diagrama da Figura 4 para ilustrar de forma mais clara a sobreposição dos canais da banda de 2,4 GHz:

Figura 4 - Canais da banda de 2,4 GHz



Fonte: (Cisco, 2013)

Com isso, pode-se concluir que para evitar problemas de interferência em um ambiente que será implementada uma rede sem fio, deve-se utilizar canais que não se sobrepõem: 1, 6 e 11. Posteriormente, será mostrado quais são as melhores práticas atuais para o desenho de uma solução Wi-Fi.

5,0 GHz

A banda de frequência de 5,0 GHz também é subdividida em canais, porém com 20 MHz de largura cada. Entretanto, ao invés de possuir apenas 3 canais que não se sobrepõem, a banda de 5,0 GHz possui 23.

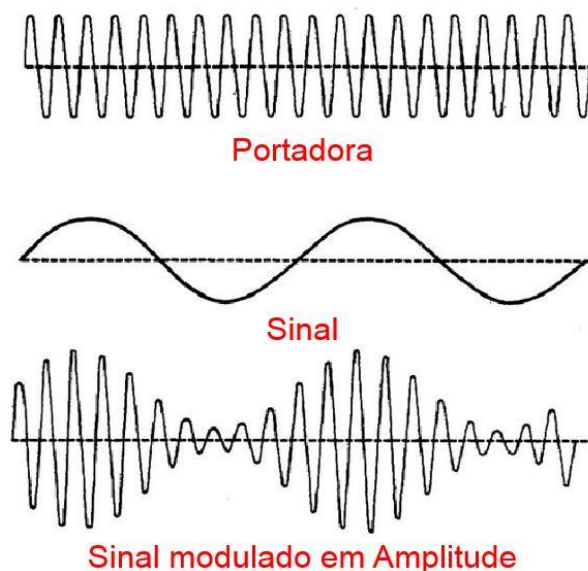
As frequências de 2,4 GHz e 5,0 GHz são altamente utilizadas atualmente para transmissão de dados em uma WLAN. Para a utilização dessas bandas, existem diversos padrões definidos pelo IEEE, que são descritos a seguir:

5.1 MODULAÇÃO E PADRÕES IEEE

O princípio básico para a transferência de uma informação através de uma onda eletromagnética é a modulação. Este processo consiste na adição de uma determinada informação em uma onda, chamada portadora, através da variação da frequência, amplitude ou fase dessa onda, de modo que um dispositivo receptor possa recuperar a informação através de um processo reverso chamado demodulação.

Um exemplo básico é a modulação em amplitude AM, que é basicamente a variação da amplitude de uma onda portadora de acordo com a informação que se deseja transmitir. A modulação AM foi o primeiro método desenvolvido de modulação e sempre foi utilizado para transmitir áudio através de ondas eletromagnéticas. Uma grande desvantagem da modulação AM é o fato de ela ser altamente vulnerável a interferências eletromagnéticas, causadas por eletricidade estática da atmosfera e dispositivos eletromecânicos como um gerador ou um motor. Quando o sinal modulado chega o receptor, ele sofre um processo chamado demodulação, que consiste na extração da informação original da onda modulada. A Figura 5 mostra um exemplo de modulação AM:

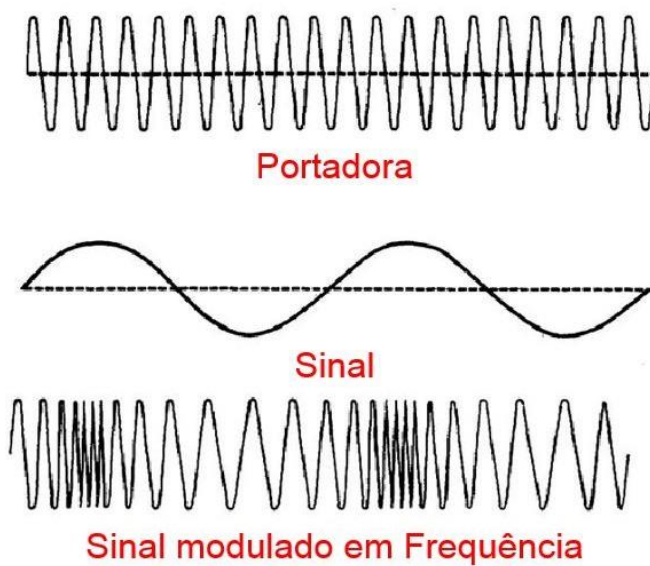
Figura 5 - Modulação AM



Fonte: (Allan Ferrari, 2013)

Existe também a modulação em frequência FM, que ao invés de alterar a amplitude da onda, altera-se a frequência, de acordo com a informação a ser transmitida. A Figura 6 demonstra o processo de modulação FM:

Figura 6 – Modulação FM



Fonte: (Allan Ferrari, 2013)

As principais aplicações para modulação FM são:

- Transmissão de rádio FM;
- Walkie-Talkie (*Two-Way radio*);
- Sistemas de transmissão de vídeo.

As modulações AM e FM são dois tipos de modulação analógica bastante populares hoje em dia. Entretanto, para as transmissões de dados através de uma WLAN, são utilizadas técnicas diferentes e mais robustas de modulação, a modulação digital.

5.1.1 O padrão original IEEE 802.11

Segundo Bernal (2002) o padrão original 802.11 é onde tudo começou quando se trata de WLANs. Atualmente, é bastante raro encontrar dispositivos que ainda utilizam esse padrão devido a suas baixas velocidades de transmissão: 1 ou 2 Mbps. Esse padrão foi estabelecido em 1997 e utiliza a banda de frequência de 2,4 GHz e as tecnologia de transmissão FHSS (*Frequency Hopping Spread Spectrum*) e DSSS (*Direct Sequency Spread Spectrum*).

5.1.1.1 FHSS – Frequency Hopping Spread Spectrum

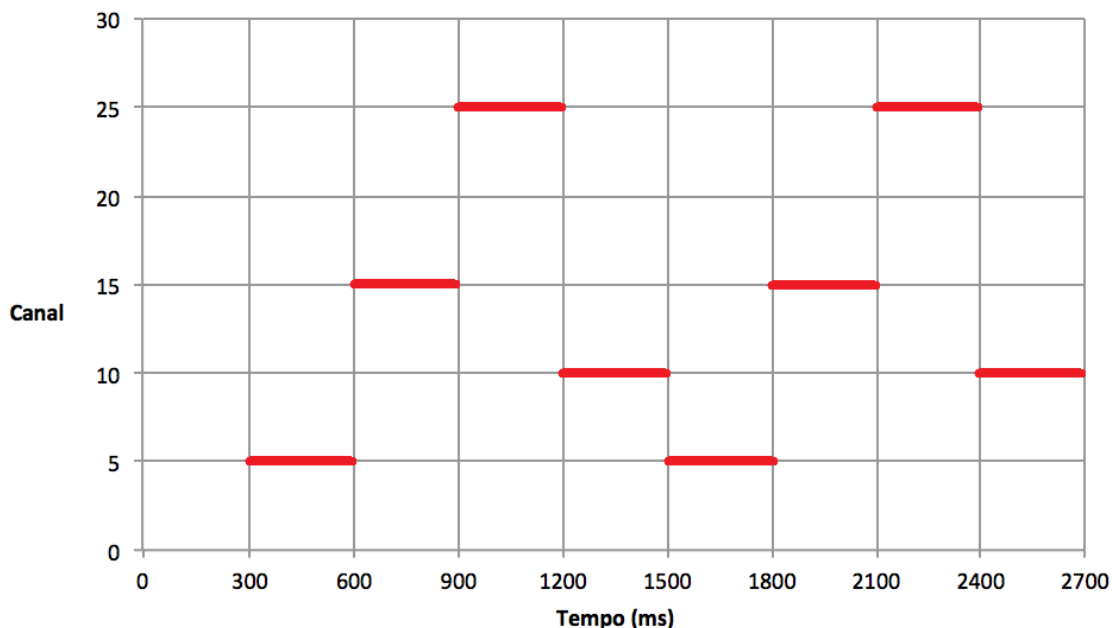
O FHSS é uma técnica de transmissão de sinais de rádio que consiste em alternar a portadora por vários canais de frequência de forma pseudoaleatória, ao longo do tempo, conhecidas por ambos transmissor e receptor.

Essa técnica tem como principal objetivo eliminar ou reduzir interferências. Sabe-se que interferência sempre foi e é até hoje um dos pontos mais preocupantes quando se trata de WLANs. Isso se deve muito a utilização da faixa de frequência de 2,4 GHz da ISM. Como essa faixa não necessita de um licença para sua utilização, diversos dispositivos a utilizam para propagar sinais de rádio. Um exemplo disso é o telefone sem fio, que também utiliza a faixa de 2,4 GHz. Dessa maneira, em um ambiente onde existe uma rede sem fio, ao utilizar um telefone desse tipo, irá ocorrer uma considerável degradação do sinal devido a interferência. Se esse telefone utilizar uma frequência fixa para transmissão de dados, dentro de um canal específico, e se este canal for o mesmo que está sendo utilizado pela WLAN, uma alta taxa de erro irá ocorrer, causando mais

retransmissão de dados e resultando numa menor taxa de transmissão, tudo devido a essa interferência. A técnica FHSS surgiu para tentar eliminar ou reduzir interferências causadas pela utilização fixa de uma determinada frequência. Se um dispositivo está transmitindo um sinal em qualquer parte da banda de 2,4 GHz (2,4 GHz – 2,483 GHz) da ISM, uma boa opção é nunca permanecer por um longo período na mesma frequência, e sim pular de uma para outra em curtos intervalos de tempo. A banda de 2,4 GHz é dividida em vários pequenos canais (aproximadamente 80) de 1MHz de largura cada. O emissor escolhe uma sequência de canais e informa o receptor sobre a escolha. A partir desse momento, o emissor passa a transmitir a informação, alterando de um canal para o outro em um intervalo de aproximadamente 300 a 400 ms. Desse modo, se uma fonte de interferência destruir o sinal em um dos canais, apenas 300 a 400 ms de informação é perdida e não a informação inteira.

O gráfico da Figura 7 ilustra a transição de canal ao longo do tempo:

Figura 7 - Saltos de canal com FHSS



Fonte: (Autor, 2013)

O gráfico acima mostra de forma bastante simples e intuitiva que a sequência de canais escolhida pelo emissor é: 5, 15, 25 e por último 10. Durante a transmissão, a cada 300 ms, será alternado o canal para o próximo da sequência. Assim, no caso de existir um outro dispositivo

também transmitindo no canal 25, por exemplo, não haverá perda total da informação, mas somente o que for equivalente a 300 ms dela.

Embora essa técnica de transmissão tente reduzir problemas de interferência, ela é bastante limitada em questões de escalabilidade e taxas de transmissão:

- Escalabilidade: se por exemplo, existirem mais de 10 emissores e receptores, os diferentes saltos de frequência podem colidir, causando interferências devido aos saltos dos outros emissores.
- Taxas de transmissão: a limitação quanto a taxa de transmissão se deve ao fato de cada canal ter apenas 1 MHz de largura. Isso significa que se um canal de frequência está em 2,412 GHz, o sinal de fato se espalha de 2,4115 GHz até 2,4125 GHz. Com uma largura de canal de apenas 1 MHz, é possível atingir taxas de apenas 1 Mbps de transmissão.

5.1.1.2 DSSS – Direct Sequence Spread Spectrum

Ao invés de utilizar canais com largura pequena e pular de um canal para outro, a informação é enviada por um canal muito mais largo, de 22 MHz. Por exemplo, se um canal é centrado em 2,412 GHz, este vai de 2,401 GHz a 2,423 GHz.

Com esta técnica, não existe saltos de canais periodicamente, como acontecia no FHSS.

Ao longo do canal de 22 MHz, são enviados vários bits de informação de forma paralela, através de um método de codificação chamado DSSS Encoding.

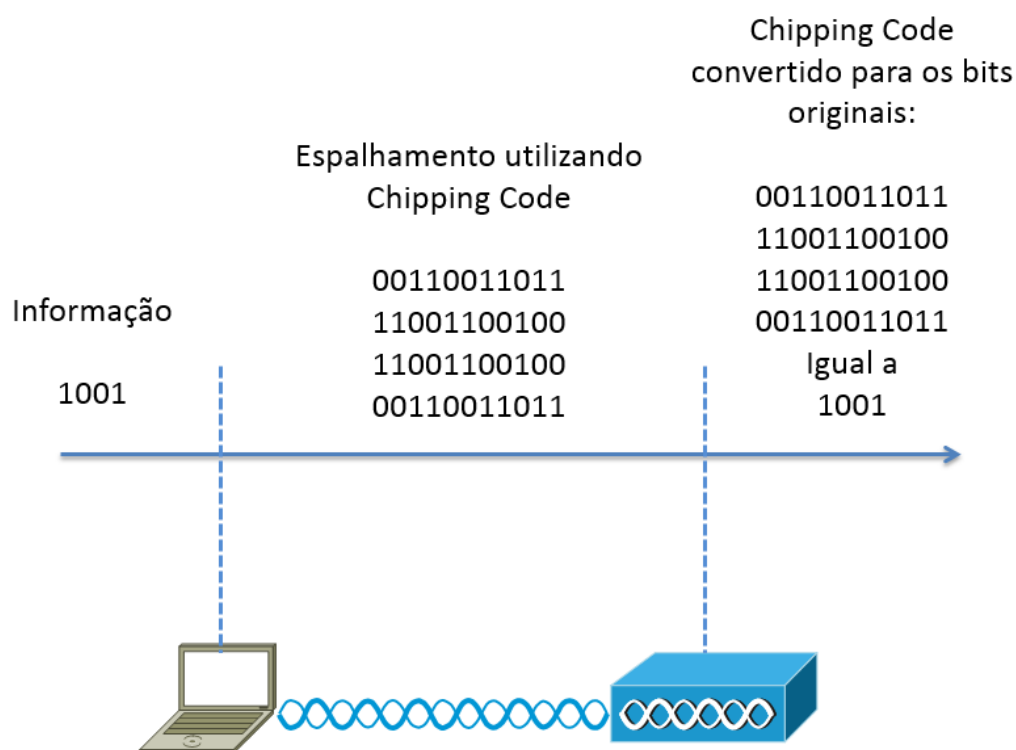
Para codificar uma determinada informação é utilizada uma *chip sequence*, que nada mais é do que uma sequência de bits que representa uma determinada informação. Um bit e um chip são praticamente a mesma coisa, porém um bit representa a informação e um *chip* é utilizado pela portadora. Codificar significa o processo de transformar uma informação de um formato para outro.

Devido a possíveis interferências em uma transmissão sem fio, DSSS utiliza uma sequência de chips. Quando DSSS espalha a informação ao longo de uma largura de banda, um simples bit de informação é representado por um string de *chips* ou um fluxo de chips. Por exemplo: o bit 1

pode ser apresentado pela sequência de *chips* 00110011011 e o bit 0 pela sequência 11001100100. Assim, ao enviar o dado 10, por exemplo, na verdade é enviado a seguinte sequência: 00110011011 11001100100. Esta sequência de chips é então enviada paralelamente utilizando todas as frequências de um determinado canal de 22 MHz.

A Figura 8 ilustra um exemplo de transmissão de dados utilizando o método de codificação por sequência de chips:

Figura 8 - Transmissão de sequência de chip

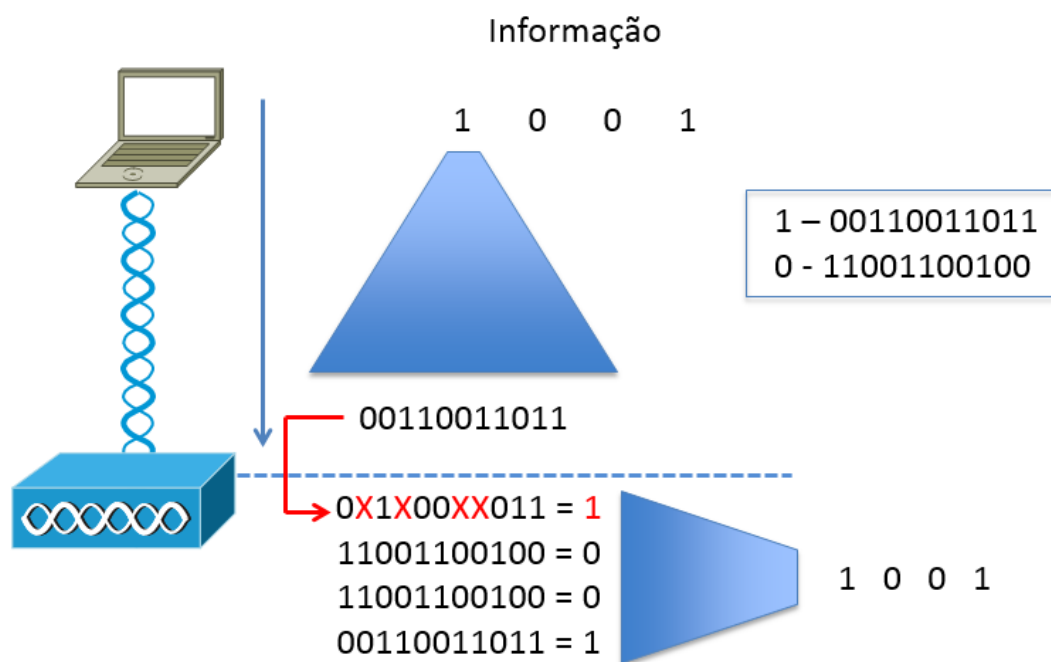


Fonte: (Cisco, 2013).

A Figura 8, mostra um dispositivo tentando enviar o dado 1001 para um ponto de acesso sem fio. Esse dado sofre o processo de codificação por sequência de chips e se transforma em uma quantidade maior de bits que serão transmitidos paralelamente ao longo das frequências de um determinado canal de 22 MHz de largura. Quando essa sequência chega o destino, ela é decodificada e o dado original (1001) é recuperado.

É importante lembrar que devido a interferências, ainda é possível que alguns dos bits de uma determinada sequência sejam perdidos ou invertidos, isto é, o bit 1 pode virar 0 ou o bit 0 pode virar 1. Entretanto, através dessa técnica de codificação, são necessários que mais de 5 bits dessa sequência sejam invertidos para alterar o valor de um bit do dado original de 1 para 0 ou vice versa. A Figura 9 ilustra de forma mais clara essa resistência a interferências:

Figura 9 - Resistência a interferência



Fonte: (Autor, 2013)

A Figura 9 mostra que ao transferir uma determinada informação, mesmo que 4 chips da sequência de um determinado bit são invertidos ou perdidos, ainda é possível saber que o bit original é o 1. Para que este seja confundido com o 0, seriam necessários que pelo menos 5 bits fossem invertidos.

Para atingir velocidades de 1 Mbps e 2 Mbps, o padrão 802.11 utiliza o *Barker Code*. Esse código define a utilização de 11 chips para codificar uma determinada informação. O Barker code de 11 chips utilizado no padrão 802.11 é: 10110111000.

Entretanto, codificar uma determinada quantidade de bits não é o suficiente para enviar uma informação através de ondas. Ainda é necessário usar algumas técnicas de modulação para poder atingir as velocidades citadas acima.

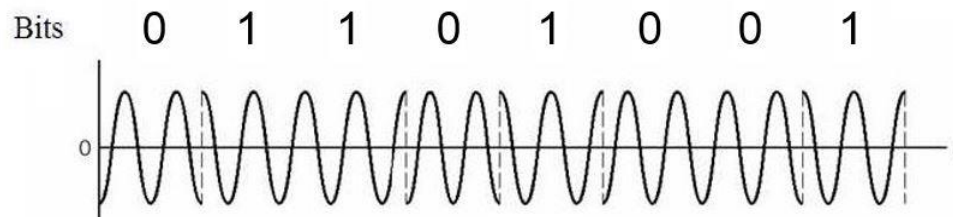
5.1.1.3 PSK e BPSK

Para atingir velocidades de 1 Mbps, é necessário utilizar uma técnica de modulação chamada de modulação por chaveamento de fase, ou PSK (*Phase Shift Keying*). Esse tipo de modulação representa uma determinada informação através da variação da fase da onda portadora.

A modulação AM é uma modulação analógica que pode representar uma determinada informação através da variação da amplitude de uma onda portadora. Segundo Rappaport (2009) neste tipo de modulação a amplitude da portadora varia em função de um sinal de interesse. Para a modulação PSK, entretanto, a variação é na fase ao invés da amplitude e por ser uma técnica de modulação digital esta pode representar bits distintos, por exemplo, para enviar 0, a onda portadora é defasada em 180° e para enviar 1, a onda portadora é defasada em 0° .

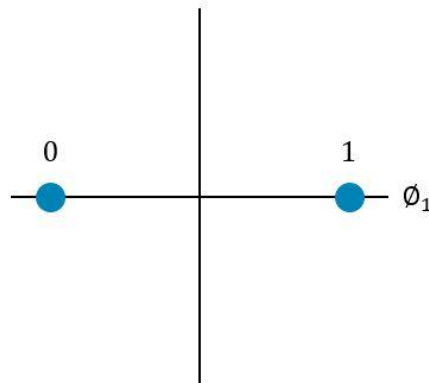
A Figura 10 mostra o processo de modulação PSK:

Figura 10 - Phase Shift Keying



Este caso, onde se representam dois símbolos (0° e 180°), é chamado de BPSK (*Binary Phase Shift Keying*) e pode ser representado pelo diagrama de constelação da Figura 11:

Figura 11 - Diagrama de Constelações BPSK



Fonte: (Autor, 2013)

Este diagrama de constelação mostra que existem dois símbolos possíveis que podem ser representados, com amplitudes iguais porém opostos em fase.

Através da técnica de modulação BPSK, é possível representar 1 bit/símbolo. Um símbolo, neste caso, é a variação de fase da portadora. Como existe a possibilidade de variação de 0° ou 180° , existem 2 símbolos. Quando a variação de fase é de 0° , sabe-se que o bit que está sendo enviado é o 1, e quando a variação é de 180° , o bit é o 0. Ou seja, através dessa modulação podemos representar 2 bits (0 e 1), através de 2 símbolos (180° e 0° de defasagem), e consequentemente, pode-se dizer que a modulação BPSK pode representar 1 bit/símbolo.

Supondo um chip rate de 11Mchips/s, a duração de transmissão de 1 *chip* é:

$$\frac{1}{11} \mu s$$

Para transmitir 11 chips do Barker Code, que é equivalente a um símbolo, são então necessários $1 \mu s$. Assim, em um segundo, é possível transmitir 10^6 símbolos. Utilizando então a modulação BPSK, que representa 1bit/símbolo, obtemos a taxa de 1 Mbit/s (1 Mega bits por segundo).

5.1.1.4 QPSK

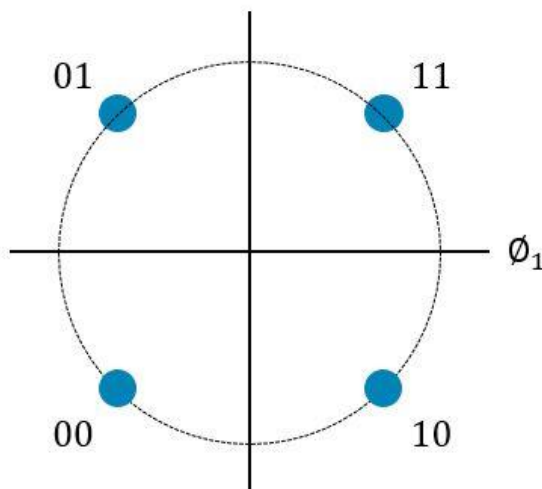
Esta técnica de modulação é utilizada em conjunto com o Barker Code para atingir taxas de 2 Mbps. QPSK vem de *Quadrature Phase Shift Keying* e ao invés de poder representar 2 símbolos como no BPSK, pode representar 4 símbolos, e estes são representados por 2 bits, como mostra o exemplo da Tabela 2:

Tabela 2 - Representação de bits com modulação QPSK

Representação de bits com modulação QPSK	
Bits	Fase
00	225°
01	135°
10	315°
11	45°

Sendo assim, pode-se desenhar o diagrama de constelações da Figura 12:

Figura 12 - Diagrama de Constelações QPSK



Fonte: (Autor, 2013)

Este diagrama demonstra que os símbolos estão defasados 90° um do outro, porém possuem a mesma amplitude. Dessa maneira, é possível codificar 2 bits/ símbolo, duas vezes mais do que o obtido no BPSK, no mesmo espaço.

Para atingir velocidades de 2 Mbps, deve-se utilizar o mesmo raciocínio abordado no item anterior. Supondo um chip rate de 11Mchips/s, a duração de transmissão de 1 chip é:

$$\frac{1}{11} \mu s$$

Para transmitir 11 chips do Barker Code, que é equivalente a um símbolo, são então necessários 1μs. Assim, em um segundo, é possível transmitir 10⁶ símbolos. Utilizando então a modulação QPSK, que representa 2bits/símbolo, obtemos a taxa de 2 Mbit/s (2 Mega bits por segundo).

A Tabela 3 a seguir resume as principais características do padrão 802.11:

Tabela 3 - Padrão 802.11

Padrão 802.11	
Estabelecido em	1997
Tecnologia RF	FHSS e DSSS
Banda de Frequência	2,4 GHz
Codificação	Barker 11
Modulação	BPSK e QPSK
<i>Data Rates</i>	1 e 2 Mbps
Canais que não se sobrepõem	1, 6, 11

5.1.2 IEEE 802.11b

O protocolo 802.11b foi desenvolvido rapidamente devido as velocidades oferecidas pelas redes cabeadas: 10 Mbps, contra 1 e 2 Mbps do 802.11. Os fabricantes foram altamente estimulados a criarem dispositivos que pudessem atingir maiores taxas de transmissão por dispositivos sem fio. Entretanto, uma preocupação sempre recorrente é em relação a interoperabilidade entre esses equipamentos. Para isso, o IEEE estabeleceu o 802.11b, que oferece maiores taxas de transmissão, chegando a 11 Mbps, com compatibilidade para 1 Mbps e 2 Mbps, utilizando a banda de 2,4 GHz ISM.

O 802.11b também utiliza a tecnologia DSSS (Direct Sequence Spread Spectrum) e atinge velocidades de 5,5 Mbps e 11 Mbps. Porém, para chegar a esses valores, ao invés de utilizar o Baker Code, utiliza uma técnica chamada de *Complementary Code Keying* e modulação QPSK (*Quadrature Phase Shift Keying*).

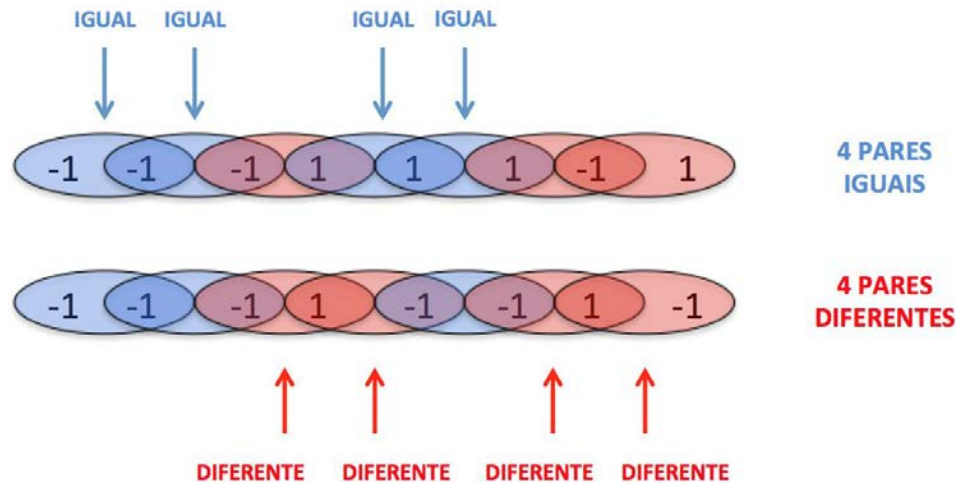
O comitê do IEEE 802.11 aprovou uma extensão, de alta velocidade, a camada física dos padrões do 802.11 das WLANs, com a intenção de fornecer taxas de transmissão similares as fornecidas pela Ethernet. A Intersil e a Lucent Technologies juntaram esforços para desenvolver um solução baseada em códigos complementares, chamada CCK (Complementary Code Keying). Em Setembro de 1998, o comitê 802.11 adotou o CCK como a base para uma extensão a camada física de alta velocidade, para atingir velocidades de até 11 Mbps. O CCK foi escolhido por oferecer características que facilitam a interoperabilidade com as taxas já existentes de 1 Mbps e 2 Mbps, como utilizar a mesma largura de banda e incorporar o mesmo *preamble* e cabeçalho para os pacotes durante a transmissão.

5.1.2.1 CCK – *Complementary Code Keying*

O CCK é uma técnica de espalhamento espectral mais avançada e complexa do que o Barker Code e que permite atingir velocidades de 5,5 Mbps e 11 Mbps. Isso é possível através de utilização de sequências de chips de 8 bits, ao invés de 11.

Essas sequências de chips de 8 bits são chamadas de sequências complementares. Elas possuem esse nome por possuir uma característica peculiar. Elas são sequências de mesmo comprimento, sendo que o número de pares de elementos iguais com uma determinada separação dentro de uma sequência é igual ao número de pares de elementos diferentes com esta mesma separação dentro da sequência complementar e vice-versa. A Figura 13 ilustra uma sequência de código complementar:

Figura 13 - Códigos Comeplementares



Fonte: (Autor, 2013)

Para atingir 5,5 Mbps, essa técnica utiliza um conjunto de 4 códigos de 8 chips cada um para codificar uma sequência de dois bits de dados. Além disso, são adquiridos mais 2 bits de dados que são utilizados para modulação de fase QPSK, resultando em um símbolo de 8 chips representando uma informação de 4 bits. Dessa maneira, podemos utilizar o mesmo raciocínio abordado para os cálculos das taxas de 1Mbps e 2 Mbps:

$$\text{Chip Rate} = 11 \text{ Mchips/s}$$

$$\text{Duração de um chip} = \frac{1}{11} \mu s$$

$$\text{Duração de transmissão de um símbolo de 8 chips} = \frac{8}{11} \mu s$$

$$\text{Taxa de transmissão de um símbolo} = \frac{11}{8} \cdot 10^6 \frac{\text{símbolos}}{s} = 1,375 \text{ Msímbolos/s}$$

Uma vez que cada símbolo codifica uma informação de 4 bits, obtemos:

$$4 \times 1,375 \text{ M} = 5,5 \text{ Mbit/s}$$

De forma similar, para atingir taxas de 11 Mbps, ao invés de utilizar 4 bits de dados, são utilizados 8 bits de dados, sendo que 6 são utilizados para selecionar uma entre 64 sequências únicas de códigos complementares compostos por 8 chips cada. Os outros dois bits, são também

utilizados para realizar a rotação do código (0° , 90° , 180° e 270°) através da modulação QPSK, resultando assim em um símbolo de 8 chips representando uma informação de 8 bits. Dessa maneira, podemos utilizar o raciocínio do item anterior para calcular a taxa de bit alcançada através desta técnica:

$$\text{Chipe Rate} = 11 \text{ Mchips/s}$$

$$\text{Duração de um chip} = \frac{1}{11} \mu s$$

$$\text{Duração de transmissão de um símbolo de 8 chips} = \frac{8}{11} \mu s$$

$$\text{Taxa de transmissão de um símbolo} = \frac{11}{8} \cdot 10^6 \frac{\text{símbolos}}{s} = 1,375 \text{ Msímbolos/s}$$

Uma vez que cada símbolo codifica uma informação de 8 bits, obtemos:

$$8 \times 1,375M = 11 \text{ Mbit/s}$$

Pode-se perceber então que a modulação utilizando CCK permite que códigos representem um maior volume de informação por símbolo. O emissor pode então enviar múltiplos bits de informação pra cada código DSSS, o suficiente para atingir taxas de bit de 11 Mbps, ao invés de 2 Mbps do padrão 802.11 original

Uma característica importante de se observar neste momento é o fato de que quanto mais distante um receptor está do emissor, menor será a taxa de bit efetiva da comunicação. Isso se deve ao fato de que quanto mais bits por símbolo está sendo amostrado, mais complexa é a modulação e em consequência disso, quanto maior a distância, maior a possibilidade da comunicação sofre ruídos, interferências e perdas de sinal, já que a demodulação fica mais sensível com a distância. Alguns equipamentos disponíveis no mercado hoje possuem um mecanismo chamado de DRS, que vem de *Dynamic Rate Shifting*. Esse recurso permite que dispositivos operando nos padrões 802.11 em 2,4 GHz mudem de velocidade de transmissão de acordo com a distância do emissor. Por exemplo, um dispositivo localizado muito próximo ao emissor está operando em 11 Mbps. Porém ao se afastar, o DRS automaticamente altera a taxa para 5,5 Mbps sem haver perda de conexão. Caso este se afaste ainda mais, o DRS altera para 2 Mbps ou até 1 Mbps se for necessário.

A Tabela 4 resume as principais características do padrão 802.11b:

Tabela 4 - Padrão 802.11b

Padrão 802.11b	
Estabelecido em	1999
Tecnologia RF	DSSS
Banda de Frequência	2,4 GHz
Codificação	Barker 11 e CCK
Modulação	BPSK e QPSK
<i>Data Rates</i>	1/2/5,5/11 Mbps
Canais que não se sobrepõem	1, 6, 11

5.1.3 IEEE 802.11g

Em junho de 2003, o IEEE estabeleceu o padrão 802.11g. Neste padrão, agora é possível atingir taxas de até 54 Mbps através de banda de 2,4 GHz. Além disso, foram adicionadas mais 7 possibilidades de taxas em adição as possíveis com o protocolo 802.11b: 6, 9, 12, 18, 24, 36 e 48 Mbps.

Este padrão é ainda compatível com o padrão 802.11b por utilizar a mesma técnica de modulação e codificação para as velocidades mais baixas, entretanto, para atingir velocidades superiores a 11 Mbps, é utilizado um conceito bastante avançado de transmissão e é utilizado com muita frequência nos dias atuais: OFDM – Orthogonal Frequency-Division Multiplexing.

Por utilizar a banda de 2,4 GHz, ainda existem somente 3 canais (1, 6 e 11) que não se sobrepõem, permanecendo aquela antiga preocupação em relação a interferências.

O tipo de modulação utilizada neste padrão são os mesmos do padrão 802.11b: BPSK e QPSK, entretanto, além de utilizar a tecnologia DSSS, para atingir altas velocidades é utilizado o OFDM. Para codificação são utilizados o Barker Code 11 e o CCK (para efeitos de compatibilidade).

5.1.3.1 OFDM – *Orthogonal Frequency-Division Multiplexing*

A taxa de transmissão de 11 Mbps ainda não era o suficiente em um planeta onde as velocidades de LANs alcançavam facilmente 100Mbps. A técnica de transmissão OFDM foi trazida de outros sistemas de transmissão RF onde já era utilizada.

Além de ser utilizada no padrão 802.11g, a técnica OFDM também é vista nos padrões mais recentes como 802.11a, 802.11n e os padrões de conexão de quarta geração como WiMAX e LTE (Long Term Evolution). OFDM é hoje a base das tecnologias de comunicação sem fio e ainda será muito utilizada por um período razoável de tempo.

Segundo Simões (2007), esta técnica, ao invés de enviar uma informação utilizando uma onda de 22 MHz de largura, divide uma onda de 20 MHz em 64 subcanais, também chamados de subportadoras, espaçadas 312,5 KHz uma da outra, através de uma função matemática chamada de Transformada Inversa Rápida de Fourier (IFFT). Os quarenta e oito (48) subcanais são individualmente modulados em fase e utilizados para representar dados vindos da aplicação. Após isso, cada símbolo modulado é combinado em um único símbolo chamado de OFDM Symbol. No lado do receptor, este OFDM Symbol é recuperado através da Transformada Rápida de Fourier (FFT), que faz a operação reversa da IFFT, trazendo de volta os símbolos modulados.

Como foi dito anteriormente, o canal de 20 MHz é dividido em 64 subportadoras, espaçadas 312,5 KHz uma da outra. Pode-se observar essa separação através da equação abaixo:

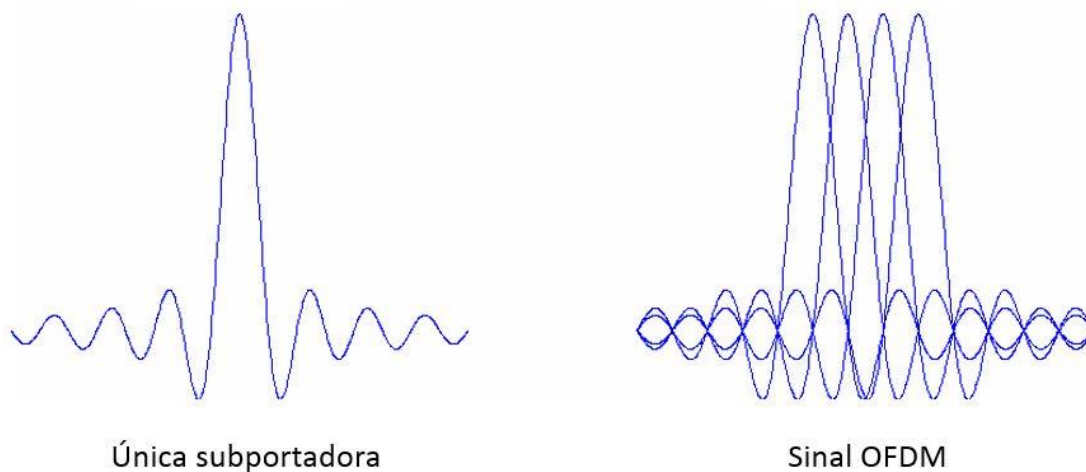
$$\frac{20 \cdot 10^6}{312,5 \cdot 10^3} = 64$$

Entretanto, nem todas essas 64 subportadoras são utilizadas para transportar dados. O 802.11g utiliza as 6 primeiras subportadoras para atuarem como uma espécie de “guardas”, isto é, proteger contra interferência de entre canais. Essas primeiras 6 subportadoras protegem o sinal contra interferências que podem ser causadas pelo canal anterior adjacente. Da mesma maneira, as 5 últimas subportadoras, que também funcionam como “guardas”, protegem contra interferências que podem ser causadas pelo próximo canal adjacente. Assim, estas 11 subportadoras estão inativas ou nulas, não transportando dados, formando o que é chamado de banda de guarda entre dois canais adjacentes. A subportadora central, também chamada de Direct Conversion Subcarrier, também

fica em estado de inatividade. Assim, dos 64 subcanais, subtraindo 12, restam agora 52 subportadoras. Destas, quatro são reservadas para serem utilizadas como Pilot Subcarriers, isto é, subportadoras que irão transportar informações referentes a tempo e frequência para auxiliar o dispositivo receptor a sincronizar o sinal recebido. Apesar destas quatro subportadoras estarem transportando dados, estes dados não são os dados da informação que está sendo transmitida de fato. Assim, dos 64 subcanais iniciais, sobram 48 para serem modulados com os dados.

Cada subportadora é então enviada defasada de 90° uma da outra (origem do nome ortogonal), de maneira que quando o sinal de uma está no máximo, o sinal das subportadoras vizinhas está no mínimo possível ou nulo. Isso reduz ou até elimina as interferências causadas pelas próprias subportadoras. A Figura 14 mostra o sinal de uma única subportadora e o espectro de um sinal OFDM no domínio da frequência:

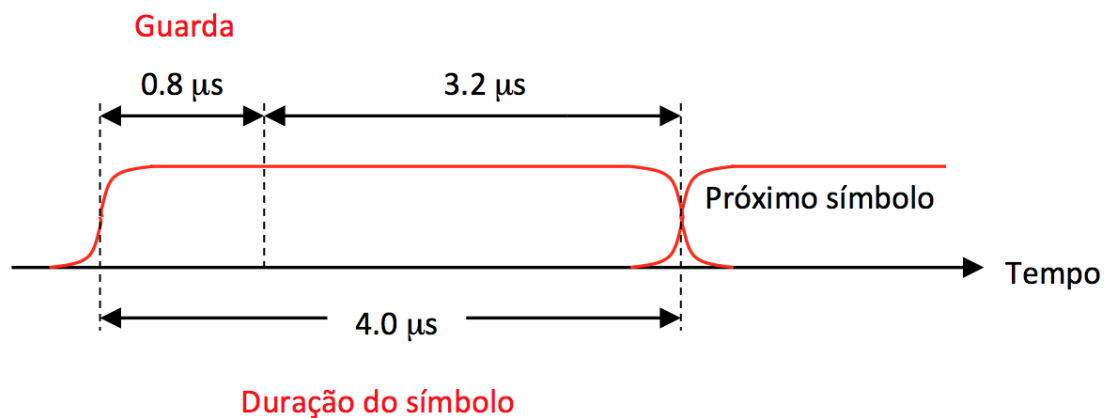
Figura 14 - Subportadora e Sinal OFDM



Fonte: (Comlab, 2013)

Um símbolo OFDM no domínio do tempo é composto por um período de guarda, com duração de $0,8 \mu s$, para evitar interferência entre símbolos e o resto do símbolo, que dura $3,2 \mu s$, totalizando uma duração de $4 \mu s$ por símbolo. A Figura 15 ilustra o sinal OFDM no domínio do tempo:

Figura 15 - Duração do símbolo OFDM



Fonte: (Autor, 2013)

Uma vez que cada símbolo OFDM tem duração de 4 μs , existem 250 000 transições de símbolos a cada segundo. Das 64 subportadoras, 48 são utilizadas para carregar dados. Cada subportadora realiza 250 000 transições de símbolos por segundo. Sendo assim, para todo o canal, podemos realizar o seguinte cálculo:

$$250\,000 \cdot 48 = 12\,000\,000$$

ou

$$250\,000 \text{ símbolos/s/subportadora} \cdot 48 \text{ subportadoras} = 12\,000\,000 \text{ símbolos/s}$$

Ou seja, por canal, de 20 MHz de largura, é possível obter uma taxa de 12 000 000 símbolos/s. O termo símbolos por segundo também é conhecido como *baud rate*, que é definido como: o número de transições de símbolos distintos realizadas em um meio por segundo. Assim, a taxa máxima de transmissão no caso é 12 000 000 baud ou 12Mbd.

A relação baud rate e data rate nem sempre é de 1 pra 1. As vezes as duas taxas são iguais, porém existem ocasiões em que isso não ocorre. O baud rate é o número de transição de símbolos por segundo, enquanto data rate é determinado pelo tipo de modulação que está sendo utilizado para produzir esse símbolo. Existem técnicas de modulação que podem representar mais de um bit por símbolo, fazendo com que a taxa de bit seja maior do que o baud rate.

Dependendo da qualidade de cada canal, o padrão 802.11g seleciona um entre quatro técnicas de modulação possíveis:

- BPSK
- QPSK
- 16 QAM
- 64 QAM

As modulações BPSK e QPSK, como foram explicados anteriormente, podem representar 1 ou 2 bits por símbolo respectivamente. A modulação BPSK é a mais simples e por isso pode se propagar por uma distância superior aos outros métodos. Esta técnica é utilizada quando a qualidade e as condições de um determinado canal são ruins devido a interferências ou os dispositivos emissor e receptor estiverem muito longe um do outro. No caso do BPSK, é possível dizer que o baud rate é igual ao bit rate. Isso se deve a possibilidade de representar apenas 1 bit por símbolo. Assim, pode-se concluir que utilizando a modulação BPSK, é possível atingir taxas de bit de 12 Mbps.

A modulação QPSK é utilizada quando as condições de um determinado canal são um pouco superiores as encontradas quando utilizado o BPSK. A modulação QPSK pode representar 2 bits por símbolo, fazendo com que o baud rate e o bit rate não sejam iguais. Utilizando a modulação QPSK, é possível atingir taxas de 24 Mbps.

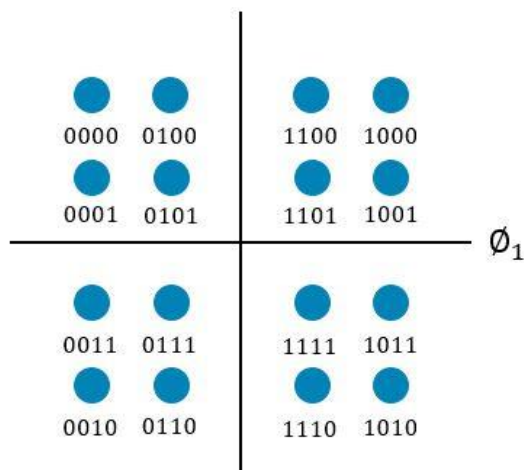
5.1.3.2 QAM – Quadrature Amplitude Modulation

Para alcançar taxas ainda maiores, é necessário abandonar as técnicas de modulação BPSK e QPSK, que representam um e dois bits por símbolo respectivamente, e utilizar uma técnica chamada de Quadrature Amplitude Modulation – QAM. Essa modulação altera a amplitude e a fase da onda para representar bits. Além das quatro fases possíveis através da modulação QPSK (0° , 90° , 180° e 270°), a modulação QAM adiciona quatro níveis de amplitude (muito baixo, baixo, médio e alto) para serem utilizados juntamente com as alterações de fase. Quatro amplitudes vezes quatro possíveis fases resultam em 16 possibilidades, ou seja, 16 símbolos. Essa quantidade de símbolos dá o nome a primeira variante desse tipo de modulação: 16-QAM. Essa variante permite

que 4 bits sejam representados por um único símbolo, já que existem 16 possíveis combinações entre fase e amplitude.

Através do diagrama de constelações da Figura 16, é possível entender de forma mais clara os símbolos representados pela modulação 16 QAM.

Figura 16 - Diagrama de Constelações 16 QAM

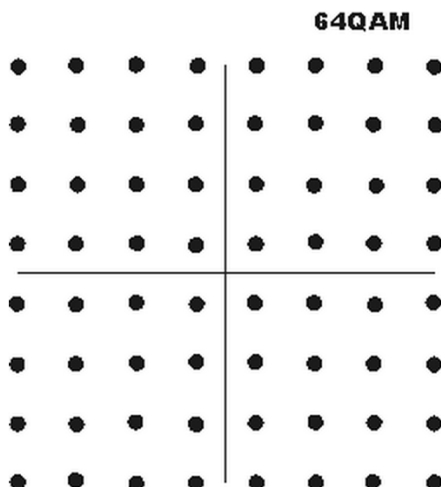


Fonte: (Autor, 2013)

Uma outra variante é a modulação 64 QAM. Esta técnica permite representar 6 bits por símbolo, já que existem 64 símbolos possíveis. Esses símbolos são resultados da combinação de alterações de fase e amplitude dos sinais da portadora. Esse tipo de modulação exige que o hardware demodulador seja de altíssima sensibilidade, uma vez que muitos bits estão sendo representados por símbolos, e estes, são muito semelhantes entre si, já que existe uma pequena variação de fase e amplitude entre eles.

O diagrama de constelações da Figura 17 ilustra os símbolos que podem ser representados:

Figura 17 - Diagrama de Constelações 64 QAM



Fonte: (Ian Poole, 2013)

Os diagramas de constelação da modulação QAM se diferem dos diagramas do BPSK e QPSK pelo fato de possuir variações na amplitude, além de variações na fase. O diagrama do BPSK possui apenas dois pontos opostos em fase um do outro. Já o diagrama do QPSK apresenta quatro pontos, indicando que podem ser representadas quatro fases, ao invés de apenas duas. Já que existem quatro símbolos disponíveis, são necessários 2 bits (2^2) para representá-los. Já nos diagramas QAM, os pontos não estão mais somente diferindo em fase, mas também em amplitude. Essa combinação faz com que uma determinada fase juntamente com uma determinada amplitude faça a representação de um símbolo. Quanto mais combinações de fase e de amplitude são feitas, maior é o nível de complexidade da modulação QAM. 64 QAM significa 64 possíveis combinações de fase e amplitude. Para representar 64 símbolos, são então necessários 6 bits ($2^6 = 64$), e é por isso que se diz que para cada símbolo, é representado por 6 bits, ou 6 bits/símbolo.

Quanto mais bits por símbolo, mais eficiente é a transmissão, já que mais bits são transmitidos em uma mesma largura de banda. Entretanto, quanto mais bits representados em um único símbolo, mais robusto tem de ser o modulador e o demodulador, visto que eles terão de “inserir” ou “extrair” mais informações de um “recipiente” pequeno. Além disso, quanto maior a interferência e maior a distância que o sinal irá percorrer, maior são as chances de haver perdas de conteúdo ou algum erro nos dados transmitidos. No caso de se utilizar uma modulação muito complexa, onde são carregados muitos bits em um único símbolo, maiores são as perdas ao

aumentar a distância. Por esses motivos, a modulação QAM é utilizada sob boas condições do canal e a pequenas distâncias, e as modulações BPSK e QPSK utilizadas em distâncias maiores e piores condições do meio.

Sabendo que o baud rate é de 12 Mbd, podemos então calcular as taxas de bit em cada tipo de modulação, através da Tabela 5:

Tabela 5 - Comparação entre técnicas de modulação

Comparação entre técnicas de modulação				
Modulação	Símbolos	Bits/símbolo	Baud Rate	Bit Rate
BPSK	2	1	12 Mbd	12 Mbps
QPSK	4	2	12 Mbd	24 Mbps
16 QAM	16	4	12 Mbd	48 Mbps
64 QAM	64	6	12 Mbd	72 Mbps

Essas taxas calculadas, entretanto, não as taxas finais, visto que as taxas disponíveis no padrão 802.11g são: 9, 12, 18, 24, 36 e 48 Mbps. Essa diferença se deve a um mecanismo de correção de erros do OFDM chamado de Convolution Codes. Essa técnica permite a recuperação de um dado mesmo que tenha ocorrido problemas na transmissão devido a interferência de canais. O resultado desse processo é um código que representa o dado original, porém em uma tamanho maior e mais facilmente recuperado em caso de interferências.

A técnica de Convolution Codes realiza operações matemáticas para transformar os bits de dados originais em bit redundantes, antes da transmissão. Este processo pode ser realizado utilizando diversos métodos, entre eles:

- Generator Format
- Decision Tree Format
- State Format
- Trellis Format

Para fins didáticos, será abordado a seguir o método Decision Tree Format empregando uma taxa de 1/2 de codificação, ou seja, cada bit original de dado será representado por dois bits.

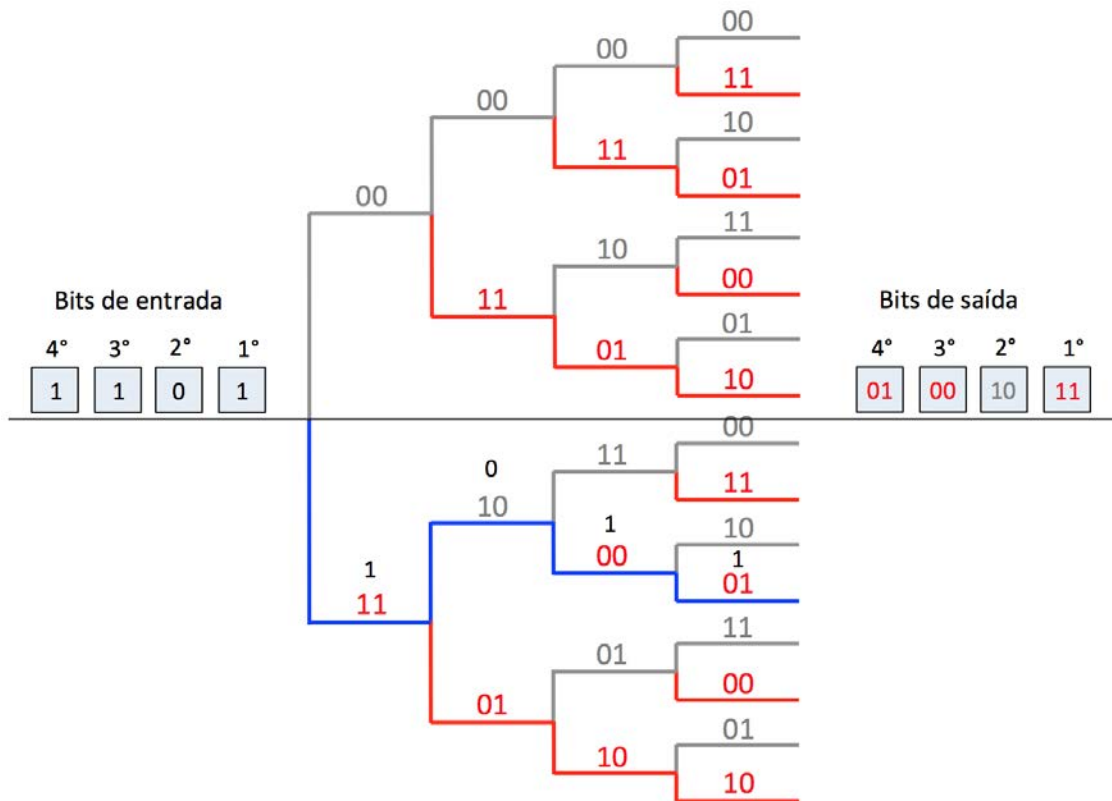
Existe também a possibilidade de se representar cada dois bits originais por três bits ($2/3$) e três bits originais por 4 bits ($3/4$). Esses dois últimos casos são bastante complexos e extensos e levam o mesmo raciocínio do de taxa de $1/2$.

Utilizando a codificação de taxa $1/2$, cada par de bits de saída representa um bit original. Transmitir um par de bits ao invés de um único bit requer o dobro de largura de banda, porém a vantagem é a confiabilidade na recuperação desse bit em caso de erros ou perdas. Uma vez que um par de bits requer o dobro de largura de banda, utilizar a taxa de codificação $1/2$ reduz a taxa do canal em 50%. Utilizar a taxa de $2/3$, ou seja, para cada 2 bits originais, utilizar 3 bits para representá-los, diminui a taxa do canal em 33%. Já a taxa de $3/4$, reduz a taxa de transmissão do canal em 25%. Sob condições não favoráveis a melhor escolha é utilizar o método de codificação que diminui mais a taxa de transmissão do canal, porém, fornece maior confiabilidade na hora de recuperar bits corrompidos.

O método Decision Tree utiliza uma árvore de valores binários que é percorrida passo a passo. Os bits de dados de entrada são separados em pequenos grupos (quatro bits por grupo, no exemplo abaixo), adquiridos sequencialmente do fluxo de dados. Para processar esse grupos de bits, haverá quatro paradas no decorrer da árvore até chegar ao seu pé. Em cada parada, deve-se fazer uma decisão: seguir para cima ou para baixo. Esta decisão irá determinar qual par de bit irá representar o bit em questão. Os pares de bits são atribuídos previamente em cada nível e não possuem uma ordem lógica, uma vez que são geradas através da lógica booleana.

A Figura 18 mostra a árvore utilizada para codificação dos bits em pares de bits:

Figura 18 - Decision Tree



Fonte: (Autor, 2013)

Neste exemplo, os bits de dados “1011” serão inseridos na árvore da esquerda para a direita e farão escolhas baseados no bit que está sendo processado. Se o bit for 0, a decisão será seguir para cima, e se o bit for 1, será ir para baixo. As linhas em verde representam as decisões tomadas pelo bit 0 e as linhas em cinza representam as decisões tomadas pelo bit 1. A sequência de codificação segue abaixo:

1. O bit 1 da esquerda será o primeiro a ser codificado. Por ser o bit 1, na primeira parada sua decisão será ir para baixo. Desse modo, o par de bits que irá representar este bit 1 será o indicado na parte de baixo da primeira parada: “11”. Esse par será armazenado e será utilizado como a primeira saída da sequência de bits.
2. O segundo bit de dados 0, continuará o caminho iniciado pelo primeiro bit, ou seja, continuará na metade de baixo da árvore, na segunda parada. Por ser o bit 0, deverá ir para cima e será representado, então, pelo par de bit “10”.

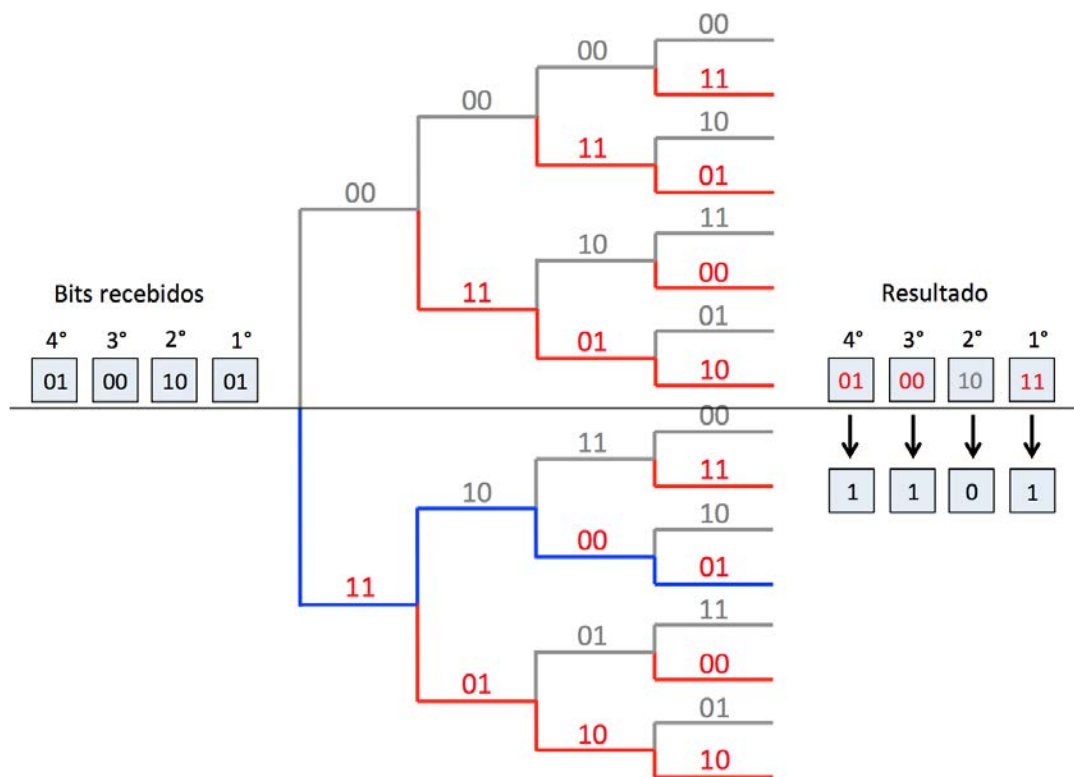
3. O terceiro bit, no caso o 1, irá continuar o caminho na terceira parada, e por ser 1, irá para baixo e será representado pelo par de bit “00”.
4. Já o quarto e último bit 1, irá também continuar o caminho já traçado e irá para a última parada. Por ser 1, também irá para baixo e será representado pelo par “01”.

Assim, o processo se conclui e a sequência resultante é: “11 10 00 01”. Essa sequência representa os quatro bits originais, e será enviada ao modulador para a transmissão.

A sequência de bits que será transmitida tem o dobro de tamanho da sequência original, fazendo com que a velocidade seja reduzida pela metade. Entretanto, essa redundância adiciona uma camada de resistência a interferência. Supondo que essa sequência de bits chegou ao demodulador com uma pequena alteração devido a interferências e ao invés da sequência correta, foi recebido “01 10 00 01”. Neste caso, o primeiro par de bits foi recebido com um erro. O receptor, no entanto, não sabe qual é o bit que contém um erro, porém ele sabe que está sendo utilizado a técnica de *Convolution Code* com taxa de $\frac{1}{2}$. Desse modo, este se prepara para decodificar a sequência utilizando a árvore de decisões com essa taxa.

Na decodificação, ocorre um processo similar ao de codificação, porém, ao invés de os bits entrarem na árvore de modo individual, são os pares de bits que vão determinar o caminho a ser tomado, como mostra a Figura 19. Já que o receptor não sabe quando uma determinada decisão foi tomada corretamente, ele terá que tratar todas as possibilidades e depois realizar um cálculo para averiguar qual caminho tem o maior número de acertos.

Figura 19 - Decision Tree para decodificação



Fonte: (Autor, 2013)

O primeiro par a entra na árvore é o “01“. Ele será testado com ambos os caminhos disponíveis da árvore no primeiro nível para ver se existe alguma correspondência. Neste caso, não há nenhuma correspondência e a única coisa a se fazer é pular para o próximo par.

O próximo par de bits é “10“. Ele será enviado a árvore e será verificado todas os caminhos possíveis até o segundo nível. Neste ponto, uma correspondência é encontrada na metade de baixo da árvore. Vale lembrar que o receptor não tem como saber se esta correspondência é correta e assim ele guarda esse resultado até que todos os bits tenham sido processados.

O terceiro par é o “00“. Novamente, todos os caminhos possíveis até chegar no terceiro nível são verificados. Neste caso, duas correspondências são encontradas: uma na metade de cima e outra na metade de baixo da árvore. Este resultado também é armazenado e o processamento continua.

O quarto e último par a entrar na árvore é o “01“. Todos os caminhos são também verificados até o quarto nível da árvore. Neste caso, existem quatro correspondências: duas na metade superior e duas na metade inferior da árvore de decisões.

Para finalizar, o decodificador compara todos os resultados para verificar quais dos caminhos possui o maior número de correspondências. Neste caso, o caminho que vai para baixo, depois para cima, para baixo e por último para baixo é o vencedor, o que vem a ser a sequência original de par de bits antes da transmissão: “11 10 00 01“.

Assim, para obter a sequência dos bits de dados, o decodificador simplesmente mapeia a direção tomada na árvore atribuindo “0“para cima e “1“para baixo, resultando em : baixo (“1“), cima (“0“), baixo (“1“) e baixo (“1“), que no fim é: “1011“.

Este caso mostra um simples exemplo de como funciona a técnica de *Convolution Codes*. Entretanto, em situações reais, muitas dessas adivinhações podem não ser a correta, especialmente em casos onde existem mais do que 1 bit errado.

Neste exemplo, foi utilizado a taxa de $\frac{1}{2}$ para codificação, ou seja, qualquer bit de dados será representado por dois bits, fazendo com que a velocidade de transmissão seja reduzida pela metade. Além desta, existem as taxas de $\frac{2}{3}$ e $\frac{3}{4}$. Essa redundância de bits é o que determina a velocidade final de transmissão utilizando a técnica OFDM. Na Tabela 5 foram calculados alguns valores, porém aqueles não representam os valores reais de transmissão do padrão 802.11g, pois não foi levado em consideração essa técnica de codificação. A seguir, a Tabela 6 mostra as velocidades reais do padrão 802.11g, de acordo com a técnica de modulação e a taxa de codificação:

Tabela 6 - Taxa de Transmissão 802.11g

Taxas de transmissão 802.11g					
Modulação	Símbolos	Bits/símbolo	<i>Baud Rate</i>	<i>Coding Rate</i>	Bit Rate
BPSK	2	1	12 Mbd	1/2	6 Mbps
BPSK	2	1	12 Mbd	3/4	9 Mbps
QPSK	4	2	12 Mbd	1/2	12 Mbps
QPSK	4	2	12 Mbd	3/4	18 Mbps
16 QAM	16	4	12 Mbd	1/2	24 Mbps
16 QAM	16	4	12 Mbd	3/4	36 Mbps
64 QAM	64	6	12 Mbd	2/3	48 Mbps
64 QAM	64	6	12 Mbd	3/4	54 Mbps

A Tabela 7 a seguir resume as principais características do padrão 802.11g

Tabela 7 - Padrão 802.11g

Padrão 802.11g	
Estabelecido em	2003
Tecnologia RF	DSSS e OFDM
Banda de Frequência	2,4 GHz
Codificação	Barker 11 e CCK
Modulação	BPSK e QPSK
<i>Data Rates</i>	1/2/5,5/11 Mbps com DSSS e 6, 9, 12, 18, 24, 36, 48 e 54 Mbps com OFDM
Canais que não se sobrepõem	1, 6, 11

5.1.4 IEEE 802.11a

O padrão 802.11a foi estabelecido em 1999, quatro anos antes do estabelecimento do 802.11g. Seu principal objetivo naquela época era evitar interferências de outros dispositivos que utilizavam a banda de 2,4 GHz (*Bluetooth*, fornos de microondas, telefones sem fio, etc), já que

esta é uma banda ISM. A principal diferença e característica do 802.11a é o fato de utilizar a banda de 5,0 GHz, exclusiva para WLANs (naquela época), ao invés da de 2,4 GHz.

Este padrão oferece até 23 canais que não se sobrepõem, contra apenas 3 do 802.11b/g. Essa característica facilita muito no desenho de uma solução e evita em muitas ocasiões interferências de células adjacentes que podem prejudicar o desempenho da rede wireless, além de aumentar a capacidade e escalabilidade da solução.

Os canais são também separados por 20 MHz, possibilitando o uso do OFDM e *Convolution Code* como método de correção de erros.

Em geral, a única característica diferente ao padrão 802.11g é o fato de utilizar a banda de 5,0 GHz para reduzir problemas de interferências, já que também utiliza as técnicas de modulação BPSK, QPSK, 16 QAM e 64 QAM e atinge os mesmos *data rates*.

A banda de frequência de 5,0 GHz é dividida em várias partes, com 100MHz cada, chamadas de *Unlicensed National Information Infrastructure (UNII)*, que foram designadas para diferentes aplicações cada. A Tabela 8 mostra os diferentes usos dessas frequências:

Tabela 8 - Utilização das frequências de 5,0 GHz

<i>Unlicensed National Information Infrastructure (UNII)</i>			
Banda	Frequência	Utilização	Canais
UNII - 1	5,150-5,250 GHz	<i>Indoor</i> , com antena interna	36, 40, 44 e 48
UNII - 2	5,250-5,350 GHz	<i>Indoor/Outdoor</i> , com possibilidade de antena externa	52, 56, 60 e 64
UNII – 2e	5, 470-5,725 GHz	<i>Indoor/Outdoor</i> , com possibilidade de antena externa	100, 104, 108, 112, 116, 120, 124, 128, 132 e 136
UNII - 3	5,725-5,825 GHz	<i>Indoor/Outdoor</i> , com possibilidade de antena externa	149, 153, 157, 161 e 165

O padrão 802.11a não teve tanta aceitação quanto os padrões 802.11b e 802.11g. Isto se deve a um simples motivo: a utilização da faixa de 5,0 GHz. Utilizar o padrão 802.11b faz com que os clientes 802.11 original ainda sejam suportados. Migrar para 802.11g faz com que os clientes 802.11b também sejam suportados, entretanto, mudar para 802.11a surge a necessidade de substituir todas as antenas e placas de redes de todos os usuários para o padrão 802.11a, já que este utiliza uma faixa de frequência diferentes dos outros padrões. Resumindo, a pouca aceitação se deve a incompatibilidade do padrão 802.11a com os padrões anteriores.

Uma outra característica bastante importante deste padrão é o fato de o sinal em 5,0 GHz sofrer uma maior atenuação ao atingir obstáculos, em comparação a banda de 2,4 GHz. Em consequência disso, ao planejar um ambiente RF, se faz necessário a instalação de uma maior quantidade de antenas para cobrir todo o local.

5.1.5 IEEE 802.11n

O padrão 802.11n foi publicado em 2009 com o objetivo de aumentar as taxas de transmissão existentes naquela época. Para isto, o 802.11n conta com três importantes recursos:

- Possibilidade de utilizar um intervalo de guarda mais curto: 400 ns ao invés de 800 ns. Isto pode aumentar a taxa de transmissão significativamente, porém pode aumentar o risco de interferências em ambientes com muitos dispositivos utilizando a mesma banda de frequência. O intervalo de guarda é o intervalo de tempo entre dois símbolos em uma transmissão, utilizados para minimizar interferências entre símbolos adjacentes. Essa redução permite transmitir mais símbolos por unidade de tempo, aumentando significativamente a performance da transmissão.
- Agregação de canal: possibilidade de juntar dois canais adjacentes de 20 MHz para formar um de 40 MHz. Isso faz com que mais suportes estejam disponíveis para transmissão de dados, duplicando as taxas de transferência por canal;
- MIMO: *Multiple Input Multiple Output*. Este recurso é explicado no item a seguir.

5.1.5.1 MIMO – Multiple Input Multiple Output

Segundo Haykin (2008) este mecanismo pode ser descrito simplesmente pelo fato de utilizar múltiplas antenas no mesmo canal para transmitir e receber ao mesmo tempo, possibilitando diversos melhoramentos:

- *Transmit Beamforming*: um determinado emissor envia o mesmo sinal através de mais de uma antena. Através do mapeamento deste sinal baseado nas informações enviadas pelo dispositivo 802.11n receptor, o emissor consegue direcionar os sinais de modo que estes sejam recebidos em fase, e em consequência disso, aumenta a potência do sinal recebido, permitindo maiores distâncias e maiores taxas de transmissão.
- *Spatial Multiplexing*: um emissor pode enviar diferentes sinais simultaneamente através de mais de uma antena. O receptor 802.11n irá receber todos esses sinais em todas as suas antenas, sendo que, cada antena irá decodificar separadamente cada sinal recebido. Após isso, cada sinal recebido será combinado com os sinais das outras antenas, resultando em uma maior taxa de transmissão. Cada sinal diferente enviada em uma determinada antena é chamado de *spatial stream*.

Através destas técnicas, é possível atingir, por exemplo, taxas de 300 Mbps, com dois *spatial streams*, intervalo de guarda reduzido e canais de 40 MHz. O quadro 1 mostra alguns dos possíveis *data rates* alcançados pelo padrão 802.11n, onde GI significa intervalo de guarda (*Guard Interval*, em inglês):

Quadro 1 – Data rates do padrão 802.11n

<i>Spatial Streams</i>	Modulação	<i>Coding rate</i>	<i>Data rate</i>			
			Canal de 20 MHz		Canal de 40 MHz	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI
1	BPSK	1/2	6,50	7,20	13,50	15,00
1	QPSK	1/2	13,00	14,40	27,00	30,00
1	QPSK	3/4	19,50	21,70	40,50	45,00
1	16 QAM	1/2	26,00	28,90	54,00	60,00
1	16 QAM	3/4	39,00	43,30	81,00	90,00
1	64 QAM	2/3	52,00	57,80	108,00	120,00
1	64 QAM	3/4	58,50	65,00	121,50	135,00
1	64 QAM	5/6	65,00	72,20	135,00	150,00
2	BPSK	1/2	13,00	14,40	27,00	30,00
2	QPSK	1/2	26,00	28,90	54,00	60,00
2	QPSK	3/4	39,00	43,30	81,00	90,00
2	16 QAM	1/2	52,00	57,80	108,00	120,00
2	16 QAM	3/4	78,00	86,70	162,00	180,00
2	64 QAM	2/3	104,00	115,60	216,00	240,00
2	64 QAM	3/4	117,00	130,00	242,00	270,00
2	64 QAM	5/6	130,00	144,40	270,00	300,00
3	64 QAM	5/6	195,00	216,70	405,00	450,00

5.1.5.2 Compatibilidade com padrões anteriores

O padrão 802.11n utiliza tanto a faixa de 2,4 GHz quanto a de 5,0 GHz, sendo assim compatível com os padrões 802.11b/g/a. Entretanto, algumas restrições se aplicam ao projetar uma solução utilizando esse padrão. A solução ideal, que atingiria a melhor performance, seria utilizar uma rede com dispositivos somente 802.11n em 5,0 GHz, já que esta faixa oferece mais canais e menos interferência se comparada a faixa de 2,4 GHz. Porém, uma rede somente 802.11n seria impraticável para clientes 802.11b/g. Desse modo, pode-se pensar em uma rede mista, ou seja, 802.11b/g/n e a utilização de antenas *dual-band*, ou seja, que trabalham tanto em 2,4 GHz e 5,0 GHz, ao mesmo tempo. Entretanto, misturar clientes utilizando diferentes padrões pode não ser uma boa prática.

Quando existem clientes 802.11n na banda de 2,4 GHz junto com clientes 802.11b e 802.11g, ocorre uma significativa perda de performance para os usuários 802.11n. Isto ocorre porque os clientes de padrão mais antigos não entendem as transmissões realizadas a taxas mais altas, e para isso, a rede deve ser configurada corretamente para suportar todos os padrões. Dessa maneira, quando uma antena envia um determinado dado para um cliente 802.11n, a primeira parte dessa transmissão, o cabeçalho, deve alertar a todos os clientes que esse dado tem como destino um cliente 802.11n e será utilizado uma alta taxa de transmissão e assim clientes 802.11b e 802.11g podem ignorar o resto desta transmissão. Entretanto, para que isso funcione de maneira adequada, o cabeçalho deve ser enviado a uma velocidade na qual os clientes 802.11b e 802.11g possam entender, ou seja, a baixas velocidades. Isso significa que os clientes 802.11n devem esperar um pouco mais do que deveriam esperar se não houvessem clientes utilizando padrões mais antigos.

Para isso, existe uma solução utilizada por algumas empresas chamada de band steering. Esse recurso funciona somente se a antena possui dois rádios, um 2,4 GHz e outro 5,0 GHz. O band steering aloca todos os clientes 802.11n na faixa de 5,0 GHz, onde os clientes 802.11b/g não podem ir, e deixa estes na frequência de 2,4 GHz. Assim, os clientes 802.11n podem operar em suas velocidades máximas.

5.1.6 IEEE 802.11ac

Este padrão começou a ser desenvolvido em 2011 e atualmente está em processo de melhoria. Entretanto, em 2013, já foram iniciadas as vendas dos primeiros equipamentos com suporte a este padrão.

O 802.11ac fornece uma enorme benefícios com base nas melhoras obtidas através dos recursos do 802.11n:

- Ao invés de possibilitar a agregação de canais para formar um único canal de 40 MHz como no 802.11n, agora é possível formar canais de 80 ou até 160 MHz de largura, possibilitando aumentos de até 333% na taxa de transmissão.
- Além da técnica de modulação 64 QAM, com o 802.11ac é possível utilizar uma técnica mais densa, 256 QAM. Esta técnica permite representar 8bits/símbolo, aumentando assim a eficiência espectral.

- Mais *spatial streams*. O padrão 802.11n permitia até 4 *spatial streams*, enquanto o 802.11ac agora permite até 8 *spatial streams*, aumentando a performance em mais 100%.
- Também utiliza a frequência de 5,0 GHz, que é menos suscetível a interferências e ainda possui mais canais que não se sobrepõem do que a banda de 2,4 GHz.

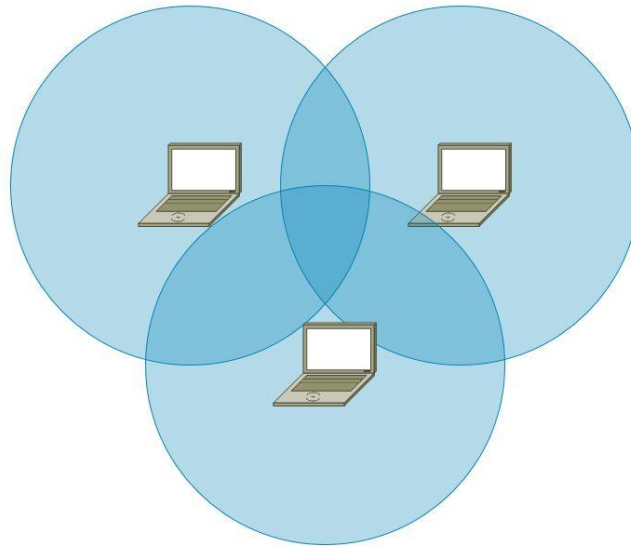
6 TOPOLOGIAS E TERMINOLOGIA

Assim como existem as LANs (*Local Area Networks*), MANs (*Metropolitan Area Networks*) e as WANs (*Wide Area Networks*), para as redes sem fio existem as redes análogas: WLANs (*Wireless Local Area Networks*), WMANs (*Wireless Metropolitan Area Networks*) e as WWANs (*Wireless Wide Area Networks*). Podemos classificá-las da seguinte forma:

- WLAN: Conexão em até 100m de distância, como escritórios e empresas, utilizando as bandas de 2,4 GHz e 5,0 GHz, conectando vários clientes ao mesmo tempo;
- WMAN: Estende a área de cobertura para áreas geográficas maiores do que a WLAN, como subúrbios e cidades. Suas aplicações podem variar de ponto-a-ponto para ponto-multiponto, onde vários usuários se conectam ao mesmo tempo. WMANs geralmente utilizam frequências licenciadas. WiMAX é um exemplo de implementação de WMAN.
- WWAN: Fornece conectividade para uma área bastante extensa. WWANs são utilizadas por operadoras de telefonia móvel para fornecer serviços de voz e dados, através de frequências licenciadas.

Além dessas citadas acima, existem topologias mais específicas. A mais básica e de fácil implementação é a chamada de *ad hoc network*. Esta topologia é utilizada quando alguns dispositivos perto um do outro precisam se comunicar de forma bastante simples, porém com uma cobertura limitada. Para isso, uma das estações define os parâmetros de RF e o nome da conexão, enquanto os outros só precisam detectar a conexão e ajustar seus próprios parâmetros para iniciar a conexão com o primeiro dispositivo. Neste caso, não é necessário um dispositivo central para permitir ou controlar a comunicação, dessa forma, não existe muito controle ou métodos de acesso como autenticação. Quando dispositivo wireless se conectam a outro através desta rede wireless, é formado uma *Basic Service Set* (BSS), e como neste tipo de conexão não existe um dispositivo central, além das próprias estações, essa rede também é chamada de *Independent Basic Service Set* (IBSS). A Figura 20 ilustra uma IBSS:

Figura 20 - Independent Basic Service Set



Fonte: (Autor, 2013)

Como dito anteriormente, redes *ad hoc* são limitadas em funcionalidades e segurança porque não existe um dispositivo central controlando a comunicação e decidindo algumas regras, como parâmetros de RF, prioridades, redundância e até área de cobertura. Para realizar todas essas funções de controle, é utilizado um dispositivo chamado de *Access Point*, ou simplesmente AP.

Os dispositivos *wireless* enviam sinais para um AP, que por sua vez, envia o sinal para o dispositivo de destino, que pode estar presente tanto na rede *wireless*, quanto na rede cabeada. Um AP age similarmente a um hub, onde somente um dispositivo por vez pode enviar informações, formando uma rede half-duplex.

Um AP oferece uma BSS e não uma IBSS, já que ele é o dispositivo central que controla a comunicação. A área coberta por um *Access Point* é chamada de *Basic Service Area* (BSA) ou célula de cobertura. Devido ao fato de os clientes se comunicarem a um dispositivo central, este tipo de rede é chamado de *infrastructure mode*, ao invés de *ad hoc*.

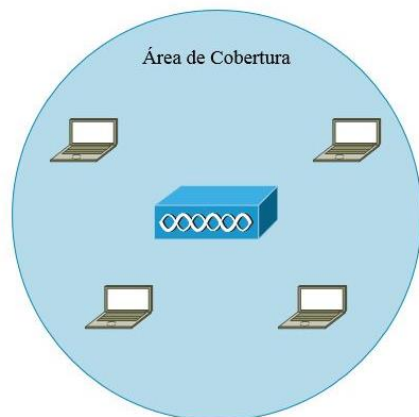
A Figura 21 mostra como um AP é representado em uma topologia e a Figura 22 ilustra uma BSA:

Figura 21 - Representação de um Access Point em uma topologia



Fonte: (Cisco, 2013)

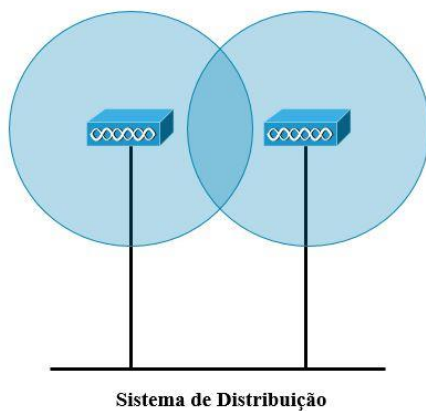
Figura 22 - Basic Service Area (BSA)



Fonte: (Autor, 2013)

Existe também uma outra sub-topologia do modo infraestrutura: *Extended Service Set* (ESS). Essa topologia compreende dois ou mais APs conectados por um sistema de distribuição, como mostra a Figura 23.

Figura 23 - Extended Service Set (ESS)



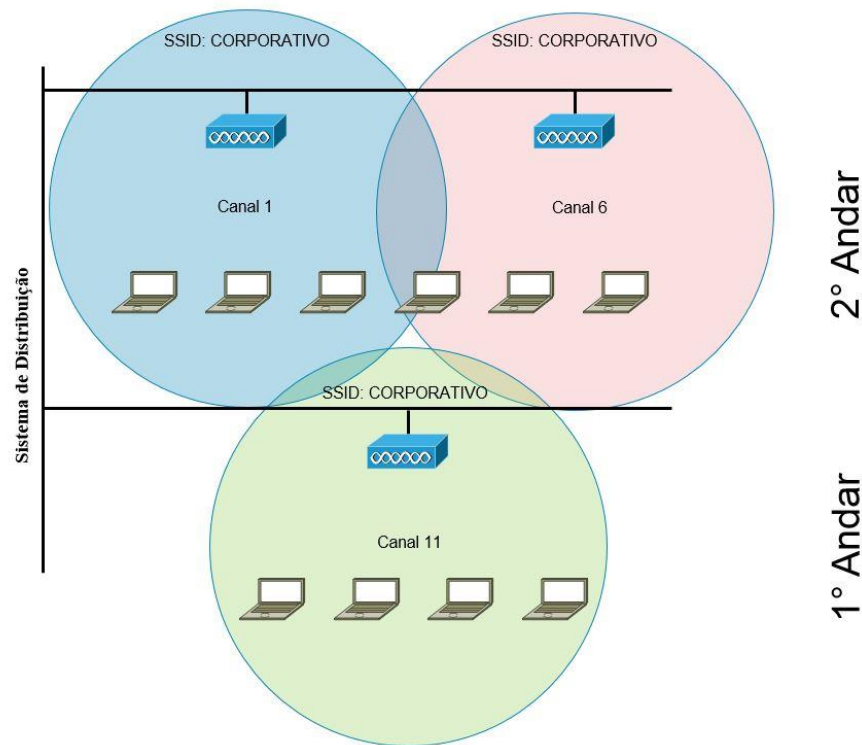
Fonte: (Autor, 2013)

Quando um cliente sai da área de cobertura de um AP no qual estava conectado e entra no BSA de outro AP, o cliente sofre um processo chamado de *roaming*. BSAs vizinhas geralmente trabalham em canais diferentes para evitar problemas com interferências. Para que um cliente detecte que um AP vizinho oferece a mesma conexão oferecida pelo AP antigo, é utilizado um nome para identificar uma conexão *wireless*, chamado de *Service Set Identifier* (SSID). APs vizinhos que oferecem a mesma conexão e os mesmos parâmetros, utilizam o mesmo SSID, entretanto, cada AP se identifica na rede através do seu endereço Camada 2, chamado de *Basic Service Set Identifier* (BSSID), o que possibilita que cada estação saiba qual AP oferece qual SSID.

Uma outra característica bastante importante de *Access Points* é o fato de haver a possibilidade de um único AP propagar mais de um SSID. Este recurso é bastante útil no caso de haver a necessidade de oferecer serviços e métodos de autenticação diferentes para cada SSID. Um exemplo disso é a rede *wireless* em uma determinada empresa. Os APs podem ser configurados para propagar uma rede corporativa e outra rede para visitantes. As estações que se conectam a rede corporativa tem acesso a todos os arquivos da empresa, bem como *hardwares* e serviços, enquanto as estações que se conectarem à rede para visitantes terão acesso restrito a esses recursos, geralmente limitando somente para acesso à internet. Obviamente, os métodos de autenticação para a rede corporativa são muito mais robustos e complexos do que para a rede de visitantes. Desse modo, ao invés de instalar dois APs, um para rede corporativa e outra pra rede de visitantes, é utilizado somente um AP propagando dois SSIDs: Corporativo e Visitantes. Assim, quando um determinado usuário se conectar a um desses SSIDs, ele terá à disposição os recursos liberados para aquele SSID.

Atualmente, a maioria das empresas e até em ambientes domésticos e industriais, é utilizado a topologia ESS, ou seja, múltiplos *Access Points* propagando diversos SSIDs pelos diversos ambientes do local. Assim, um usuário pode se conectar a rede independentemente do AP no qual ele está associado, já que todos irão propagar aquele mesmo SSID, além disso, ao migrar de uma BSA para outra, este usuário não sofrerá interrupção da conexão já que o processo de *roaming* é configurado para ser transparente para o cliente. A Figura 24 mostra um exemplo bastante comum de topologia para um ambiente corporativo, cujo escritório possui, por exemplo, dois andares:

Figura 24 - Exemplo de topologia de uma rede coporativa



Fonte: (Autor, 2013)

Neste exemplo todos os três APs propagam o mesmo SSID, entretanto, dois estão localizados no 2º andar e um no 1º andar, mas todos conectados ao mesmo sistema de distribuição da empresa, que no fim são os switches e roteadores responsável por conectar os dispositivos *wireless* a todos os outros componentes da rede cabeada, bem como prover acesso a internet. No 2º andar, existem dois APs adjacentes um ao outro. Neste caso, é recomendado instalar os APs de modo que o sinal deles se sobreponham de 10% a 15 %, com o objetivo de tornar o processo de *roaming* entre APs transparente. Assim, quando um usuário estiver conectado ao AP da esquerda e se locomover em direção ao AP da direita, o sinal recebido da primeira antena irá diminuir enquanto o da segunda irá aumentar, fazendo com que ele se associe ao *Access Point* da direita de modo imperceptível.

Vale observar também que na Figura 24, os três APs foram configurados cada um com um canal diferente. Isto tem como objetivo eliminar interferências das células de cobertura vizinhas, já que existe uma sobreposição de sinal entre elas.

7 EQUIPAMENTOS

7.1 ACCESS POINTS

Atualmente, existem diversos fabricantes de equipamentos de rede no mercado. Quando se trata de wireless também não são poucos. Existem diversos modelos, para diferentes utilidades e ambientes.

Access Points podem se diferenciar pela frequência de operação, pelos recursos de gerência de RF, pela potência, quantidade de antenas, e se estas são internas ou externas.

Em termos de frequência, os mais comuns hoje em dia são os que operam somente em 2,4 GHz ou os que são *dual-band*, ou seja, operam tanto na banda de 2,4 GHz quanto na de 5,0 GHz simultaneamente.

Alguns APs (*Access Points*) possuem recursos que auxiliam na otimização de um ambiente RF. Um destes recursos é o direcionamento de clientes 802.11n para a banda de 5,0 GHz e os clientes 802.11b/g para a banda de 2,4 GHz, evitando a perda de performance para cliente 802.11n ao formar uma rede mista. Outro recurso bastante interessante é a realização de varreduras frequentes nos canais de RF para avaliar uma possível troca de canal para um menos congestionado para diminuir problemas com interferências.

Em termos de antenas, os APs mais atuais trabalham com o padrão 802.11n, e com isso, utilizam a tecnologia MIMO. Para tirar proveito desta tecnologia, alguns APS oferecem duas antenas para transmissão e duas para recepção. Esta configuração é geralmente demonstrada pela seguinte forma: 2x2. Além disso, uma outra característica do AP é a quantidade de *spatial streams* possíveis, ou seja, a quantidade de sinais diferentes que podem ser transmitidos pelas antenas. Se um AP possui duas antenas de recepção e duas de transmissão com dois *spatial streams*, pode-se representar essa configuração através da seguinte forma: 2x2: 2, onde o último 2 representa o número de *spatial streams*. As configurações mais comuns de APs são: 2x2:2, 2x3:2, 3x2:2, 3x3:2 e recentemente 4x4:3.

Existem ainda *Access Points* para áreas *indoor* e para *outdoor*. Estes se diferem pelas dimensões físicas, formas de conexão, potência, resistências a fatores ambientais, formas de instalação, dentre outros.

Todas essas características devem ser levadas em consideração na hora de escolher um AP para uma determinada aplicação.

A Figura 25 mostra alguns *Access Points* utilizados atualmente:

Figura 25 - Modelos de Access Points



Fonte: (Cisco, Aruba, 2013)

7.2 CONTROLADORAS

Dependendo do ambiente no qual uma determinada solução for implementada, a quantidade de APs pode variar desde um até milhares. No caso de poucos APs, a configuração de parâmetros de rádio, autenticação, SSID, modos de operação, endereço IP, características de *roaming*, canais, etc, pode ser realizado um a um em cada AP, entretanto, no caso de um determinado projeto envolver muitos APs, esta configuração manual pode se tornar impraticável. Para estes casos, existe um hardware chamado *Wireless LAN Controller* (WLC).

Uma controladora wireless tem como objetivo facilitar a implementação e a inserção dos APs na rede, além de gerenciar todos esses equipamentos quando estiverem em funcionamento. Uma WLC é um dispositivo central onde são realizadas todas as configurações e então estas são passadas para todos os *Access Points*. Desse modo, as funções da rede *wireless* são divididas entre um AP e uma controladora. Este modo de operação é chamado de *split MAC*. A Tabela 9 a seguir mostra algumas das principais atribuições de cada um:

Tabela 9 - Atribuições do AP e WLC

Atribuições do AP e WLC	
<i>Access Point</i>	<i>Controladora</i>
Gerenciamento de envio de Beacons.	Processos de autenticação e associação.
Criptografia.	Qualidade de serviço e gerenciamento de segurança.
Envio de <i>frames</i> para as estações.	Processos de <i>roaming</i> .
Monitoramento do meio para detecção de interferências e dispositivos que não pertencem a rede.	Gerenciamento de parâmetros de RF.
	Interfaceamento entre os APs e o sistema de distribuição.

Beacons são mensagens enviadas pelos APs contendo informações de SSID, informações do fabricante, taxas de transmissão suportadas, entre outras. São esses *beacons* que os dispositivos wireless detectam ao procurar uma rede para se conectarem.

A última função da controladora listada na Tabela 9 é o interfaceamento entre os APs e o sistema de distribuição, isso quer dizer que todo o tráfego gerado pelos clientes ou que tem como destino esses clientes, passa pela WLC antes de serem direcionados aos outros dispositivos, tanto da rede *wireless*, quanto da rede cabeada, ou para a internet.

Uma controladora possui diversos mecanismos de gerenciamento de RF que funcionam automaticamente, dependendo das informações enviadas pelo AP. Estas informações são processadas pela WLC para que os parâmetros de RF sejam ajustados da melhor maneira possível para o ambiente. Dentre as funcionalidades mais fundamentais de gerenciamento de RF estão:

- Alteração automática do canal de qualquer *Access Point* associada a controladora. Ao fazer uma varredura no ambiente, o AP envia informações para a WLC contendo detalhes sobre a utilização dos diversos canais da banda operante. A WLC então processa estas informações e verifica se uma mudança de canal daquele AP pode diminuir problemas de interferências.

- No caso de falha de um *Access Point*, APs adjacentes irão detectar este problema e irão reportar para a WLC. Através de algoritmos complexos a controladora mapeia o local e sabe exatamente que parte do ambiente ficou um buraco de cobertura devido a falha do AP. Para resolver esse problema, a WLC aumenta a potência dos APs adjacentes para suprir esta falta de cobertura.
- Do mesmo modo que a WLC pode aumentar a potência para cobrir falhas de cobertura, ela também pode diminuir a potência de APs para reduzir a sobreposição de sinais de APs vizinhos, já que o recomendado é apenas de 10% a 15%.

Existem vários modelos de controladoras atualmente. Geralmente, o que muda entre elas é a capacidade de APs que ela pode gerenciar, desde cinco até a casa dos milhares.

Em muitas empresas grandes, com várias filiais espalhadas em uma cidade ou país, pode haver a necessidade de serem utilizadas mais de um controladora. Da mesma maneira que uma WLC pode facilitar a implementação de vários APs, existem softwares que podem ajudar na implementação de várias controladoras, bem como gerenciar todos os equipamentos da rede, como switches, controladoras e APs.

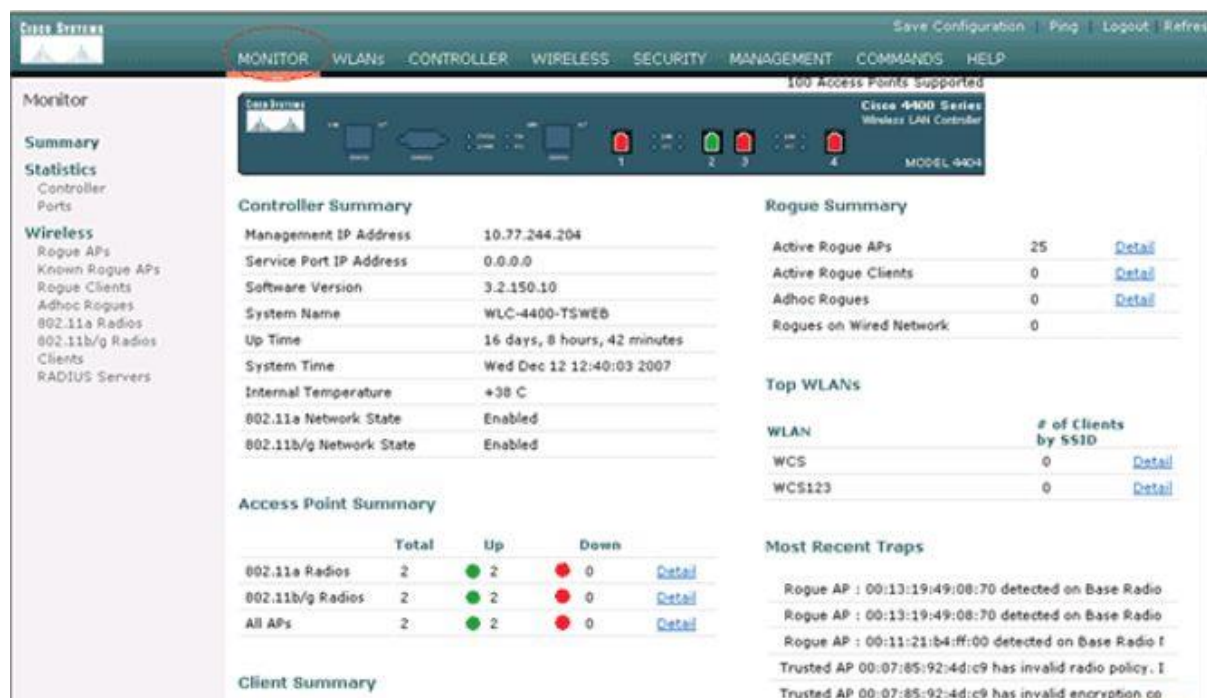
A Figura 26 mostra algumas controladoras disponíveis no mercado atualmente e a Figura 27 mostra uma das telas de gerenciamento dos APs:

Figura 26 - Modelos de controladoras wireless



Fonte: (Cisco, Aruba, 2013)

Figura 27 - Tela de gerenciamento de uma WLC



Fonte: (Cisco, 2013)

8.2 PREDIÇÃO

Este processo consiste em inserir as plantas do local no software e desenhar cada elemento físico sobre esta planta. Dentre estes elementos estão: paredes (concreto, tijolo, gesso), portas (finas, grossas, de vidro), janelas, áreas de baias, áreas de vão de elevador, áreas de depósitos com baixa, média ou alta densidade, etc. Estes elementos ajudam o software a calcular da maneira mais real possível todos os tipos de atenuações que os sinais dos APs podem vir a sofrer. A base de dados do software já sabe quais os valores das atenuações de cada elemento listado acima. Por exemplo, uma parede de concreto atenua muito mais o sinal do que uma parede de gesso. Além disso, é possível configurar manualmente o valor da atenuação em dB de cada elemento. A Figura 30 mostra os valores de atenuação configurados como padrão pelo software:

Figura 30 - Valores de atenuação padrão do Air Magnet



Window Office	3 dB
Brick Wall	8 dB
Cinder wall	4 dB
Concrete Wall	12 dB
Dry Wall	4 dB
Glass Wall with Metal Frame	6 dB
Heavy Door	15 dB
Light Door	4 dB
Metal Door	11 dB
Plasterboard Wall	3 dB
Thick Window	4 dB
Thin Window	2 dB
Window Office	3 dB

Fonte: (AirMagnet, 2013)

A Figura 31 e a Figura 32 mostram o resultado do processo de predição dos andares 6 e 7 respectivamente.

Figura 32 - Predição do 7º andar



Fonte: (Autor, 2013)

Dependendo do software, já existe uma base de dados de modelos de *Access Points* de diversos fabricantes. O que difere um do outro e o que realmente importa para o software na hora da simulação é o tipo de antena, potência, altura de instalação e canal de operação. Após inserir todos os obstáculos que possam causar algum tipo de atenuação no sinal, deve-se escolher qual tipo de AP que será utilizado no projeto. Para este caso, é utilizado o Cisco AIR-CAP3502I-N-K9, ilustrado na Figura 33:

Figura 33 - Cisco Access Point 3502



Fonte (Cisco, 2013)

Este AP é utilizado para aplicações *indoor* e possui a configuração MIMO 2x3: 3. As potências de transmissão que podem ser escolhidas para este equipamento estão listadas na Tabela 10:

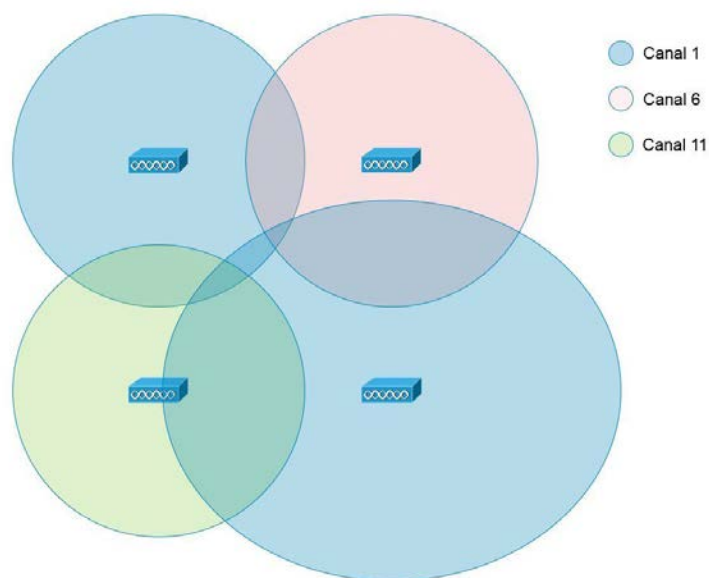
Tabela 10 - Potências disponíveis para o AP Cisco 3502

Potências Disponíveis			
2,4 GHz		5,0 GHz	
23 dBm	200 mW	20 dBm	100 mW
20 dBm	100 mW	17 dBm	50 mW
17 dBm	50 mW	14 dBm	25 mW
14 dBm	25 mW	11 dBm	12,5 mW
11 dBm	12,5 mW	8 dBm	6,25 mW
8 dBm	6,25 mW	5 dBm	3,13 mW
5 dBm	3,13 mW	2 dBm	1,56 mW
2 dBm	1,56 mW	-1 dBm	0,78 mW
-1 dBm	0,78 mW		

Quanto maior a potência, maior é o alcance do sinal do AP, entretanto, colocar muitos APs na potência máxima para atender o quesito cobertura não é sempre a melhor solução. Vale lembrar que para a frequência de 2,4 GHz existem somente três canais que não se sobrepõem, isto é, canais cujo intervalo de frequência não se cruzam, e por isso não causam interferência. Desse modo, colocar quatro *Access Points* em um ambiente pequeno e com pouca atenuação, fará com que, possivelmente células se sobreponham. Como somente três canais podem ser utilizados, um destes

quatro APs utilizará um canal já utilizado por outro AP, e neste ponto de sobreposição de célula haverá uma grande interferência. A Figura 34 mostra esta situação hipotética:

Figura 34 - Interferência de canais



Fonte: (Autor, 2013)

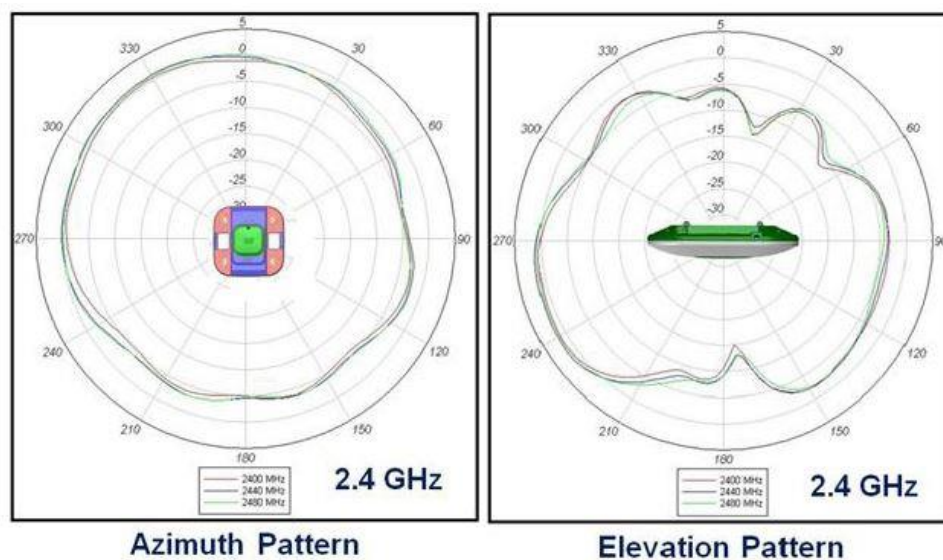
Nesta situação, o melhor a se fazer é reduzir a potência do AP do canto inferior direito para evitar interferência com o AP de mesmo canal do canto superior esquerdo. Em um ambiente real, o sinal de um AP não se propaga de maneira uniforme, como no exemplo acima. Isso tudo vai depender dos obstáculos encontrados pela frente, e sendo assim, pode haver mais ou menos interferência entre canais. Por isso, deve-se desenhar a disposição de APs de modo que este problema não ocorra, entretanto, essa interferência de canais nem sempre pode ser totalmente evitada já que APs de salas ou até andares de outros estabelecimentos podem estar trabalhando no mesmo canal que os *Access Points* do projeto e não é possível alterar suas configurações de canais, já que pertencem a outras empresas e outros administradores de rede.

Para o processo de predição, a melhor prática para escolha da potência é selecionar uma potência intermediária, pois a WLC terá margem para aumentar ou diminuir caso haja necessidade. Em uma situação hipotética em que um determinado AP venha a falhar em um determinado ambiente, os APs vizinhos irão reportar a controladora, e esta, irá aumentar suas potências para tentar cobrir a sombra de cobertura deixada pelo AP que parou de funcionar. Se todos estes APs já

estiverem configurados em potência máximo, este processo se tornará impraticável. Na maioria das vezes, quando os APs são gerenciados por uma controladora, ela já configura as potências como intermediárias, exceto quando existe uma necessidade específica. Já que no maior caso das vezes os APs irão trabalhar em potência intermediária, para simular da maneira mais real possível, deve-se configurar o AP nestas potências no processo de predição.

A altura de instalação é aproximadamente três metros. Este é um fator bastante relevante. O AP escolhido utiliza antenas internas omnidirecionais, ou seja, propagam seu sinal para todos os lados, se visto de cima. Se visto de lado, o sinal se propaga para baixo até uma distância de aproximadamente cinco metros. Este tipo de equipamento deve ser instalado no teto do ambiente para propagar seu sinal para baixo e para os lados. Como a altura ideal é de aproximadamente cinco metros, não é recomendado utilizar este equipamento para ambientes com mais de 6 metros de altura, visto que uma mesa tem aproximadamente um metro de altura. A Figura 35 mostra o padrão de radiação do sinal, onde a imagem da esquerda é o AP visto de cima, chamado de *Azimuth* e a da direita é o AP visto de lado, chamado de *Elevation*:

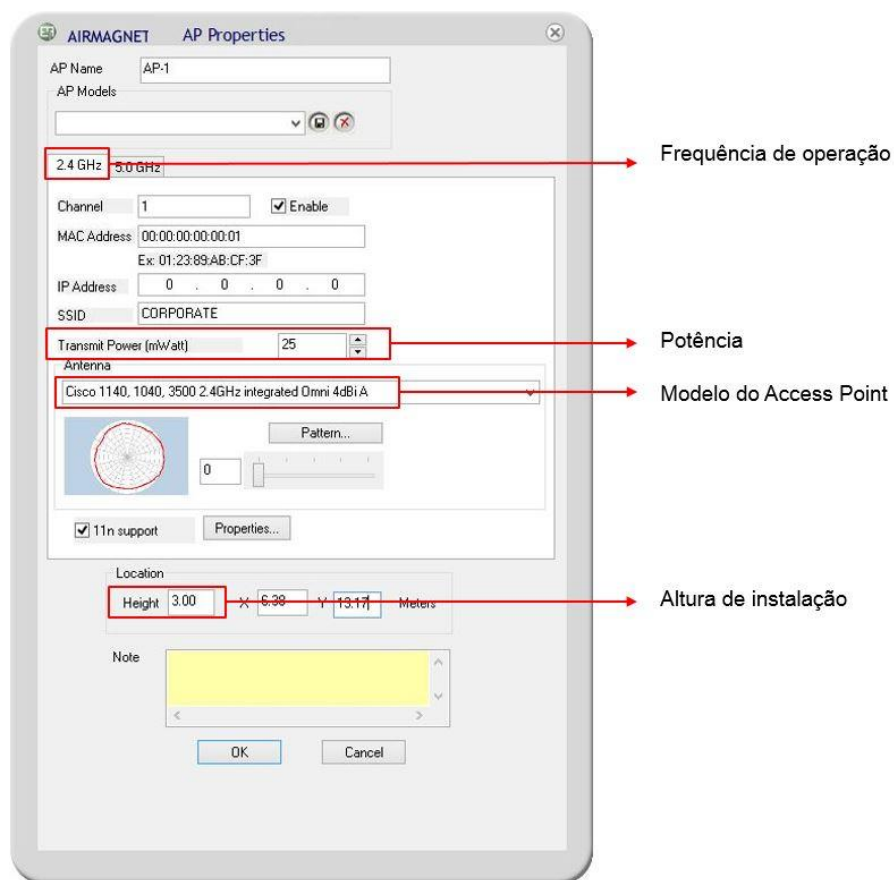
Figura 35 - Padrão de radiação de sinal



Fonte (Cisco, 2013)

Após escolher todos estes parâmetros, o AP está pronto para ser inserido na planta, já com os obstáculos. A Figura 36 mostra a janela de configuração do AP no Air Magnet para a banda de 2,4 GHz. A mesma configuração deve ser realizada para a aba de 5,0 GHz.

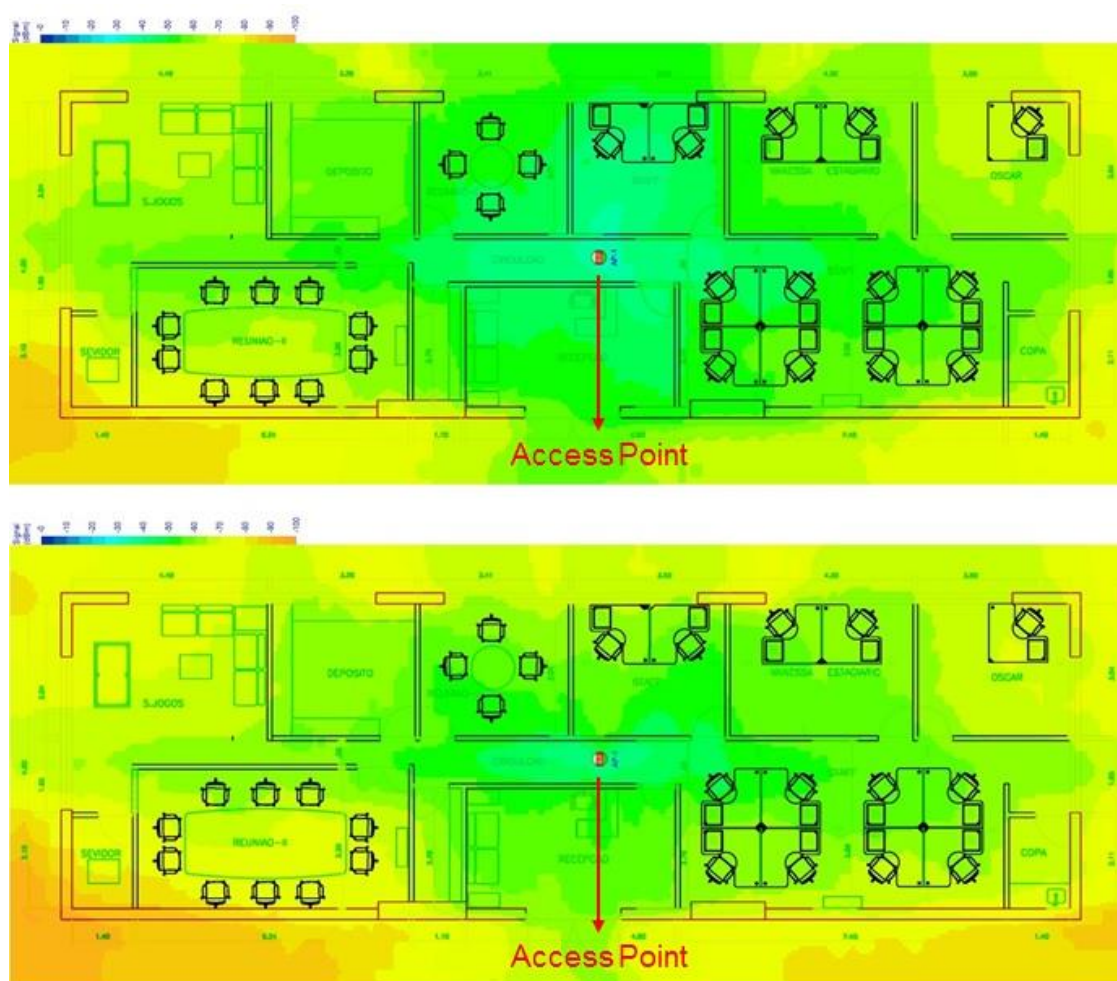
Figura 36 - Configuração do AP no Air Magnet



Fonte (AirMagnet, 2013)

O *Access Point* pode ser colocado em qualquer lugar da planta somente para que se possa ter uma noção de até onde o sinal pode chegar. O seu sinal em 2,4 GHz (superior) e 5,0 GHz (inferior) é mostrado através da Figura 37:

Figura 37 - Propagação do sinal em 2,4 GHz e 5,0 GHz



Fonte: (Autor, 2013)

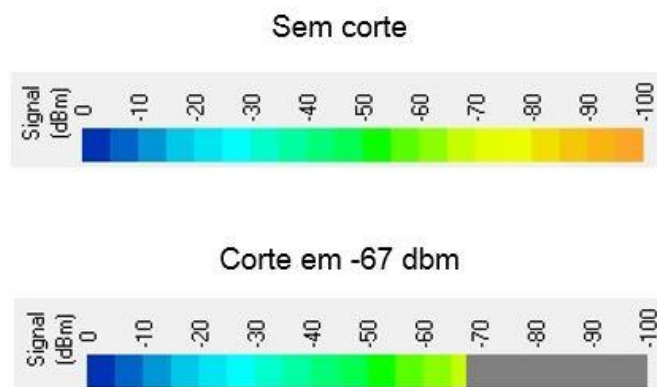
De acordo com a escala de sinal, localizada acima de cada imagem, o local que possui a cor mais próxima de azul é onde o sinal apresenta uma maior intensidade, e o mais próximo de laranja, uma pior intensidade.

Pode-se observar que o sinal em 2,4 GHz se propaga a uma maior distância do que o sinal em 5,0 GHz. Isso segue a lei de atenuação que comprova que quanto maior a frequência, maior é a atenuação em relação a distância. Além disso, com obstáculos, o sinal em 5,0 GHz atenua muito mais.

Antes de movê-lo para um local mais adequado, um ajuste bastante importante deve ser feito no software. Dentre os objetivos do projeto, está o planejamento da rede sem fio para a

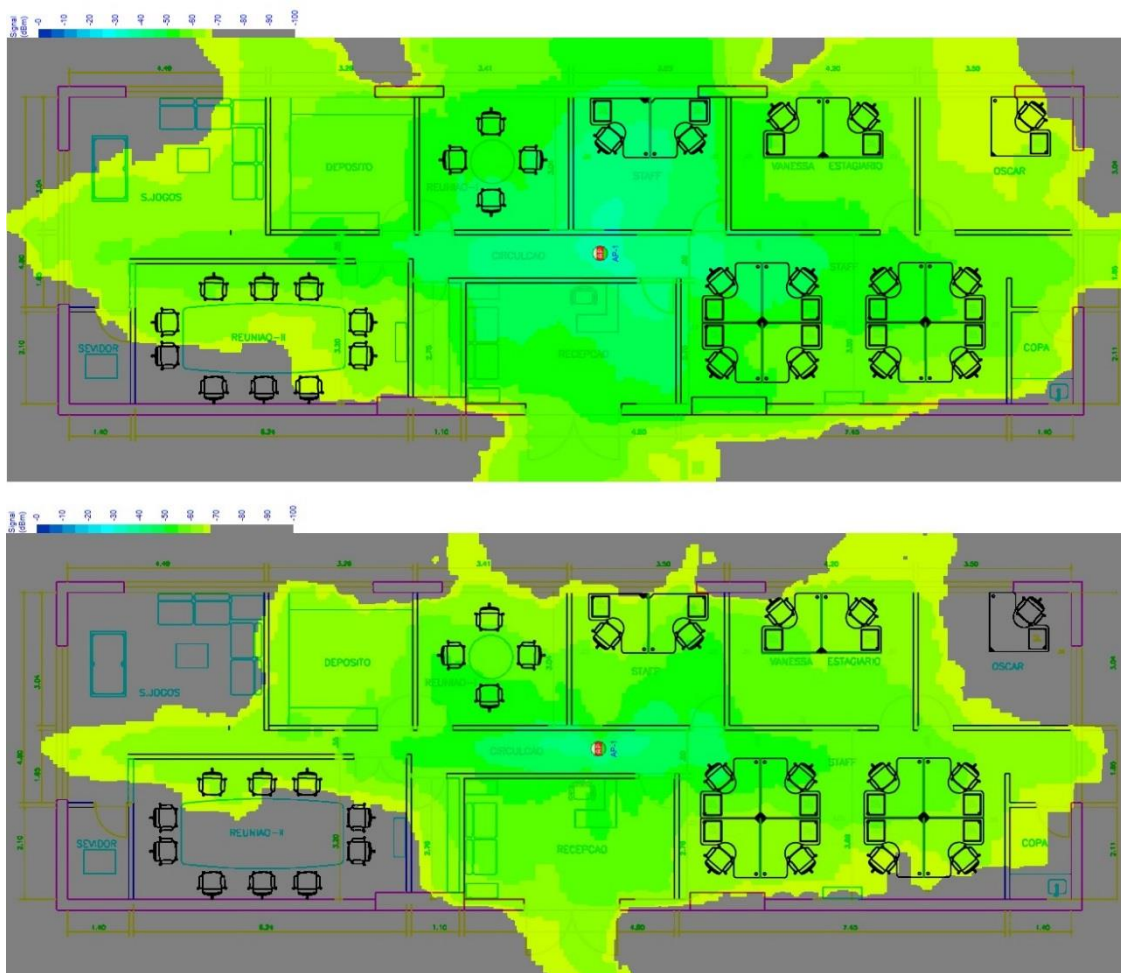
utilização de telefones IP sem fio. Para aplicações de voz, o planejamento deve ser um pouco mais cuidadoso, visto que este tipo de aplicação demanda mais da rede. Sendo assim, deve-se configurar um limite de potência de sinal recebido para assegurar a qualidade necessária para aplicações de voz. O recomendando pela maioria dos fabricantes é receber um sinal com -67 dBm para aplicações de voz e -75 dBm para aplicações somente de dados. Esta escala varia de 0 a -100 dBm. No software, esta potência é representada por um mapa de calor, que pode variar de azul (0 dBm – muito forte), até laranja escuro (-100 dBm - muito fraco). Para visualizar de maneira mais precisa até onde o sinal chega a uma potência de -67 dBm, é recomendado ajustar a barra de escala, localizada na lateral da janela, para corte em -67 dBm. Fazendo isto, qualquer sinal pior do que -67 dBm irá aparecer na planta em cinza, e qualquer sinal melhor irá aparecer colorido na sua respectiva cor. A Figura 38 mostra a barra de escala ajustada para corte em -67 dBm e a Figura 39 mostra o sinal, em 2,4 GHz (superior) e 5,0 GHz (inferior) após configurar o corte em -67 dBm.

Figura 38 - Barra de sinal em dBm



Fonte (AirMagnet, 2013)

Figura 39 - Sinal do AP com corte em -67 dBm em 2,4 GHz e 5,0 GHz



Fonte: (Autor, 2013)

Realizados estes ajustes, o AP pode agora ser movido para o local mais adequado. A partir daí, mais APs podem ser adicionados para cobrir totalmente o local, lembrando que deve haver uma sobreposição de células de 10% a 15%, para que possa haver *roaming* transparente para o usuário.

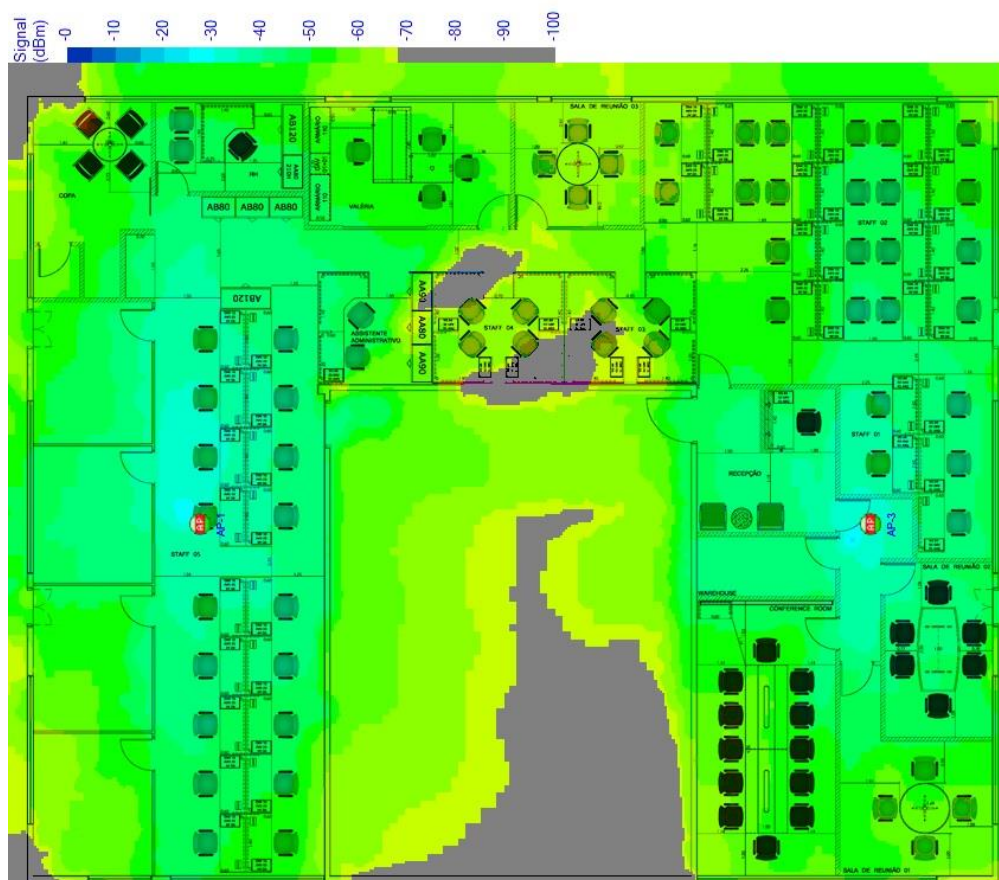
Para este projeto, foram estipulados aproximadamente 30 e 60 conexões para o 6º e 7º andares respectivamente. A recomendação da fabricante deste AP é aproximadamente 30 conexões simultâneas para cada equipamento. Visto que além dos 30 e 60, irão existir alguns telefones IP que também irão utilizar a rede sem fio para realizar chamadas. Sendo assim, pela quantidade de usuários, pode-se dimensionar 2 e 3 APs para o 6º e 7º andares respectivamente. Além disso, essa

sobra da uma margem para escalabilidade e crescimento da base de usuários, e em consequência disso, caso haja a necessidade de mais conexões, não será necessário adicionar mais APs e realizar um outro processo inteiro de dimensionamento.

O primeiro objetivo é cobrir o ambiente com o número de APs calculados com base no número de conexões requisitadas pelo cliente. Se forem muitos APs para um ambiente pequeno, provavelmente é um ambiente com alta densidade, e para isto, deve-se utilizar APs com potência reduzida para que a sobreposição de células não ultrapasse 15%. No caso de o número de APs calculados não forem o suficiente para cobrir toda a área estipulada, deve ser utilizado o número de APs necessários para cobrir 100% o local, de acordo com a predição realizada no Air Magnet.

De acordo com a Figura 39 pode-se perceber que apenas um AP não é o suficiente para realizar a cobertura do andar inteiro, tanto em 2,4 GHz quanto em 5,0 GHz, além disso, de acordo com as necessidades de conexão do cliente, são necessários dois *Access Points*. Outro ponto bastante importante para se levar em consideração nestes casos é a disponibilidade da rede sem fio. Em caso de falha neste único AP, o andar inteiro irá permanecer sem conexão. Por motivos de redundância, é bastante recomendar não utilizar somente um *Access Point*, pois em caso de falha, a controladora pode aumentar a potência do outro AP para cobrir a área que ficou sem sinal. Como apenas um AP já cobre uma área bastante significativa do ambiente, adicionar mais um irá resultar em uma área de sobreposição bastante grande. Porém, este problema ficará a cargo da WLC que irá diminuir a potência destes AP conforme o necessário. A Figura 40 mostra o resultado da predição com 2 APs, para 2,4 GHz (superior) e 5,0 GHz (inferior), com corte em -67 dBm.

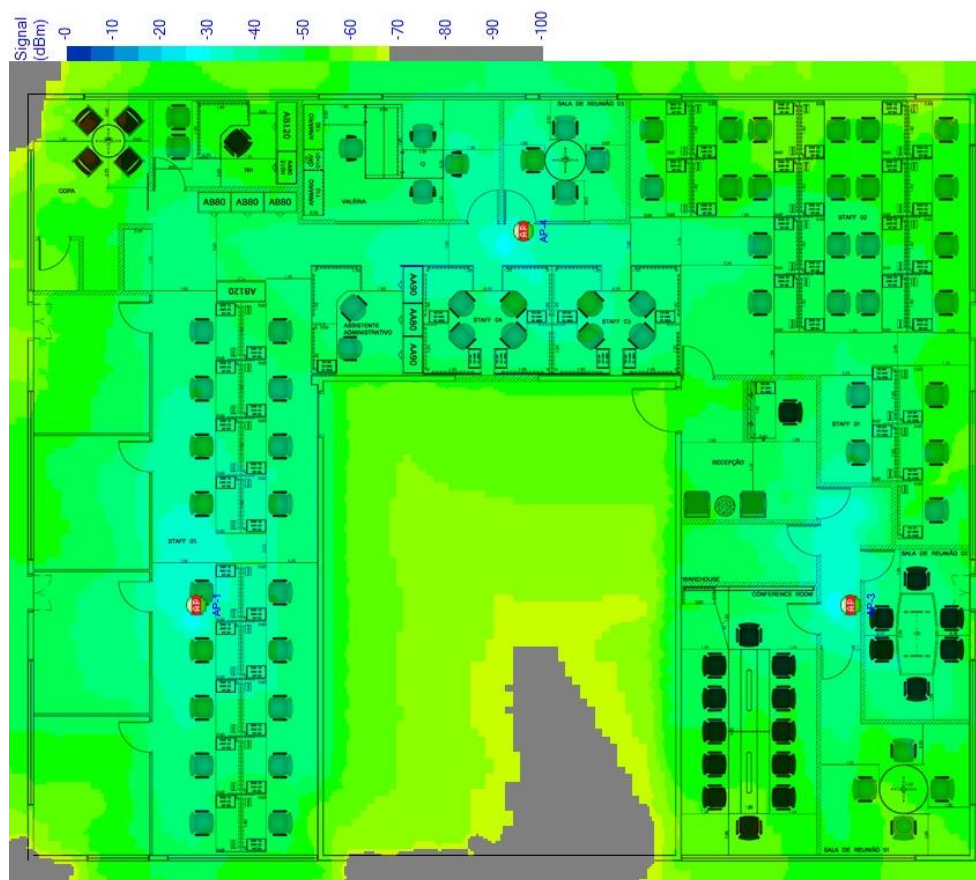
Figura 41 - Propagação do sinal do 7º andar em 5,0 GHz e corte em -67 dBm



Fonte: (Autor, 2013)

Pode-se perceber novamente que neste caso, somente dois APs também não são suficientes para cobrir todos os ambientes, além disso, para o número de conexões simultâneas, essa quantidade não atende, e por isso são utilizados 3 APs, como mostra a Figura 42. Mesmo se dois APs fossem o suficiente para cobrir toda a área, a necessidade da aplicação do projeto demanda três, e por isso, devem ser utilizados três APs.

Figura 42 - Propagação do sinal do 7º andar em 5,0 GHz com três APs

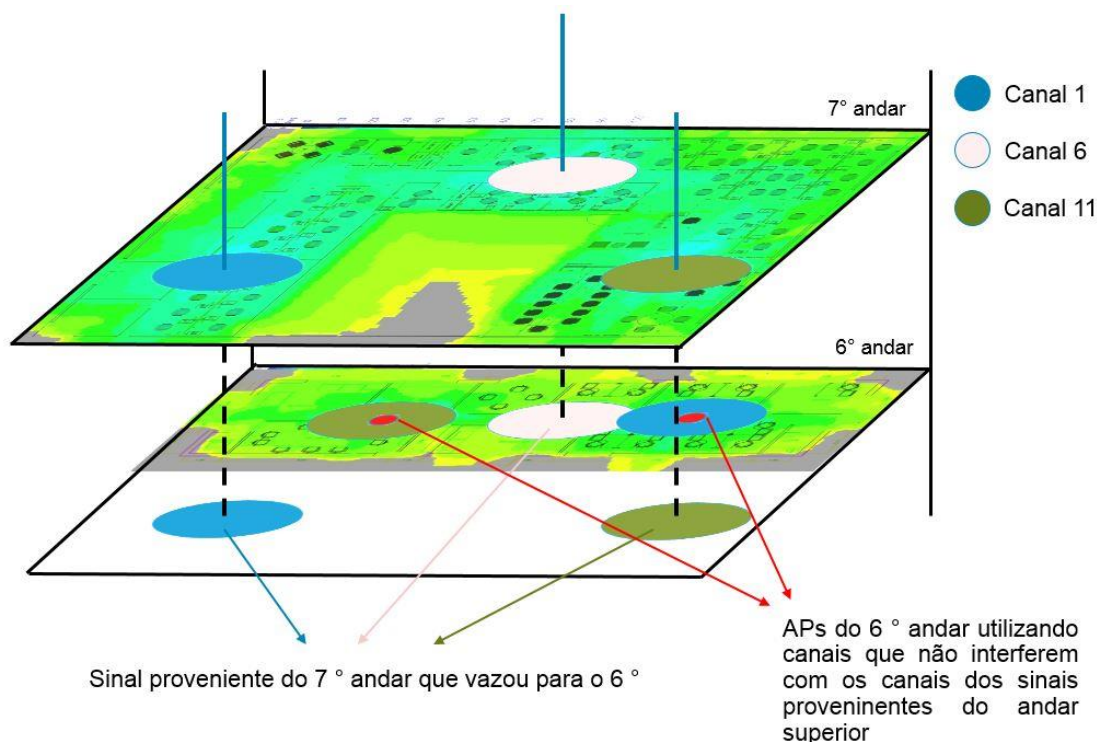


Fonte: (Autor, 2013)

Um outro ponto de atenção que deve ser observado durante a predição é a localização dos APs quando o projeto envolve mais de um andar próximo ao outro. Neste caso, o projeto envolve o 6º e 7º andar, que é um em cima do outro. Nestas situações, os APs devem ser dispostos de tal maneira que evite interferências com APs de andares próximos, ou seja, deve ser levado em consideração os dois andares em conjunto e os canais de operação de cada um dos cinco APs envolvidos. Embora a recomendação da fabricante é utilizar um dispositivo *wireless* a até cinco metros abaixo do AP, o sinal deste pode ultrapassar o limite do chão e vazar para andares inferiores. Neste projeto, como são utilizados três APs no 7º andar, estes podem ser configurados com os canais 1, 6 e 11 e assim, os APs do 6º andar podem ser configurados no canal 1 e 11, intercalando com os canais dos sinais provenientes de cima.

Assim, caso os sinais dos APs do 7º andar vazem para o 6º andar, os sinais utilizando o mesmo canal ficarão em lados opostos, evitando interferências, como mostra a Figura 43. Entretanto, para ambientes com muitos APs, este estudo se torna muito mais complexo.

Figura 43 - Propagação do sinal entre andares



Fonte: (Autor, 2013)

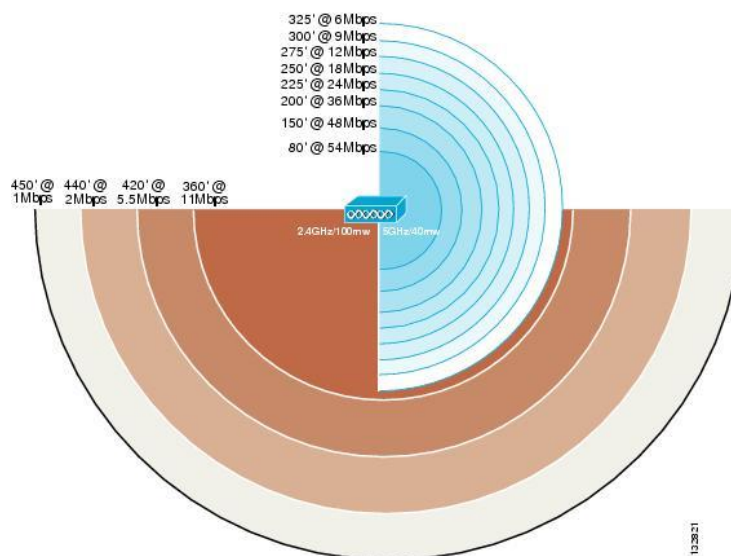
Embora a controladora fique responsável por selecionar o canal de operação dos APs, durante o planejamento deve ser levado em consideração estes problemas para garantir o pleno funcionamento da rede sem este tipo de interferência.

Essa preocupação com alocação de canais para evitar interferências se torna menos recorrente para a banda de 5,0 GHz, já que esta possui 23 canais que não se sobrepõem. Assim, existe muito mais liberdade para alocar os canais nos diversos APs do ambiente. Entretanto, atualmente, muitos equipamentos de empresas ainda operam somente em 2,4 GHz, dificultando o planejamento da rede sem fio. Entretanto, este cenário está começando a mudar, visto que a maioria de smartphones e tablets disponíveis atualmente possuem placas de rede *dual-band*, ou

seja, operam nas duas frequências. Além disso, o padrão 802.11ac que se tornará predominante daqui há alguns anos utiliza somente o 5,0 GHz.

Outra característica de rede que também deve ser levado em consideração é a banda disponível para cada usuário, dependendo do *data rate* disponível. Vale lembrar que o *data rate* diminui com o aumento da distância, devido a complexidade do tipo de modulação. Ao se distanciar do AP, o tipo de modulação pode mudar para um tipo menos complexo para que não haja perdas de informação durante a transmissão, resultando em *data rates* menores. Isso é realizado pelo DRS (*Dynamic Rate Shifting*). A Figura 44 mostra o *data rate* disponível em relação a distância do AP:

Figura 44 - Data rate em relação a distância



Fonte (Cisco, 2013)

Sendo assim, supondo a utilização do padrão 802.11n com 108 Mbps, devido a procedimentos de confiabilidade no transporte do padrão 802.11, esta taxa é reduzida pela metade, sendo o real 54 Mbps. No caso de 30 usuários conectados em um AP, a banda será dividida aproximadamente igual e cada um terá disponível um *data rate* de 1,8 Mbps. Entretanto, no 6º, haverá dois APs e os usuários irão se dividir entre eles, então, provavelmente o *data rate* disponível será maior do que este valor. Seguindo este raciocínio, quando uma determinada aplicação requisitar um alto *data rate*, deve-se também dimensionar a quantidade de AP pela banda

disponível para cada usuário, sempre levando em consideração distância deste usuário ao AP, já que em maiores distâncias, o *data rate* disponível é menor.

8.3 SITE SURVEY

Após a realização da predição, a disposição e quantidade dos APs devem ser testadas no ambiente real do projeto, já que podem haver outros fatores que não são possíveis simular por predição e que podem influenciar a propagação do sinal. Para isto, além do software, será necessário também levar ao local um AP de modelo similar ao utilizado na predição e configurado com os mesmo parâmetros de potência e um tripé para levantar o AP e simular seu funcionamento na altura em que será instalado.

O site survey consiste em subir o tripé com o AP em cada local indicado na predição, conforme Figura 45 e caminhar por todo o ambiente medindo o sinal daquele AP através do software. Feito isso, o resultado obtido de cada AP é combinado com a medição individual dos outros APs em apenas uma planta, para ser avaliado. Caso o site survey indique uma falha de cobertura não prevista na predição, duas ações podem ser tomadas:

- Alterar a posição de algum AP para cobrir aquele local, sem que abra uma nova falha;
- Adicionar um outro AP para suprir a falha.

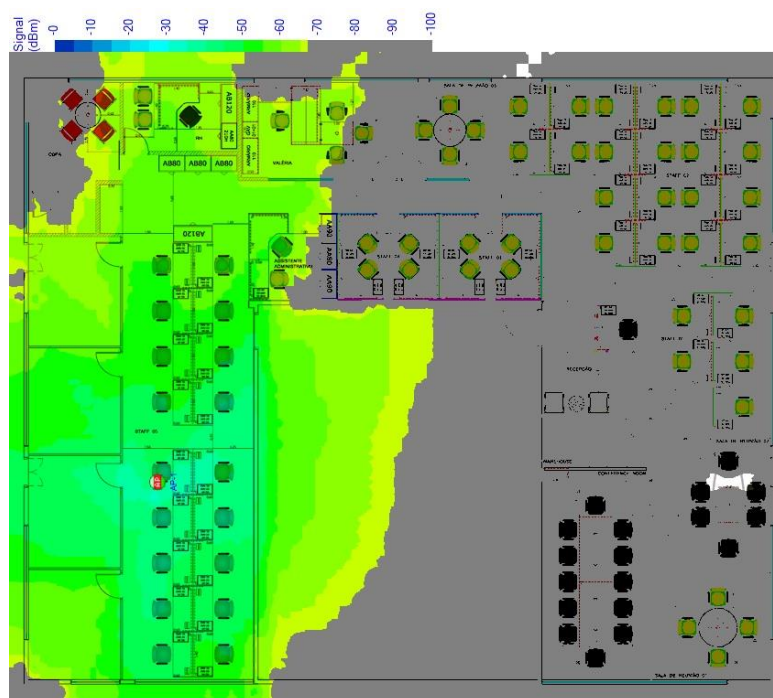
A Figura 46 mostra a medição do site survey do AP 1 do 7º andar, para 5,0 GHz com corte em -67 dBm para aplicações de voz:

Figura 45 - Simulação da altura de instalação com um tripé



Fonte: (Autor, 2013)

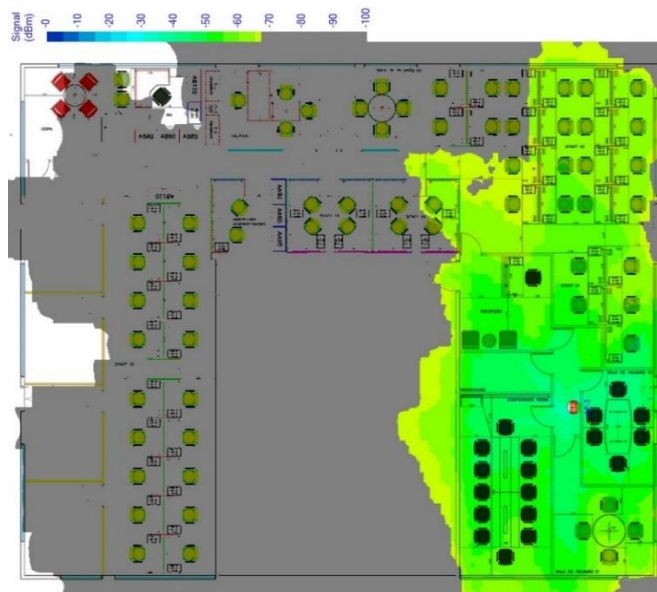
Figura 46 - Propagação do sinal do AP 1 do 7º andar em 5,0 GHz e corte em -67 dBm



Fonte: (Autor, 2013)

A Figura 47 mostra a medição do *survey* do AP 2 do 7º andar, para 5,0 GHz e -67 dBm:

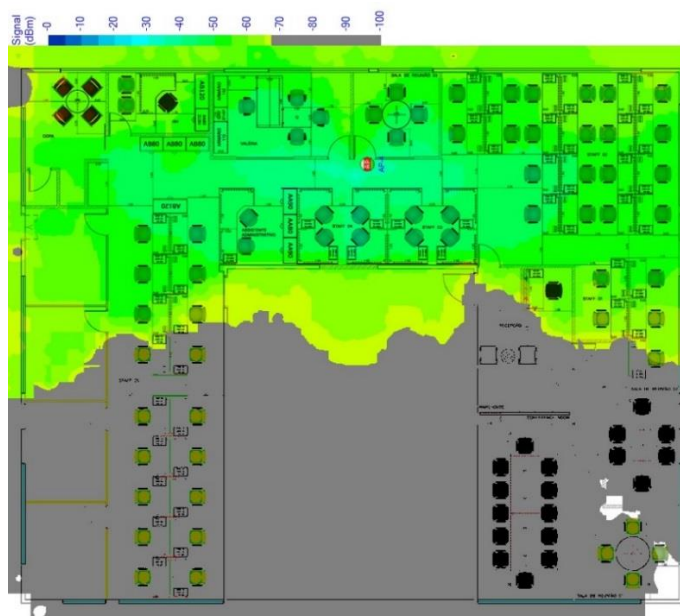
Figura 47 - Propagação do sinal do AP 2 do 7º andar em 5,0 GHz e corte em -67 dBm



Fonte: (Autor, 2013)

A Figura 48 mostra o *survey* do AP 3 do 7º andar, para 5,0 GHz com corte em -67 dBm:

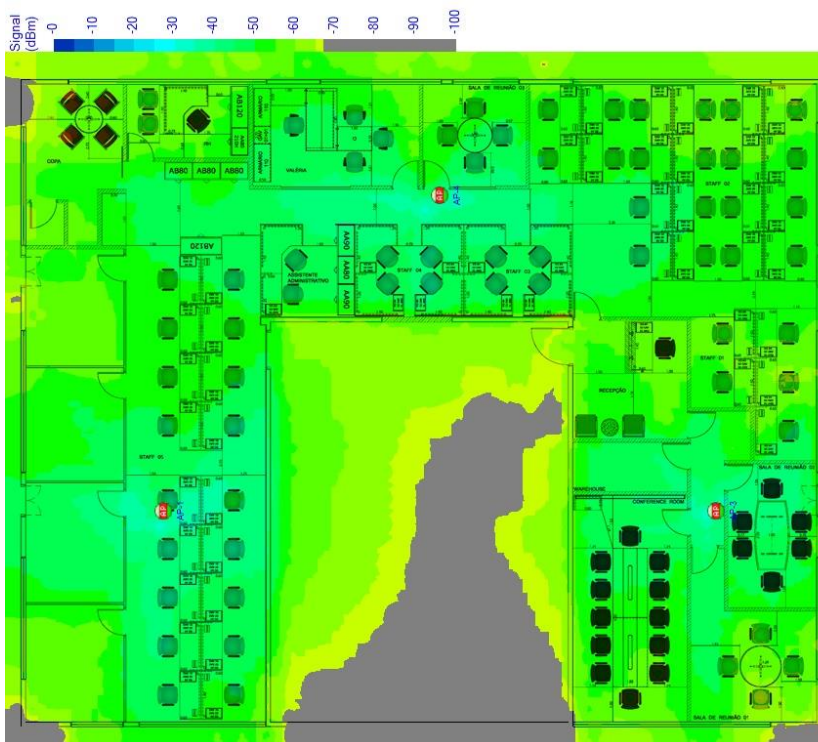
Figura 48 - Propagação do sinal do AP 3 do 7º andar em 5,0 GHz e corte em -67 dBm



Fonte: (Autor, 2013)

Após realizadas as medições dos 3 APs individualmente, deve-se combinar estes três dados para um único arquivo que irá mostrar a cobertura do andar inteiro resultante dos sinais de cada AP. O próprio software já possui um recurso que possibilita essa junção e o resultado é mostrado na Figura 49, em 5,0 GHz com corte em -67 dBm.

Figura 49 - Combinação de sinais no 7º andar em 5,0 GHz e corte em -67 dBm



Fonte: (Autor, 2013)

Pode-se observar que os resultados obtidos através do site survey são bastante satisfatórios e atendem aos requisitos de cobertura do projeto. Vale lembrar que o survey deve ser realizado tanto em 2,4 GHz quanto em 5,0 GHz já que é um dos requisitos do projeto. Entretanto, para que não fique muitas imagens, foram inseridas somente a da banda de 5,0 GHz, já que na maioria dos casos, apresenta a pior situação.

Em alguns casos, o cliente necessita de apenas cobertura em 2,4 GHz por possuir somente equipamentos mais antigos que operam apenas nesta frequência. Na teoria, o sinal de 2,4 GHz se propaga a uma distância maior, e por isso, dependendo do projeto, pode-se ser utilizados menos APs do que seriam utilizados caso fosse necessário cobertura também em 5,0 GHz.

8.4 SITE SURVEY PÓS INSTALAÇÃO

Esta etapa é realizada quando a solução já foi entregue e instalada no cliente. Este site survey tem como papel a validação do planejamento e detecção de problemas.

Neste processo, não é necessário levar um AP similar ou até mesmo o tripé, já que o equipamento real já está instalado no teto do local. Assim, o software pode captar o sinal transmitido pelo próprio AP do cliente e mapear na planta configurada no Air Magnet. Assim, é possível avaliar de fato e da maneira mais real possível a qualidade da solução projetada.

Além disso, este site survey ainda pode detectar problemas que possam ser causados por dispositivos não pertencentes a rede, como outros *Access Points* de ambientes ou andares vizinhos.

8.5 TOPOLOGIA LÓGICA

Uma vez comprovado através do site survey que a quantidade de APs dimensionados para o projeto é o suficiente para prover cobertura wireless de acordo com os requisitos do cliente, inicia-se então o processo de instalação física dos equipamentos. A Figura 50 mostra um dos *Access Points* já instalados no teto do local.

Figura 50 - Access Point instalado no teto



Fonte (Cisco, 2013)

Para que a rede funcione de maneira correta, não basta somente instalar e ligar as antenas no teto. É necessário também conectar e configurar corretamente outros equipamentos de rede que compõem a solução.

Cada AP deve ser conectado diretamente a um switch, bem como os desktops que necessitam de conexão cabeada e os telefones IP POE. Quando um telefone ou AP é POE significa que a energização do equipamento é feita através do cabo de rede, dispensando o uso de um cabo de energia. Esse recurso torna diversas aplicações muito mais práticas pois eliminam a necessidade de um ponto de energia para ligar um determinado aparelho. Entretanto, para que um equipamento possa ser energizado através do cabo de rede, o switch ao qual é conectado também deve suportar este recurso.

Para configuração e gerência dos APs, é utilizado uma controladora *wireless*. Esta controladora também deve ser conectada a um switch da rede. Além disso, é necessário um roteador para saída para a internet e um equipamento chamado de *gateway* de voz, que tem como principal função encaminhar o tráfego dos telefones IP para a rede de telefonia. Estes dois equipamentos também são conectados ao switch.

Como há switches distintos em cada andar, estes deverão se comunicar entre si através de uma conexão cabeada entre eles.

A Tabela 11 mostra a quantidade de portas no switch necessárias para cada andar:

Tabela 11 - Quantidade de portas de switch necessárias

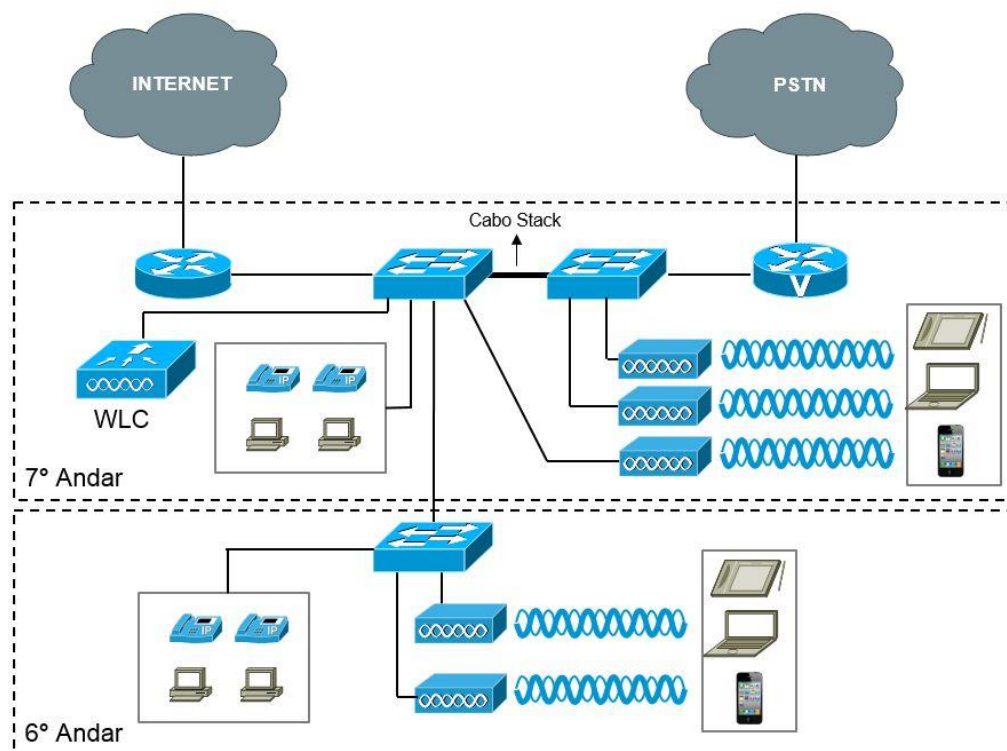
Quantidade de portas no switch necessárias			
6º Andar		7º Andar	
<i>Access Points</i>	2	<i>Access Points</i>	3
Telefones IP	5	Telefones IP	20
Desktops	10	Desktops	50
Switch 7º andar	1	Switch 6º andar	1
		Roteador	1
		<i>Gateway</i> de voz	1
		Controladora	1
TOTAL	18	TOTAL	77

Existem switches disponíveis no mercado de 8, 24 e 48 portas e alguns modelos que são chamados de modulares, nos quais são possíveis de adicionar módulos de portas adicionais.

Para projetos deste porte, é bastante comum utilizar um switch de 24 portas para o 6º e dois de 48 portas para o 7º andar. As portas excedentes ficam como uma margem de folga para questões de escalabilidade. Como são utilizados dois switches no 7º andar, estes também devem se comunicar entre si através de uma conexão cabeada. Entretanto, para casos como este, existe uma conexão específica através de um cabo chamado de *stack*. Este cabo tem como principal função juntar dois switches para que estes funcionem como apenas um equipamento, porém de 96 portas. A principal vantagem deste tipo de conexão é a facilidade de manutenção e gerência dos switches, além da possibilidade de combinar o poder de processamento dos dois equipamentos. Esta conexão através de cabo *stack* não consome uma porta convencional do switch, e portanto, não será contabilizado.

Com isso, pode-se montar a topologia mostrada na Figura 51.

Figura 51 - Topologia do projeto



9 APLICAÇÕES ATUAIS E APOSTAS PARA O FUTURO

9.1 3G/4G OFFLOAD

A constante evolução das tecnologias de comunicação móvel, tem permitido um aumento das taxas de transmissão de dados, algo que os padrões do Wi-Fi sempre buscaram. O sistema de comunicação 2G tinha como objetivo fornecer somente um meio de comunicação de voz eficiente para os usuários finais. Os sistemas de terceira geração (3G) de telefonia móvel vieram para mudar os hábitos e a maneira como os clientes utilizam seus celulares. Agora, com a chegada da tecnologia 4G que possibilita taxas de transmissão ainda mais elevadas, as aplicações se tornarão cada vez mais robustas e os usuários finais cada vez mais exigentes.

O 3G e o 4G permitem a criação de novas aplicações indisponíveis e impraticáveis na era 2G. A popularização de smartphones e tablets, que permitem diversas aplicações como mensagens, navegação na internet, compartilhamento massivo de arquivos, *streaming* de vídeo, envio de fotos e músicas, etc, está exigindo cada vez mais das operadoras de telefonia celular.

As aplicações de vídeo, que requerem uma taxa muito maior de transmissão do que qualquer outra aplicação móvel, irão se tornar cada vez mais frequentes e demandar muito mais infraestrutura das redes de celular. Este é um grande desafio a ser enfrentado pelas operadoras. Além disso, aumentar o tráfego não significa necessariamente aumentar o faturamento, o que pode gerar um grande empecilho para justificar novos investimentos.

O aumento do tráfego de dados não é somente uma preocupação das operadoras. Os clientes finais ficam sujeitos a limites de tráfego impostos pelas operadoras para que esta situação não fique tão grave. Com a crescente utilização de aplicações que demandam mais dados, essas quotas de dados se esgotam rapidamente fazendo com que a velocidade diminua de maneira drástica para o usuário, ou este fica sujeito a um pagamento extra para continuar a utilizar o serviço de dados. Ainda, mesmo dentro das quotas, os usuários finais podem enfrentar lentidão e até queda no serviço devido a alta carga de dados na rede móvel, gerando grande insatisfação.

Para resolver esses problemas que podem se tornar cada vez mais frequentes, tecnologias alternativas estão sendo implementadas recentemente para descongestionar as redes celulares. Uma

delas é similar a implementação de uma rede sem fio de alta capacidade, isto é ao invés de utilizar somente uma antena em potência alta para cobrir todo o ambiente, são utilizadas várias antenas com potência menor, e portanto menor raio de cobertura, para distribuir os usuários de forma mais homogênea em cada célula. Essa solução faria com que cada célula suportasse uma menor quantidade de usuários, porém iria melhorar a cobertura e a relação sinal ruído, bem como a qualidade do serviço oferecido. Existem duas tecnologias atualmente que utilizam esse conceito para descongestionar a rede.

9.1.1 Femtocélulas

Femtocélulas são dispositivos que operam da mesma maneira que macrocélulas das redes celulares, utilizando espectro licenciado, porém com menor alcance e capacidade. Por operarem na mesma frequência das macrocélulas, os aparelhos celulares não necessitam de nenhum tipo de modificação para que funcionem com esta tecnologia.

As femtocélulas são destinados a utilização *indoor* e se conectam a rede da operadora por banda larga já existente no local. Desse modo, o custo de infraestrutura é reduzido de forma drástica, já que não há necessidade de pagar por terrenos ou aluguéis para a construção de torres para instalação de antenas, bem como infraestrutura de rede para levar a conexão a esta torre. Além disso, o dispositivo seria pago pelo usuário e ainda utilizaria a conexão banda larga da sua própria residência ou estabelecimento.

Através desta tecnologia, um usuário, ao entrar em um determinado estabelecimento, irá se conectar a femtocélula ao invés da macrocélula, reduzindo o tráfego da macrocélula. Os principais alvos desta tecnologia são residência, shoppings, aeroportos, hospitais, escolas, estabelecimentos comerciais como lojas, bares, restaurantes, etc.

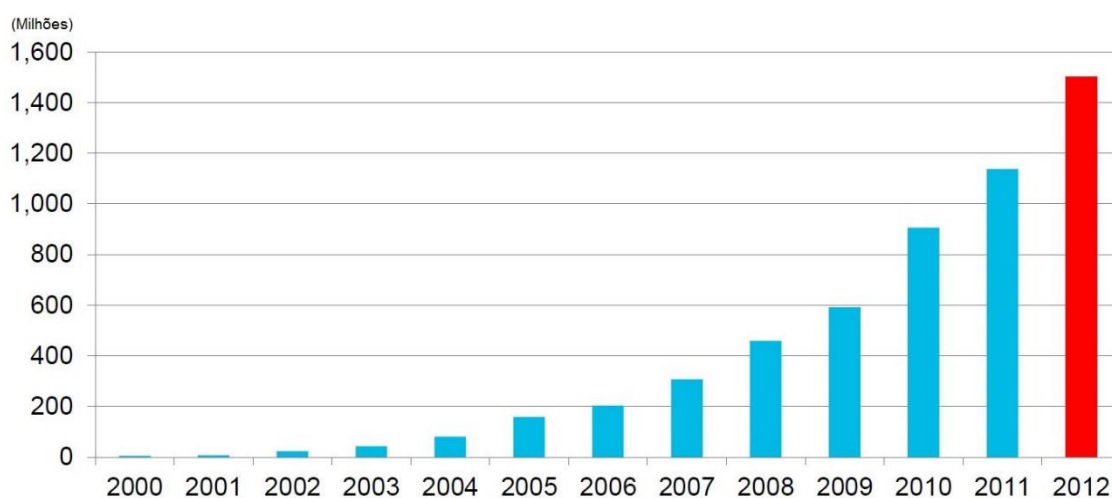
As femtocélulas estão sendo estudadas há alguns anos e sua utilização em massa está prevista para os próximos anos a partir de agora.

9.1.2 Wi-Fi

Uma outra solução para descongestionar o tráfego de dados das redes de celular é a utilização do Wi-Fi. Com os recentes avanços nas taxas de transmissão desta tecnologia, bem como a padronização dos equipamentos para que haja interoperabilidade dentre os diversos fabricantes, o Wi-Fi se tornou um forte candidato para auxiliar as operadoras nesse grande desafio que elas tem pela frente.

A quantidade de chipsets Wi-Fi vendidos anualmente vem crescendo de forma bastante significativa, como mostra a Figura 52. Este é um fator bastante importante na escolha desta tecnologia para o *offload* das redes móveis.

Figura 52 - Quantidade de chipsets Wi-Fi vendidos nos últimos anos



Fonte (Cisco, 2013)

A utilização da tecnologia Wi-Fi para descongestionar as macrocélulas consiste em instalar diversos *Access Points* nas ruas e ambientes *indoor*, conectados a infraestrutura das operadoras que passam por estes locais.

As operadoras de celular estão instalando diversos APs em pontos críticos de diversas cidades para fornecer cobertura Wi-Fi nestes locais. Desse modo, quando um determinado usuário estiver dentro da área de cobertura de um desses APs, ao tentar se conectar a internet pelo 3G associado a macrocélula, este será direcionado automaticamente para a rede Wi-Fi fornecida por sua operadora de telefonia móvel. Isso faz com que qualquer usuário próximo a um *Access Point*

de sua operadora utilize o serviço de Wi-Fi para tráfego de dados, deixando a macrocélula livre para quem não estiver perto de um AP.

A política de segurança empregada nesta tecnologia é o EAP-SIM que autentica o usuário com base em seu *sim card* da operadora. Desse modo, um usuário não consegue utilizar o serviço Wi-Fi de outra operadora diferente da sua.

A utilização do Wi-Fi faz com que o serviço de dados fornecido por cada operadora tenha uma significativa melhora na qualidade, já que são utilizadas antenas de menor capacidade e menor alcance, porém em quantidades cada vez maiores. Um único *Access Point* pode suportar aproximadamente 30 a 50 conexões simultâneas. Bastante se for comparado as femtocélulas, que suportam em média quatro a dez usuários distintos.

Para implementar o Wi-Fi nas ruas, assim como para ambientes *indoor*, deve haver um planejamento. As técnicas de predição e survey são bastante parecidas, podendo até mesmo ser utilizado o mesmo software. A Figura 53 mostra um survey utilizando o Google Earth e o software Air Magnet para mapeamento do sinal de diversos *Access Points* instalados em um bairro.

Figura 53 - Survey outdoor realizado com o Air Magnet



Fonte: (Autor, 2013)

9.2 MOBILE CONCIERGE E ANALYTICS

Mobile Concierge é um conceito bastante inovador e interessante do ponto de vista do usuário e do provedor de serviços. Esta tecnologia traz ao usuário aplicações extremamente úteis e facilitadoras através da utilização do Wi-Fi.

Com base na rede Wi-Fi de um determinado estabelecimento, é possível detectar a presença e a localização de qualquer usuário com o Wi-Fi ativo. Os APs instalados nos diversos ambientes conseguem monitorar o local e enviar dados para que um equipamento chamado MSE (*Mobility Services Engine*) consiga realizar cálculos extremamente complexos e indicar a localização de um usuário naquele ambiente.

Esta tecnologia vem acoplada de uma outra chamada de *Analytics*, que consiste em processar todo tipo de informação de localização e fornecer relatórios detalhados de históricos e eventos relacionados aos usuários.

Este conceito possibilita uma infinidade de aplicações e serviços que podem facilitar a vida de clientes finais e gerar receita para provedores de serviço sobre o Wi-Fi. Até então, o Wi-Fi é utilizado por operadoras para melhorar o serviço de dados, entretanto, isso não significa diretamente aumento dos lucros. Com o conceito de *mobile concierge*, as operadoras podem fornecer serviços a outros clientes e a partir disso, obter lucro através do Wi-Fi.

Mobile Concierge consiste na utilização da rede Wi-Fi para prover serviços e dados de localização tanto para usuários finais quanto para empresas. Um exemplo clássico é a utilização deste conceito em um *shopping center*. Através dos diversos APs instalados ao longo dos corredores e lojas deste *shopping*, é possível monitorar a localização de um determinado cliente caminhando neste estabelecimento. Quando um cliente qualquer passar em frente a uma loja, esta loja será informada sobre o evento e poderá disparar no mesmo instante uma mensagem via Wi-Fi para este cliente lhe oferecendo algum tipo de desconto ou promoção. Além disso através do serviço de *analytics* será possível obter um histórico do cliente e obter informações como: por onde ele caminhou enquanto estava no shopping, por quais lojas ele passou mais tempo em frente a vitrine, por quais departamentos ele permaneceu mais tempo dentro de uma loja, etc. Essas informações são extremamente valiosas para os donos dos estabelecimentos comerciais. Sabendo

isso, eles poderão alocar mais ajudantes a um determinado setor da loja, saber quais produtos chamam mais ou menos atenção e até mesmo saber quais dos clientes que entraram na loja são novos ou antigos e assim personalizar o atendimento ou até mesmo oferecer ofertas exclusivas.

Uma outra aplicação que já vem sendo implementada em diversos locais nos Estados Unidos é a utilização dos serviços de localização *indoor* para auxiliar clientes a localizarem seus pontos de interesse. Por exemplo, em um aeroporto, um turista pode utilizar um aplicativo disponibilizado pelo próprio aeroporto e procurar pelo balcão de sua companhia aérea para realizar o *check-in*. O usuário seleciona no aplicativo a companhia aérea e o número do voo e o aplicativo simplesmente abre um mapa *indoor* com os trajetos que o turista deve seguir, assim como um GPS para ruas, porém dentro do aeroporto. Após realizado o *check-in*, é possível procurar pelo portão de embarque e seguir as orientações do aplicativo para chegar ao destino. Além disso, é possível procurar por sanitários, restaurantes, polícia federal, lojas de conveniência, farmácias, entre outros.

Este conceito auxilia também os funcionários dos aeroportos. Com o analytics, é possível obter informações como os locais que possuem um maior fluxo de passageiros e assim, o aeroporto pode disponibilizar uma equipe maior para aqueles locais afim de auxiliar os passageiros.

A implementação desta tecnologia no Brasil está em fase de testes por parte das fabricantes e provedoras de serviços. Tudo indica que em breve essa tecnologia será utilizada em diversos ambientes comerciais para fornecer aos clientes experiências cada vez mais personalizadas.

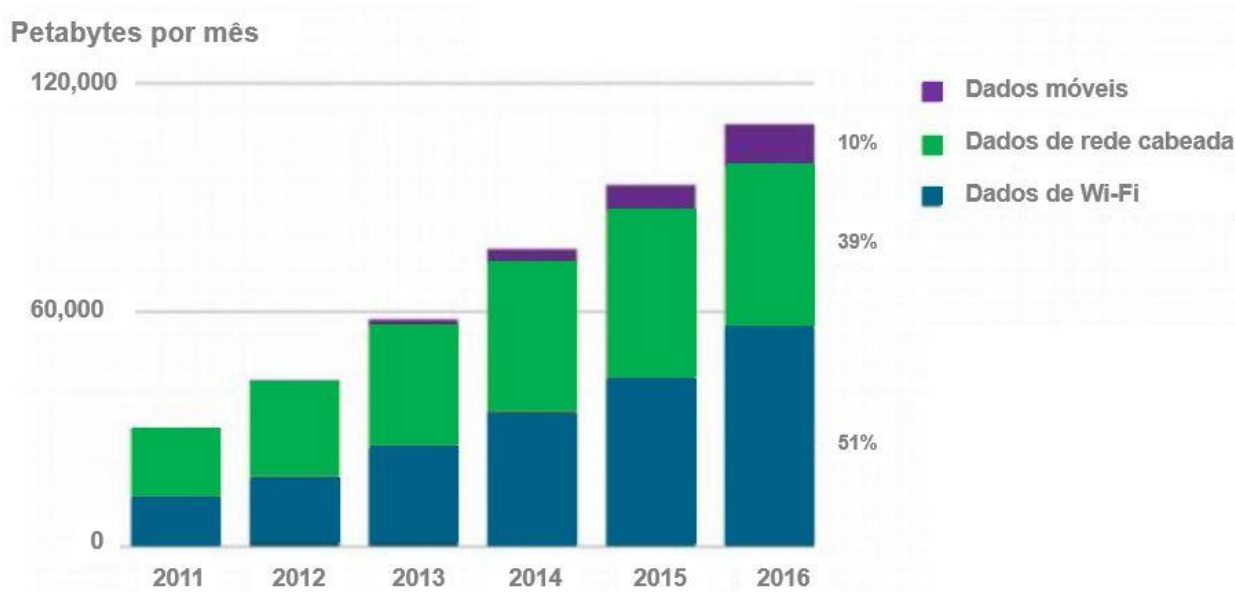
10 CONCLUSÕES

Este trabalho apresentou os conceitos de redes de computadores, fundamentais para o funcionamento das redes sem fio, visto que uma rede Wi-Fi depende de uma rede de distribuição para o seu correto funcionamento. Além disso, foram apresentados os motivos pelos quais o Wi-Fi está sendo fortemente adotado por diversas empresas e usuários domésticos, bem como as mais modernas técnicas de planejamento de RF utilizadas em diversas empresas no mundo inteiro. Essas técnicas são de extrema importância para evitar problemas de performance causados por interferências. Foram citados também os equipamentos que compõem o planejamento e a implementação de uma rede de comunicação sem fio. Através destes conceitos, é possível obter uma noção de como funciona o processo de entrega de um projeto de Wi-Fi. Os métodos e as melhores práticas descritas aqui podem servir tanto para ambientes domésticos como ambientes corporativos, desde casas, escritórios, prédios, galpões, shoppings center e até estádios de futebol.

A popularização da internet e dos dispositivos móveis como *smarphones* e *tablets* transformou a forma como as pessoas utilizam a tecnologia a favor de pessoas e empresas. A tecnologia Wi-Fi teve e ainda tem um papel bastante importante nesta transformação.

São diversas as aplicações encontradas atualmente e através da constante evolução das tecnologias envolvidas no Wi-Fi, cada vez mais aplicações irão surgir. Com isso, segundo a Cisco, a previsão para que o tráfego gerado por redes Wi-Fi superem o das redes cabeadas é 2015, como mostra a Figura 54.

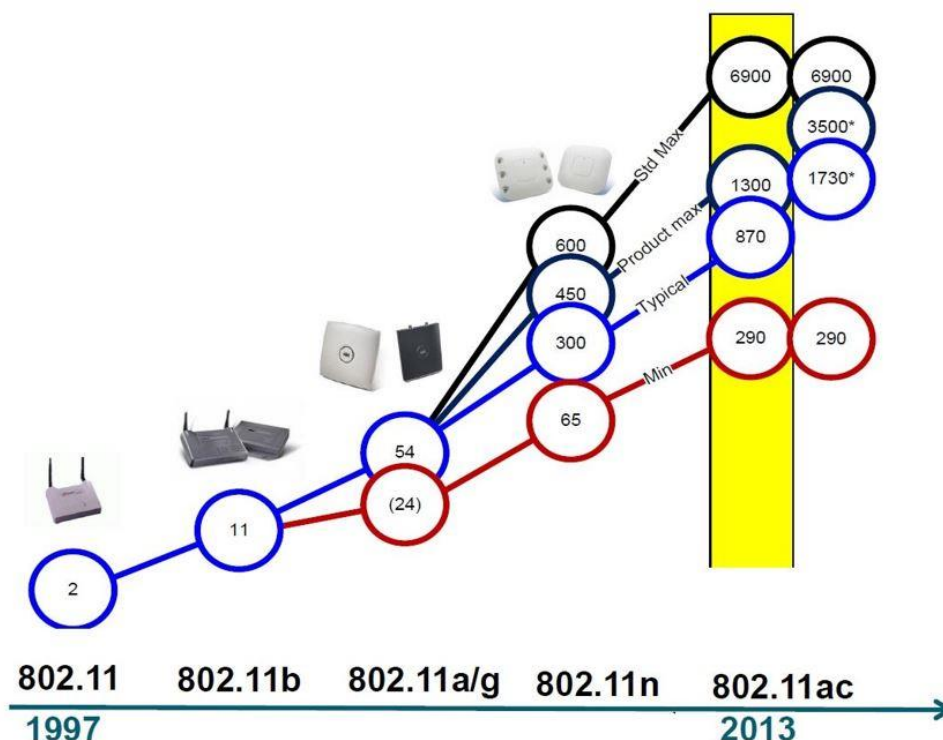
Figura 54 - Previsão de tráfego de dados pelo Wi-Fi



Fonte (Cisco, 2013)

Os padrões 802.11 vistos neste documento tendem a evoluir, aumentando ainda mais a taxa de transmissão e possibilitando aplicações e serviços antes inimagináveis. O atual padrão 802.11n tende a ser substituído pelo 802.11ac já nos próximos anos. Diversos fabricantes de smartphones, ultrabook e notebooks já estão entregando seus produtos com suporte a este novo padrão, bem como as empresas fabricantes de *Access Points*. Recomenda-se fortemente que as empresas escolham por produtos que suportem esta tecnologia já nos seus próximos ciclos de atualização. A Figura 55 ilustra a evolução dos padrões Wi-Fi com o passar dos anos.

Figura 55 - Evolução dos data rates dos padrões Wi-Fi



Fonte (Cisco, 2013)

Com a adoção desses novos padrões, a tendência é eliminar o uso da frequência de 2,4 GHz, causador de inúmeros problemas de performance por conta de interferência. O 802.11ac utiliza a frequência de 5,0 GHz e por isso, seu sinal está menos propício a vazar para outros ambientes e andares, fazendo com que a implementação de uma rede Wi-Fi possua mais antenas com um menor raio de cobertura, porém com uma maior qualidade de sinal para todos os usuários. Este pensamento também deve predominar no desenho e planejamento das femtocélulas e APs para descongestionamento das redes móveis, ou seja, utilizar uma maior quantidade de antenas com menor área de cobertura, porém com maior qualidade de sinal.

Através dos diversos argumentos citados neste trabalho, bem a apresentação da evolução das tecnologias que envolvem o Wi-Fi e suas diversas aplicações que vem surgindo com o tempo, este documento deixa claro a importância do Wi-Fi atualmente e para os projetos futuros. Esta tecnologia ainda será muito utilizada nos próximos anos aumentando a eficiência de processos e abrindo uma nova gama de serviços disponíveis.

REFERÊNCIAS

- RAPAPPORT, T.S. **Comunicações sem fio princípios e práticas**. 2. Ed. Prentice Hall. Brasil, 2009. São Paulo.
- HAYKIN, S.; MOHER, M. **Sistemas modernos de comunicação wireless**. 1. Ed. Bookman, 2008. Brasil.
- BERNAL, P.S.M.; MOHER, M. **Comunicações móveis: tecnologias e aplicações**. 1. Ed. Érica, 2002. Brasil.
- AGILENT TECHNOLOGIES. **RF testing of WLAN products**. Disponível em:<<http://www.cp.literature.agilent.com/litweb/pdf/5988-3762EN.pdf>>. Acesso em 01 nov 2013.
- MALBURG, M.M. **Trabalho dinal de redes I**. 2004. Disponível em:<http://www.gta.ufrj.br/grad/04_2/Modulacao/>. Acesso em 27 out 2013.
- CORDEIRO, C.M.; GOSSAIN, H.; ASHOK, L.; AGRAWAL, D.P. **The last mile: wireless technologies for broadband and home networks**. Cincinnati. Disponível em:<<http://www.cs.uc.edu/~cordeicm/course/wirelessbroadband-text.pdf>>. Acesso em 27 out 2013.
- HANSEN, J. **802.11B/A – A physical medium comparison**. 2002. Disponível em:<<http://www.mobiledevdesign.com/news/80211ba-physical-medium-comparison/>>. Acesso em 07 nov 2013.
- FAINBERG, M. **A Performance analysis of the IEEE 802.11b Local area network in the presence of bluetooth personal area network**. 2001. Disponível em:<<http://www.eeweb.poly.edu/dgoodman/fainberg.pdf>>. Acesso em 20 out 2013.
- SIMÕES, J.E. **WiMAX**. 2007. Disponível em:<http://www.gta.ufrj.br/grad/07_2/jefferson/index.html>. Acesso em 22 out 2013.
- CISCO. **WLAN radio frequency design considerations**. Disponível em:<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch3_WLAN.pdf>. Acesso em 15 out 2013.
- BRAGA, N.C. **Técnicas de modulação AM/FM**. Disponível em:<<http://www.newtoncbraga.com.br/indedx.php/telecomunicacoes/6413-tel075>>. Acesso em 10 out 2013.

FERRARI, A. **Modulação angular**. 2013. Disponível em:< <http://www.ackf006eletronica.blogspot.com.br/2013/05/modulacao-angular.html>>. Acesso em 04 out 2013.

POOLE, I. **Comparison of 8-QAM, 16-QAM, 32-QAM, 64-QAM, 128-QAM, 256-QAM, etc.** Disponível em:< <http://www.radio-eletronics.com/info/rf-technology-design/pm-phase-modulation/8qam-16qam-32qam-64wam-128qam-256qam.php>>. Acesso em 05 out 2013.

ADMIN. **What is a “stream” anyway? (how 802.11n works)**. 2009. Disponível em:< <http://www.blog.merunetworks.com/blog/2009/08/what-is-a-stream-anyway-how-802-11n-works/>>. Acesso em 10 nov 2013.

BOYD, R. **Not all streams are created equal**. Disponível em:< <http://www.blogs.cisco.com/cin/not-all-streams-are-created-qual/#more-60253>>. Acesso em 10 nov 2013.

CISCO. **Configuring 802.11 parameters**. Disponível em:< http://www.cisco.com/en/US/docs/wireless/7.5/config_guide/b_cg75_chapter_0101.html#ID1326>. Acesso em 13 nov 2013.

TELECO. **WLAN de alta velocidade I: protocolos**. Disponível em:< http://www.teleco.com.br/tutoriais/tutorialredeswlan/pagina_5.asp >. Acesso em 20 set 2013.

CONOVER, J. **Anatomy of IEEE 802.11b wireless**. 2000. Disponível em:< <http://www.networkcomputing.com/1115/1115ws2.html> >. Acesso em 25 out 2013.

GAO, J. **CDMA with direct sequence spread spectrum**. 2007. Disponível em:< <http://www.cs.sunysb.edu/~jgao/CSE370-spring10/dsss.pdf>>. Acesso em 19 out 2013.

CISCO. **Capacity coverage & deployment considerations for IEEE 802.11g**. Disponível em :< http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00801d61a3.shtml>. Acesso em 13 nov 2013.

CISCO. **Cisco aironet 1600/2600/3600 series access point deployment g**. Disponível em:<http://www.cisco.com/en/US/docs/wireless/technology/apdeploy/Cisco_Aironet.html#wp44990>. Acesso em 13 nov 2013.

ESTRADA, P. **Using spectrum wisely with band steering**. 2011. Disponível em:<<http://www.meraki.cisco.com/blog/2011/04/using-spectrum-wisely-with-band-steering/>>. Acesso em 16 nov 2013.

CALHOUN, P. **What's up with MIMO? – part deux**. 2007. Disponível em:<http://blogs.cisco.com/wireless/whats_up_with_mimo_part_deux/>. Acesso em 17 nov 2013.

CISCO. **802.11ac: the fifth generation of Wi-Fi technical white paper**. 2007. Disponível em:<http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.html>. Acesso em 18 nov 2013.

CISCO. **Radio channel frequencies**. Disponível em:<<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.pdf>>. Acesso em 01 nov 2013.

CISCO. **Cisco aironet 3500 series access point**. Disponível em:<http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/data_sheet_c78-594630.pdf>. Acesso em 01 nov 2013.

APÊNDICE A 1 - REDES DE COMPUTADORES

Os conceitos básicos de redes de computadores são fundamentais para o entendimento das redes sem fio. Este anexo e os anexos seguintes apresentam as principais características e como funciona uma rede de computadores.

As redes de computadores surgiram da necessidade de enviar, acessar, receber e processar informações localizadas em um outro computador. Este computador pode estar tanto na sala ao lado quanto do outro lado do planeta.

Uma rede de computador é um conjunto de computadores interconectados, tanto diretamente ou através de um equipamento intermediário que liga dois ou mais computadores. Em uma rede, computadores transferem informações um para o outro através das conexões entre eles. Essa conexão pode ser estabelecida tanto através de cabos ou através de tecnologias sem fio.

Dispositivos de rede que originam, terminam ou roteiam um tipo de informação é chamado de nó.

Atualmente, empresas e seus profissionais criam suas próprias redes de computadores com o objetivo de compartilhar arquivos, recursos e rodar aplicações com o intuito de trazer facilidade e eficiência para o profissional. Um exemplo: uma determinada empresa possui uma rede de computadores composta por notebooks de seus funcionários. Quando eles desejam imprimir algum documento na impressora, não seria muito cômodo cada um levar o seu notebook para perto da impressora, conectar o cabo entre os dois e aí sim iniciar a impressão. Para melhorar essa situação, as empresas passaram a conectar a impressora na rede de computadores onde estavam os notebooks. Dessa maneira, cada funcionário, de sua própria mesa, poderia enviar uma requisição de impressão para a impressora e levantar para buscar somente ao término da operação, sem a necessidade de levar seu notebook. Talvez fique ainda mais claro com este outro exemplo: essa mesma empresa possui diversas áreas, entre elas a área de pré-vendas, responsável por realizar propostas comerciais aos seus clientes. Essa área necessita de uma quantidade considerável de planilhas e documentos para consolidar uma proposta de maneira competitiva. Entretanto, a área de pré-vendas é composta por diversos profissionais, cada um responsável por uma parte da proposta, porém todos necessitam de acesso aos documentos. Uma solução que uma rede de

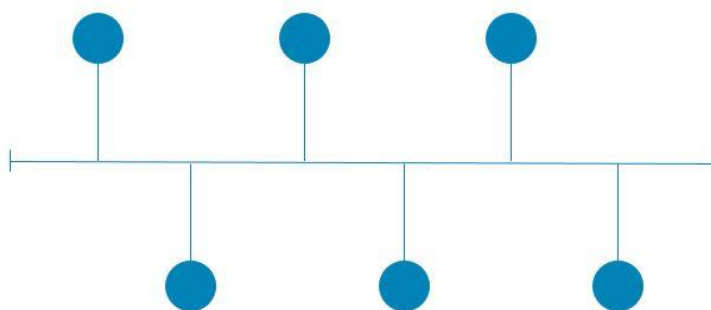
computador proporciona nesse caso é o armazenamento de todas essas planilhas e documentos em um servidor central, conectado na rede da empresa, permitindo o acesso por todos os funcionários da área em questão. Assim, as redes de computadores são projetadas com o intuito de compartilhar recursos, tanto de software quanto de hardware, independentemente da localização física do recurso ou do usuário.

Pode-se imaginar uma rede pequena como o caso do exemplo da impressora, citado acima, ou uma rede de uma empresa multinacional onde funcionários de um país possuem acesso a recursos computacionais de um servidor localizado em um outro continente. Existem ainda as redes ponto-a-ponto, menos comum hoje em dia, formado pela conexão direta de um computador a outro, através de um meio físico, como um par metálico ou um cabo coaxial. Um enlace multiponto é um exemplo de enlace utilizado em tecnologias LAN (Local Area Network). Uma LAN é uma rede de computadores que conecta os dispositivos em uma área limitada, como uma casa, escola, ou um prédio de uma empresa. Existem diversas topologias nas quais uma LAN pode estar baseada:

Topologia em barramento

A Figura 56 ilustra uma topologia em barramento:

Figura 56 - Topologia em barramento



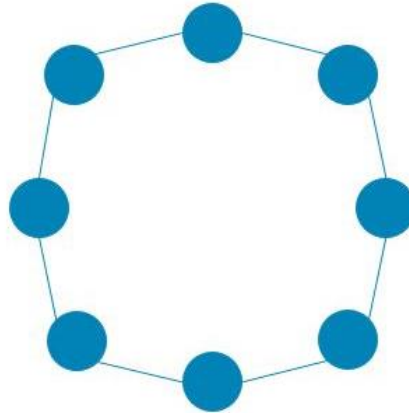
Fonte: (Autor, 2013)

Em uma topologia em barramento, todos os dispositivos são conectados por apenas um único cabo.

Topologia em anel

A Figura 57 ilustra uma topologia em anel:

Figura 57 - Topologia em anel



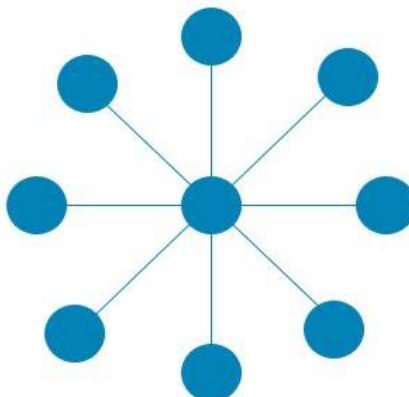
Fonte: (Autor, 2013)

Em uma topologia em anel, todos os dispositivos estão conectados em um formato de anel. Em algumas implementações, um *token* viaja ao redor do anel parando em cada um dos dispositivos. Se um dispositivo quer enviar alguma informação, este adiciona o endereço de destino e o dado em si ao token. Então, o token viaja para ao redor do anel, até que ele encontre o dispositivo de destino. Uma vantagem deste tipo de topologia é que não existem colisões de pacote de dados.

Topologia em estrela

A Figura 58 mostra uma topologia em estrela, muito utilizada atualmente.

Figura 58 - Topologia em estrela



Fonte: (Autor, 2013)

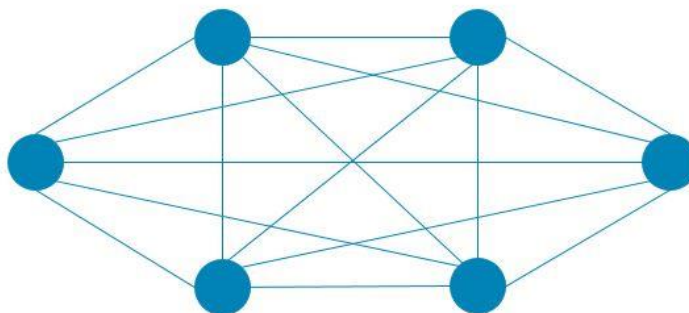
Este tipo de topologia é a mais utilizada em redes Ethernet LAN atualmente. Ela consiste em uma conexão central a um dispositivo onde todos os segmentos se encontram. Cada dispositivo é conectado ao dispositivo central com seu próprio cabo. Dessa maneira, problemas que podem vir a ocorrer com um determinado cabo irá afetar somente um dispositivo e não a rede inteira, como ocorre em topologias em barramento e em anel.

Apesar deste tipo de topologia ser um pouco mais custoso, seus benefícios fazem valer a pena.

Topologia *Mesh*

A Figura 59 ilustra uma topologia *Mesh*:

Figura 59 - Topologia Mesh

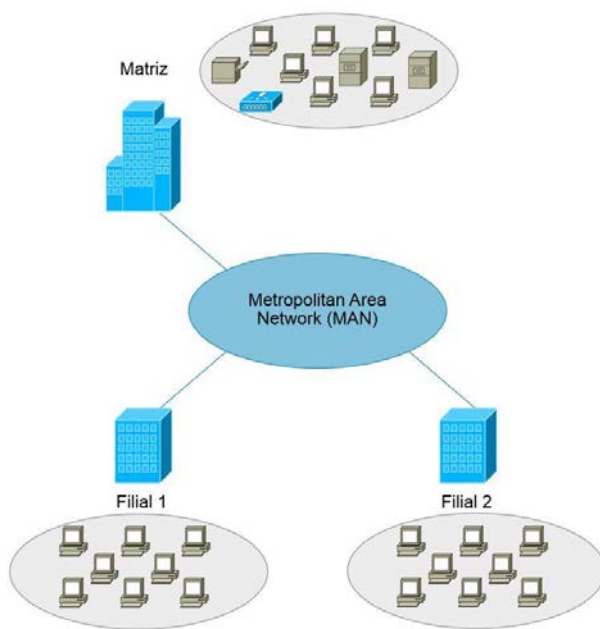


Fonte: (Autor, 2013)

A topologia *mesh* conecta todos os dispositivos a todos os outros da topologia para redundância e resiliência. Este método é o mais resistente a falhas, entretanto, o mais caro e complicado de se implementar.

E se uma filial de uma empresa precisa se conectar a rede da matriz, localizada em um local diferente da cidade? Para esses casos, existem as MANs (Metropolitan Area Network), que se caracterizam por dois ou mais computadores conectados, porém separados geograficamente, mas na mesma cidade. As MANs permitem a conexão de diversas LANs localizadas dentro de uma mesma cidade, como ilustra a Figura 60:

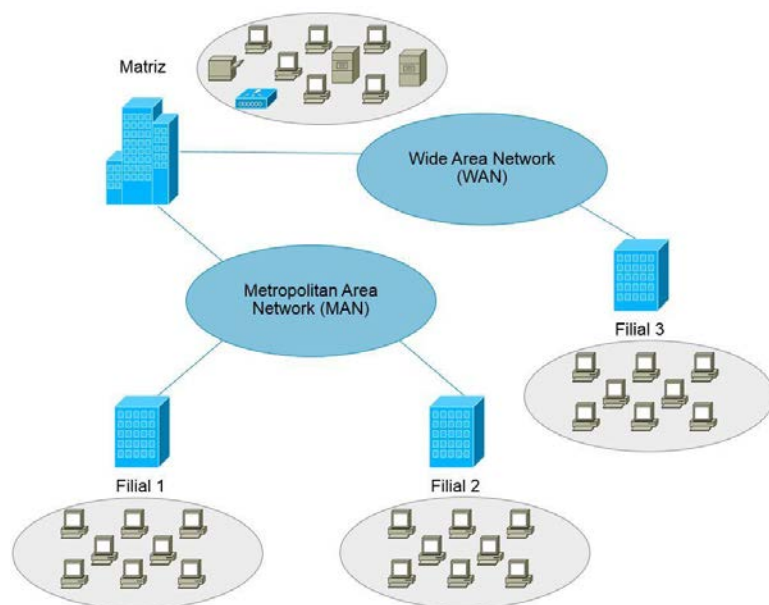
Figura 60 - Metropolitan Area Network



Fonte: (Autor, 2013)

Por último, temos o caso de uma empresa multinacional com sua matriz em um país e diversas filiais localizadas em outros países e até em outros continentes. Para conectar as filiais entre si e com a matriz, é utilizado a tecnologia WAN (Wide Area Network). Uma WAN é uma rede de computadores que se espalha por uma vasta área, ultrapassando limites de cidades, países e continentes, e permite transferir informações e dados entre várias LANs e MANs. A Figura 61 ilustra uma WAN, onde a Filial 3, no caso, está localizado em outro estado ou até país.

Figura 61 - Wide Area Network



Fonte: (Autor, 2013)

Uma WAN pode ser privada, ou seja, pertence a uma empresa particular, ou pode ser projetada e construída por uma ISP (Internet Service Provider), que disponibiliza acesso a internet para as LANs das empresas. Quando uma empresa deseja realizar a conexão entre duas LANs separadas geograficamente por uma distância muito longa, as ISPs geralmente são contratadas para realizar o empréstimo de suas linhas de transmissão, uma vez que o custo para passar um cabo transmissor da fonte até o destino seria inviável para essa empresa. Essas linhas de transmissão de uma ISP são chamadas de *Leased Lines* e o contratante, no caso a empresa, paga uma taxa mensal pela sua utilização. *Leased Lines* conectam dois locais distantes um do outro provendo serviços privado de voz e/ou dados.

APÊNDICE A 1.1 - MODELO OSI

A partir do momento em que um usuário envia alguma informação pela internet, diversos processos ocorrem até que a informação chegue efetivamente ao destino. Essa transmissão de informação é baseada em uma série de protocolos que foram criados principalmente para facilitar o processo de interconectividade entre máquinas de diferentes fabricantes. No início da expansão da internet, diversos fabricantes desenvolviam equipamentos que permitiam a conexão entre diversos computadores, montando assim uma rede. Porém, devido ao fato de cada fabricante possuir sua própria arquitetura, não era possível interligar esses equipamentos com o objetivo de unir duas ou mais redes formadas por diversos outros computadores. Devido a este fato, uma série de padrões internacionais foram criados com o intuito de compatibilizar todos esses equipamentos de diferentes fabricantes.

O Modelo OSI (Open Systems Interconnection), lançado em 1984 pela ISO (International Organization for Standardization), foi o primeiro modelo conceitual que caracteriza e padroniza as funções internas de um sistema de comunicação através do particionamento em camadas. Este modelo agrupa funções de comunicação similares em uma das sete camadas. O Modelo OSI permite a compatibilidade, portabilidade, escalabilidade e interoperabilidade entre equipamentos de diversos fabricantes através da atribuição de serviços e funções para cada camada do modelo.

A Tabela 12 a seguir mostra as sete camadas do modelo OSI:

Tabela 12 - Camadas do Modelo OSI

Camadas do Modelo OSI	
Número	Camada
7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

APÊNDICE A 1.1.1 - CAMADA DE APLICAÇÃO

A camada de aplicação do modelo OSI é a que se situa de maneira mais próxima ao usuário final. Tanto a camada de aplicação quanto o usuário, interagem diretamente com uma determinada aplicação/software. Essa camada interage com aplicações que utilizam serviços de comunicação, entre eles, aplicações de e-mail, aplicações de transferência de arquivos, jogos online, aplicações de mensagem online, etc. As principais funções da camada de aplicação são identificar com quem aquela aplicação irá se comunicar e se este está disponível, determinar os recursos de comunicação disponíveis e realizar a sincronização da comunicação.

APÊNDICE A 1.1.2 - CAMADA DE APRESENTAÇÃO

A camada de apresentação tem suas funções definidas para que todas as informações enviadas à camada de aplicação sejam legíveis e aceita por esta. A camada seis do Modelo OSI converte, formata e realiza a criptografia, quando necessário da informação.

APÊNDICE A 1.1.3 - CAMADA DE SESSÃO

A camada de sessão é responsável pelo controle de conexões entre dois computadores, estabelecendo, gerenciando e finalizando conexões entre aplicações locais e remotas.

APÊNDICE A 1.1.4 - CAMADA DE TRANSPORTE

Talvez uma das mais importantes camadas do modelo OSI, a camada de transporte é responsável por receber os dados da camada de sessão e segmentá-los para que sejam enviados a cada de rede. A camada quatro do modelo fornece uma transferência de informações confiável entre dois nós. Essa confiabilidade é possível através de diversos recursos que essa camada oferece, como: controle de fluxo, segmentação de informação e controle de erro.

Os dois protocolos mais comuns da camada de transporte são o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol). Eles são responsáveis pelo gerenciamento da comunicação entre múltiplas aplicações e fornecer serviços de comunicação para os processos das aplicações e os dispositivos da rede.

O TCP é um protocolo orientado a conexão, ou seja, uma conexão deve ser estabelecida entre a fonte e o destino antes do envio de qualquer dado. Através dessa conexão, a camada de transporte consegue rastrear todos os segmentos que foram enviados ao destino e reenviar aqueles que falharam. Além disso, essa conexão permite conferir se os segmentos chegaram na ordem correta, impedindo que o dado seja inutilizado. Todos esses processos fazem com que o TCP seja um protocolo de alta confiabilidade, porém mais lento na transmissão de dados. Já o UDP é um protocolo mais ágil, mas em contrapartida, não efetua todos esses processos de verificação de erros, ordem e controle de fluxo.

Não é porque um protocolo é mais ágil que o outro, que o UDP não é utilizado. Cada um tem suas vantagens e desvantagens e por isso possuem suas aplicações específicas. O TCP é utilizado para aplicações de e-mail, compartilhamento de arquivos e downloads. Já o UDP, por ser mais ágil e não possuir mecanismos de controle de falha, é utilizado em aplicações de streaming de vídeo e voz (que requerem uma velocidade maior na transmissão) uma vez que uma pequena falha no envio de um dado não acarretaria um grande problema na aplicação como um todo, uma vez que é possível entender um vídeo, mesmo que haja uma pequena informação faltando, como alguns milissegundos do vídeo, ao contrário do que ocorre com um compartilhamento de arquivos. Pode não ser possível aproveitar e utilizar um determinado arquivo se ele vier com algum tipo de defeito.

APÊNDICE A 1.1.5 - CAMADA DE REDE

A camada de rede fornece meios para transferência de pacotes de dados de uma rede a outra. Os roteadores (equipamento de rede responsável pela seleção de caminho) operam nessa camada.

APÊNDICE A 1.1.6 - CAMADA DE ENLACE

A camada de enlace fornece um link confiável de conexão entre dois nós, detectando e corrigindo erros que possam acontecer na camada física.

Essa camada também fornece recursos de controle de acesso aos meios físicos de conexão. Por exemplo, em uma topologia de barramento, somente um dispositivo pode enviar informações de cada vez. A camada de enlace é responsável por controlar qual dispositivo enviará dados em um determinado instante afim de não haver dois dispositivos enviando ao mesmo tempo, e consequentemente, não haver colisão de informação.

APÊNDICE A 1.1.7 - CAMADA FÍSICA

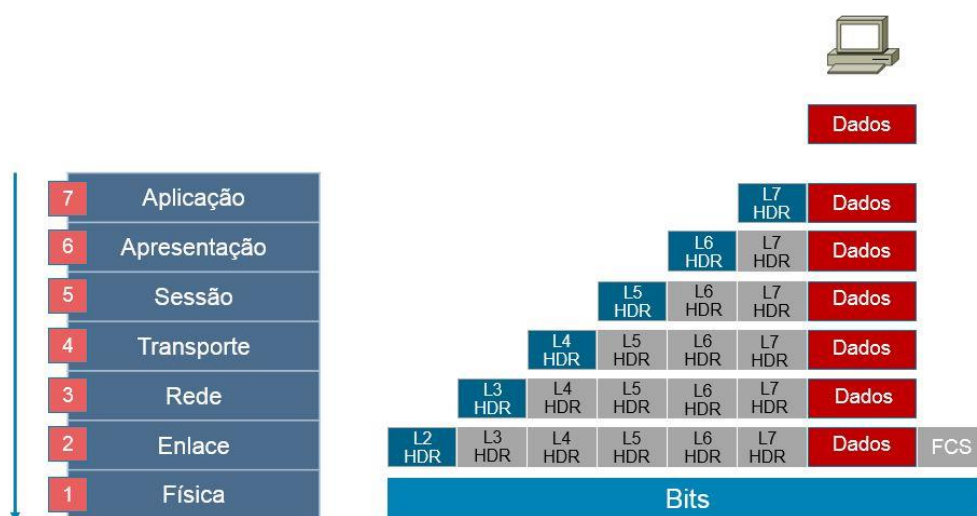
A camada física estabelece as especificações elétricas, mecânicas, procedurais e funcionais para ativação, desativação e manutenção de links físicos. Além disso, define as relações entre um dispositivo e o meio de transmissão (ex: cabo de cobre ou fibra). Isso inclui os pinos, tensões, impedância, especificações do cabo, hubs, repetidores, adaptadores de rede, etc.

APÊNDICE A 1.2 - ENCAPSULAMENTO E DESENCAPSULAMENTO

Todas essas camadas são muito importantes para o processo de comunicação e transmissão de dados entre dois dispositivos. Até agora, foi explicado qual a função de cada uma, quais os recursos que cada uma estabelece e a sua importância. Entretanto, é também de extrema importância entender como cada camada interage com as camadas vizinhas e quais transformações um dado sofre ao ser transmitido de um dispositivo a outro.

Quando uma determinada aplicação gera uma informação que deve ser transmitida a outro dispositivo, a camada de aplicação insere um cabeçalho nesta informação. Assim, este dado adicionado de um cabeçalho é passado para a próxima camada de baixo, que é a de apresentação. Essa, por sua vez, também adiciona um cabeçalho, com informações referentes a essa camada, ao dado que foi passado da camada superior. A partir daí, o processo se repete até a camada física. Cada protocolo pertencente a sua respectiva camada adiciona informações de controle no dado gerado pela aplicação e passa o dado para a camada seguinte. Quando esse dado chega a camada física, ele está atrelado a diversas outras informações de controle de diversos protocolos das camadas superiores. A Figura 62 mostra este processo até a camada física.

Figura 62 - Processo de Encapsulamento do Modelo OSI



Fonte: (Autor, 2013)

Este processo, onde cada camada adiciona ao dado, gerado pela aplicação, um cabeçalho contendo informações de controle de diversos protocolos, e passa o dado resultante para a camada inferior, é chamado de encapsulamento.

Uma vez que essa informação é transmitida pelo meio físico e chega ao dispositivo de destino, este, por sua vez, precisa entender o que, de fato, é o dado que deve ser entregue a aplicação. Além disso, a informação passou por diversos processos de formatação, segmentação, controle de erros e fluxo, e por isso, deve haver informações adicionais que permitam o dispositivo de destino saber organizar e reformatar esses dados de uma maneira que a aplicação de destino possa entender o dado enviado. Essas informações adicionais são os cabeçalhos que cada camada adicionou no processo de encapsulamento. Ou seja, para que a aplicação de destino entenda a informação que foi enviada, esta deve sofrer um processo inverso, o de desencapsulamento. Neste processo, a informação, ao invés de passar pelas camadas mais altas até a mais inferior, ela passa primeiro pela camada física e vai subindo até chegar a camada de aplicação. Nisso, cada camada retira do dado enviado e processa o cabeçalho que foi inserido pela respectiva camada no processo de encapsulamento no dispositivo de origem. Assim, ao chegar na camada sete, a informação está de um modo legível para a aplicação de destino. A Figura 63 mostra o processo de desencapsulamento:

Figura 63 - Processo de Desencapsulamento do Modelo OSI



Fonte: (Autor, 2013)

APÊNDICE A 1.3 - IP

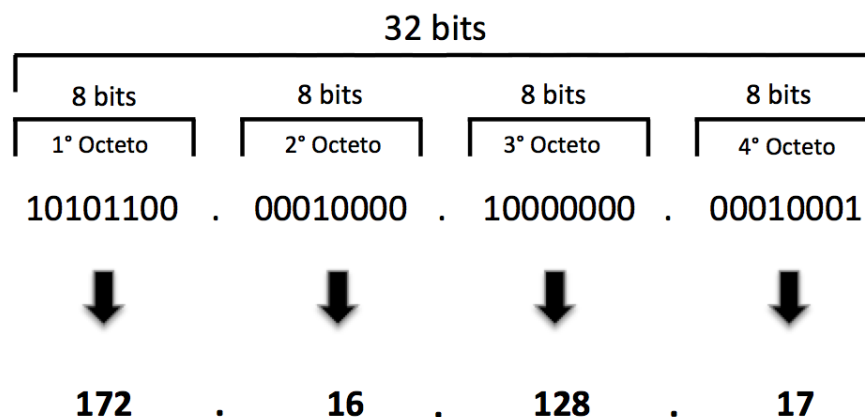
IP significa *Internet Protocol*. Este é um dos principais protocolos de rede baseados em padrões que existe atualmente. O IP determina pra onde serão roteados os pacotes de dados baseado nos endereços de destino.

Algumas de suas características são:

- Opera na camada de rede do Modelo OSI e na camada de Internet do TCP/IP;
- Utiliza pacotes para transportar informações através de uma rede;
- É um protocolo não orientado a conexão, ou seja, não existe verificação se a informação chegou, de fato, ao destino;
- Não possui recursos de recuperação de dados;
- Utiliza endereços lógicos para rotear pacotes, chamados de endereço IP.

Um endereço IP identifica unicamente um dispositivo em uma rede IP. Este endereço consiste em um número de 32 bits, dividido em quatro grupos (octetos) de oito bits. Cada octeto é representado por um número decimal entre 0 e 255, separados por um ponto (*dotted decimal notation*). A Figura 64 mostra como é formado um endereço IP.

Figura 64 - Composição de um endereço IP



Fonte: (Autor, 2013)

Um endereço IP é separado por duas partes:

- ID da rede: indica qual rede um determinado host faz parte e é usado pelos roteadores para manter informações sobre rotas.
- ID do host: identifica um único host em uma determinada rede.

Através dessa separação, pode-se classificar os endereços IP em 3 classes:

- Classe A: o primeiro octeto é utilizado para representar redes e os outros três utilizados para representar hosts;
- Classe B: primeiro e segundo octeto utilizados para representar redes e os outros dois utilizados para representar hosts;
- Classe C: os três primeiros octetos são utilizados para representar redes e o último octeto utilizado para representar hosts.

A Figura 65 ilustra a classificação dos endereços IPs:

Figura 65 - Classificação dos Endereços IP

0 1 0 0 0 0 0 0	0 1 1 0 0 0 0 0	1 1 0 0 0 0 0 1	1 1 1 1 0 0 1 0
64	96	193	242
REDE	HOST	HOST	HOST

Endereço IP Classe A

1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 1 1 0 0 1 0	0 0 0 0 0 1 0 0
172	16	242	4
REDE	REDE	HOST	HOST

Endereço IP Classe B

1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0
192	168	1	2
REDE	REDE	REDE	HOST

Endereço IP Classe C

Fonte: (Autor, 2013)

Uma rede é um conjunto de computadores interconectados diretamente ou através de um dispositivo intermediário. Cada computador ou máquina conectado a uma rede é chamado de host. Este host, recebe um endereço IP, pertencente a sua rede, para que possa ser identificado pelos

roteadores. Um roteador é um equipamento que tem a função de rotear pacotes, com base nos endereços IPs de destino. Assim, quando um roteador recebe um pacote, ele realiza o processo de desencapsulamento até obter o endereço de IP de destino, que está localizado no cabeçalho que foi inserido pela Camada de Rede do Modelo OSI, ou pela camada de Internet do modelo TCP/IP. O roteador utiliza o endereço IP de destino para verificar para onde enviar esse pacote para que este chegue de maneira mais rápida ao seu destino.

A Figura 66 mostra alguns modelos de roteadores disponíveis hoje no mercado.

Figura 66 - Modelos de roteadores



Fonte: (Cisco, 2013)

Quando profissionais de TI (Tecnologia da Informação) desenham uma topologia para representar uma rede de computadores, eles utilizam o desenho da Figura 67 para representar roteadores.

Figura 67 - Representação de um Roteador em uma Topologia



Fonte: (Cisco, 2013)

Um roteador interliga diversas redes diferentes e escolhe o melhor caminho para enviar um pacote, com base no endereço IP de destino. Mas o que é uma rede diferente? Uma determinada rede se distingue de uma outra através do endereço IP da rede. Foi visto anteriormente que os endereços IPs são divididos em duas partes: ID da rede e ID do host. Um endereço IP classe B utiliza os dois primeiros octetos (primeiros 16 bits) para representar redes e os outros dois octetos (16 bits) são utilizados para representar hosts. O endereço IP ilustrado na Figura 64 é um endereço de classe B. Assim, o IP 172.16.128.17 é um endereço de um host pertencente a rede 172.16.0.0. Uma vez que um IP classe B utiliza os dois primeiros octetos para representar uma rede, 172.16 representa a rede e 128.17 representa o host dessa rede. Da mesma maneira, o endereço IP 172.16.128.18 também é um IP dessa mesma rede. Mas qual rede? Se a rede é representada por 172.16, pode-se dizer que o endereço IP dessa rede é 172.16.0.0. Concluindo, os hosts 172.16.128.17 e 172.16.128.18 pertencem a rede 172.16.0.0.

Mas por que o endereço IP da Figura 64 é um endereço de classe B? Para classificar os endereços IPs em suas respectivas classes, deve-se analisar o primeiro octeto (8 bits). Para um endereço classe A, obrigatoriamente, o primeiro bit é sempre 0. Assim, o menor valor decimal do primeiro octeto de um IP classe A é 0 (00000000) e o maior é 127 (01111111). Porém, os valores 0 e 127 são número reservados. Desse modo, qualquer endereço IP que começa com um valor entre 1 e 126 é um endereço classe A. Já em um endereço classe B, os dois primeiros bits do primeiro octeto devem ser sempre 10, podendo um endereço ir de 128 (10000000) até 191 (10111111). E por fim, em um endereço classe C, os três primeiros bits do primeiro octeto devem ser sempre 110, e assim, podendo ir de 192 (11000000) até 223 (11011111). Dessa forma, o endereço da Figura 64 172.16.128.17 é um endereço classe B pois está entre 128 e 191.

O Quadro 2 ilustra de forma clara a classificação de endereços IPs.

Quadro 2 – Classificação de Endereços IP

Classe A	0 XXX XXXX . HOST . HOST . HOST
	Mínimo: 0 000 0000 . HOST . HOST . HOST = 0 . HOST . HOST . HOST
	Máximo 0 111 1111 . HOST . HOST . HOST = 127 . HOST . HOST . HOST
	0 e 127 reservados.
	Mínimo: 0 000 0001 . HOST . HOST . HOST = 1 . HOST . HOST . HOST
	Máximo 0 111 1110 . HOST . HOST . HOST = 126 . HOST . HOST . HOST
Classe B	10 XX XXXX . HOST . HOST . HOST
	Mínimo: 10 00 0000 . REDE . HOST . HOST = 128 . REDE . HOST . HOST
	Máximo 10 11 1111 . REDE . HOST . HOST = 191 . REDE . HOST . HOST
Classe C	110 XX XXXX . HOST . HOST . HOST
	Mínimo: 110 00 0000 . REDE . REDE . HOST = 192 . REDE . REDE . HOST
	Máximo 110 11 1111 . REDE . REDE . HOST = 223 . REDE . REDE . HOST

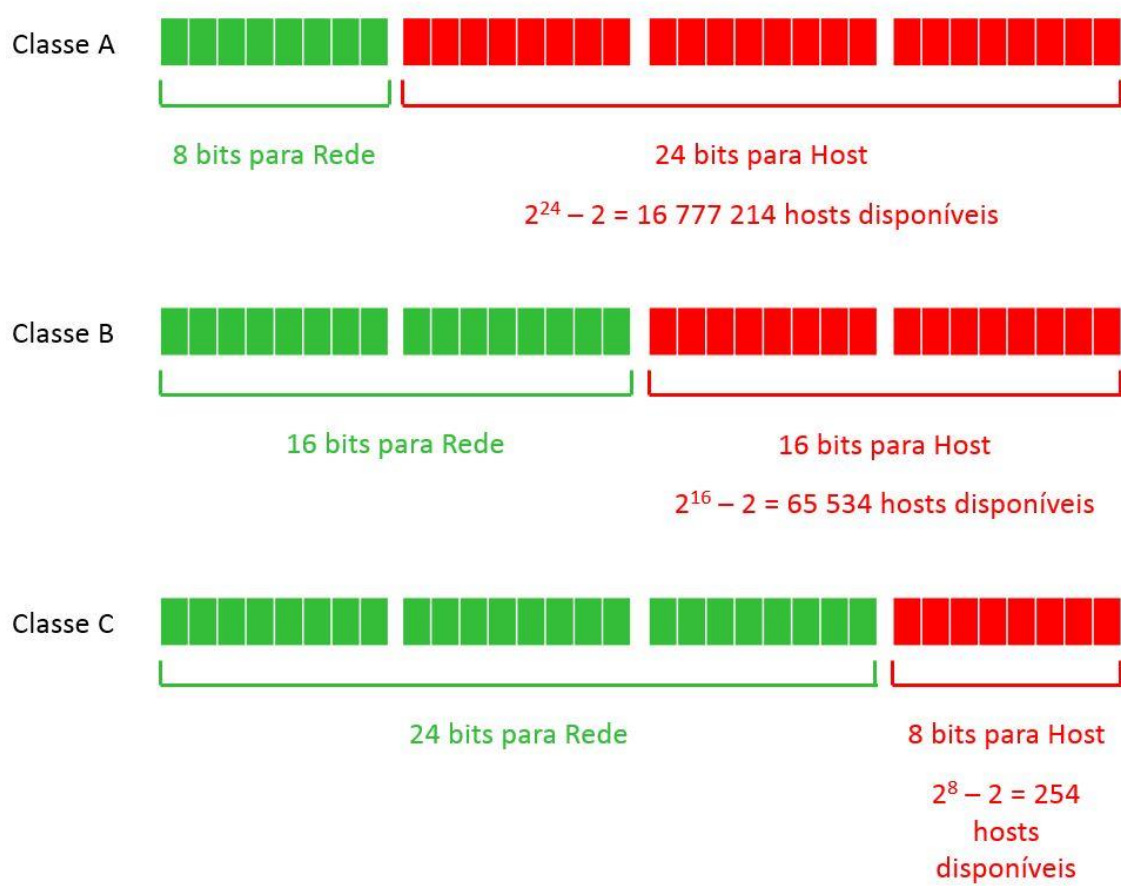
A Tabela 13 mostra alguns exemplos de endereços IPs e suas redes:

Tabela 13 - Exemplo de Endereços IP

Exemplos de Endereços IP		
IP do host	Rede	Classe
9.80.5.12	9.0.0.0	A
10.0.0.1	10.0.0.0	A
172.16.0.1	172.16.0.0	B
184.30.28.5	184.30.0.0	B
192.168.1.1	192.168.1.0	C
192.168.10.1	192.168.10.0	C

Sabe-se que um endereço de rede não pode ser atribuído para um host. Além disso, existe uma outra restrição. O último endereço de host de cada rede também não pode ser atribuído para um host. Este endereço é reservado para mensagens de *broadcast*. Uma mensagem de *broadcast* é uma mensagem cujo destino são todos os hosts dessa rede. Por exemplo, um pacote destinado ao IP 192.168.1.2. Este pacote tem como destino o host cujo IP é 192.168.1.2, pertencente a rede 192.168.1.0, uma vez que esse é um endereço IP classe C. O último endereço de host dessa rede seria 192.168.1.255, já que 192.168.2.0 já é o endereço IP da próxima rede. Porém, 192.168.1.255 é um endereço reservado para quando um host dessa rede 192.168.1.0 deseja mandar uma mensagem para todos os hosts dessa mesma rede. Assim, o último endereço que pode-se fornecer a um host dessa rede é 192.168.1.254. Isso acontece para qualquer outra rede. Por exemplo, a rede 172.16.0.0, pertencente a Classe B. O primeiro endereço que pode-se atribuir para um host dessa rede é 172.16.0.1 e o último é 172.16.255.254, já que 172.16.255.255 é reservado para mensagens de *broadcast*. Pode-se perceber então que para toda rede, dois endereços IPs não podem ser atribuídos a hosts: o próprio endereço da rede e o último endereço da rede. Através disso, pode-se fazer a análise, como mostra a Figura 68.

Figura 68 - Número de Hosts Disponíveis



Fonte: (Autor, 2013)

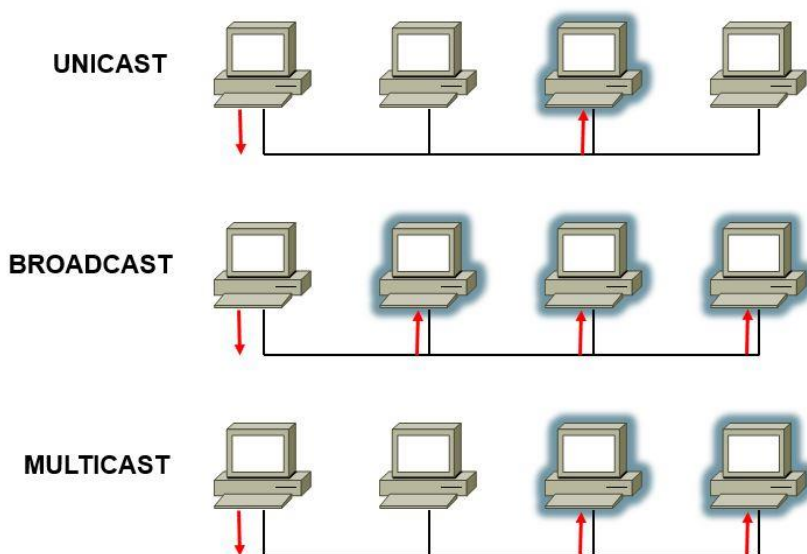
APÊNDICE A 1.4 - ETHERNET

A Ethernet é um conjunto de tecnologias desenvolvidas para redes locais (LAN), baseadas na norma IEEE 802.3, que define e estabelece diversos padrões de transmissão e tipos de interconexão para redes locais.

A Ethernet foi desenvolvida entre 1973 e 1974 na XEROX PARC (Palo Alto Research Center Incorporated) por Robert Metcalfe. A primeira variante da Ethernet foi a 10BASE5, conhecida por thick ethernet. Este padrão utilizava cabos coaxiais como um meio compartilhado de transmissão e utilizava velocidades de transmissão de 10Mbit/s, representado pelo 10 no nome. BASE significa *baseband* e 5 representa o comprimento máximo por onde um dado pode ser transmitido, que no caso significa 500 metros.

Esta tecnologia foi inicialmente desenvolvida sobre o conceito de computadores se comunicando através de mensagens broadcast por um meio compartilhado. Neste caso, quando um computador enviar um dado através do meio físico, todos os computadores conectados recebem esse dado. Existem as mensagens unicast, que são destinadas a somente um computador, e as mensagens multicast, destinadas a um grupo específico de computadores. A Figura 69 ilustra esses comportamentos.

Figura 69 - Unicast, Broadcast e Multicast



No início, as redes de computadores eram projetadas com um cabo coaxial percorrendo toda a estrutura de um prédio, ou outro estabelecimento, onde todos os computadores se conectavam a esse cabo. Porém, este tipo de topologia se tornava menos confiável a medida que mais computadores se conectavam. Um simples rompimento nesse cabo resultava na indisponibilidade total da rede. Além disso, como toda a comunicação era realizada sobre um mesmo cabo, qualquer informação enviada por um host era recebida por todos os outros, mesmo quando essa informação é destinada a somente um. Além disso, podiam ocorrer colisões quando dois hosts tentavam enviar informações ao mesmo tempo. Ao ocorrer, as informações deviam ser retransmitidas, reduzindo o throughput da rede, que é a velocidade real no qual as informações podem ser transmitidas. Para tentar evitar esse problema, existia o CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Este recurso permite verificar se o meio compartilhado está sendo utilizado, esperar a sua liberação, para iniciar a transmissão de dados. Porém, existem situações onde dois hosts verificam o meio no mesmo instante, constatarem a sua disponibilidade e iniciam a transmissão de dados simultaneamente. Neste caso, ocorre a colisão de dados, que são destruídos, e o recurso de *Collision Detection* notifica os dois hosts do ocorrido. A partir desse momento, eles iniciam um timer randômico que deve se completar para tentar enviar novamente as informações.

- *Carrier Sense*: quando uma estação transmite, o sinal é referenciado como *Carrier*. A placa de rede do host verifica a disponibilidade do meio e se estiver disponível, ela sabe que pode transmitir (*Sense*).
- *Multiple Access*: No CSMA/CD não existem prioridades atribuídas a qualquer estação em particular. Todos os hosts tem o mesmo tipo de acesso ao meio de transmissão.
- *Collision Detection*: Os hosts são alertados sobre as colisões e tentam retransmitir após um período de tempo randômico.

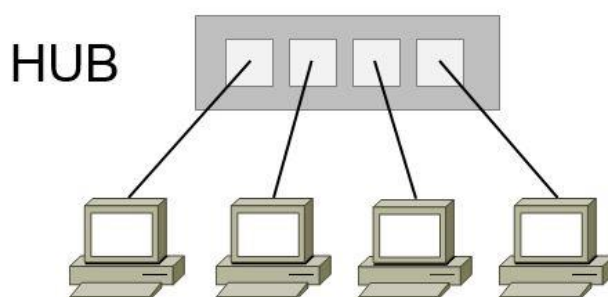
Com o passar do tempo, os cabos coaxiais foram sendo substituídos por cabos UTP (Unshielded Twisted Pair) devido as maiores velocidades e os pares trançados, que anulavam o campo magnético um do outro com o passar da corrente. Além disso, como muitas instalações já

possuíam o cabeamento de cabos trançados já prontos devido as linhas telefônicas, a adoção do UTP trouxe novas oportunidades de redução de custos e expansão das redes.

Os cabos UTP permitem conectar dispositivos a uma distância máxima de 100m. A partir dessa distância, começa a ocorrer degradação no sinal. Antigamente, para conectar dois hosts localizados a uma distância maior do que 100m, era utilizado um equipamento chamado de repetidor, que tinha como função amplificar um sinal de entrada. Este possuía duas portas: uma para entrada do sinal e outra para a saída do sinal amplificado. Dessa maneira, era possível duplicar a distância dos dois dispositivos.

Com a evolução dos equipamentos, surgiu o hub, que é simplesmente um repetidor com um maior número de portas. A sua principal vantagem sobre os repetidores é a possibilidade de amplificar o sinal recebido para mais de um dispositivo, permitindo a conexão dos hosts em topologia estrela. Este tipo de topologia traz um enorme benefício na questão da disponibilidade da rede. Por exemplo: no caso de problemas em um cabo que conecta um host ao hub, não haverá indisponibilidade total da rede, mas somente para aquele host em específico, ao contrário da topologia em barramento, que no caso de falha em qualquer parte do cabo, torna impossível a comunicação entre qualquer estação. A Figura 70 mostra a utilização de um hub em topologia estrela:

Figura 70 - Topologia em estrela com um Hub



Fonte: (Autor, 2013)

Apesar de estenderem a distância dos cabos e permitirem topologias em estrela, os hubs ainda possuem uma deficiência que impacta de forma significativa no desempenho de uma rede de computadores. Ao receber um determinado dado, o hub o envia, de forma ineficiente, para todos

os outros computadores conectados as suas portas, diminuindo drasticamente o desempenho da rede já que existe o compartilhamento da largura de banda, ainda mais que apenas um computador por vez pode enviar informações. Somado a isso, existem as colisões que podem ocorrer frequentemente e limitar drasticamente a capacidade do sistema.

Para resolver esse problema surgiram os switches, que são equipamentos que também conseguem estender a distância de cabos, porém é dotado de uma inteligência interna que o faz capaz de resolver os problemas citados acima.

A Figura 71 mostra alguns tipos de switches utilizados no mundo corporativo atualmente.

Figura 71 - Switches



Fonte: (Cisco, 2013)

Os Switches são equipamentos que atuam na camada dois do Modelo OSI, ao contrário dos repetidores e hubs que pertencem a camada um.

A seguir, são listadas as principais características dos switches, que os fazem hoje, serem amplamente utilizados em qualquer infraestrutura de rede:

- Estendem um segmento LAN para cobrir distâncias maiores;
- Possuem portas Full-Duplex (Hubs usam Half-Duplex);
- São muito rápidos e suportam portas com velocidades diferentes;

- Criam conexões virtuais, que podem ser estabelecidas simultaneamente, entre as portas que estão transmitindo e recebendo, permitindo uma conexão utilizando toda a largura de banda disponível entre um host de origem e o host de destino, não havendo compartilhamento de banda, como ocorre nos hubs;
- Eliminam as colisões, mesmo quando dois hosts enviam dados ao mesmo tempo;
- Não enviam uma determinada informação para todas as outras portas. Os Switches encaminham e filtram dados baseados no endereço MAC de cada host, fazendo com que um dado seja enviado para o destinatário correto.
- Mantém uma tabela chamada de MAC Table que associa um MAC Address a um host específico conectado ao switch;
- Fornecem uma camada extra de segurança através do recurso de Port Security, que restringe o acesso as portas do Switch, evitando que um usuário mal-intencionado se conecte a rede.
- Permite a criação de VLANs, uma separação lógica de redes que permite uma maior organização da infraestrutura de rede de uma empresa, escalabilidade e uma camada adicional de segurança para a rede.

Quando uma rede está sendo projetada, o switch é representado pelo ícone mostrado na Figura 72:

Figura 72 - Representação de um Switch em uma topologia



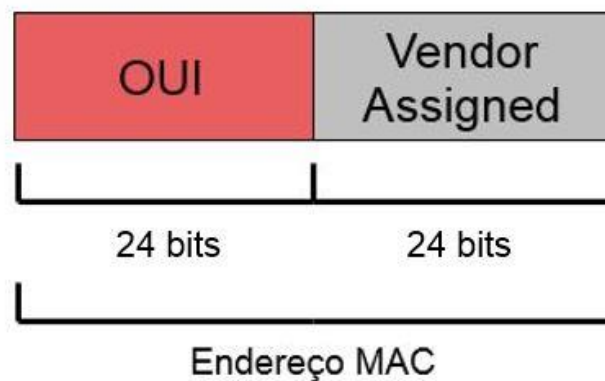
Fonte: (Cisco, 2013)

Quando um hub recebe dados provenientes de um host, ele simplesmente os envia para todos os outros hosts conectados as suas outras portas, causando uma redução drástica na performance de toda a rede, visto que enquanto um transmite, ninguém mais transmite. Um switch, quando recebe um determinado frame, como é chamado o dado quando em tratamento pela camada dois, ao invés de encaminhá-lo para todos os dispositivos conectados as suas portas, ele envia baseado no endereço MAC.

A camada de enlace fornece um esquema de endereçamento que é utilizado para transportar frames através do meio compartilhado. Este endereçamento atribuído a um dispositivo final é chamado de endereçamento físico e é único em uma rede. Em uma LAN que utiliza Ethernet, este endereço físico é chamado de endereço MAC.

Um computador que acessa uma rede deve ter uma NIC (*Network Interface Card*) que é uma placa de circuito impresso que fornece meios de comunicação em rede de um computador para uma rede e vice-versa. Cada NIC, também conhecida por adaptador LAN, possui um MAC address composto por dois componentes de 24 bits totalizando 48 bits. A *Figura 73* ilustra a composição de um endereço MAC.

Figura 73 - Composição do endereço MAC



Fonte: (Autor, 2013)

- 24 bits – OUI – *Organizational Unique Identifier*: identifica o fabricante do adaptador. A alocação dos números OUI é regulada pelo IEEE.
- 24 bits – *Vendor Assigned end-station address*: essa porção de 24 bits identifica unicamente o hardware Ethernet e é atribuída pelo próprio fabricante.

O endereço MAC identifica unicamente um dispositivo em uma rede LAN e não pode ser alterado. Ele é representado em grupos de número hexadecimais que são organizados em pares ou conjuntos de 4 dígitos, como mostram os exemplos a seguir:

- 00:00:0c:43:2e:07
- 0000:0c43:2e07

Um switch, por ser um dispositivo da camada dois, ao receber um frame, analisa o endereço MAC de destino para saber qual é o seu destino correto, ao invés de simplesmente encaminhar para todos os hosts a ele conectado. Como em uma LAN, não existem dois endereços MAC iguais, somente um host irá receber o frame. Deste modo, as mensagens *broadcast* são evitadas, melhorando a eficiência da rede minimizando tráfego desnecessário na rede. Além disso, quando diversos hosts conectados a um switch desejam enviar dados ao mesmo tempo, não existe o risco de haver colisão e também não há compartilhamento de banda, uma vez que o switch estabelece, internamente, conexões virtuais entre as portas que estão recebendo e transmitindo.

Assim, por haver uma certa “inteligência “ e uma espécie de processamento dentro do switch, ele elimina os problemas que eram encontrados em redes desenvolvidas com hubs.

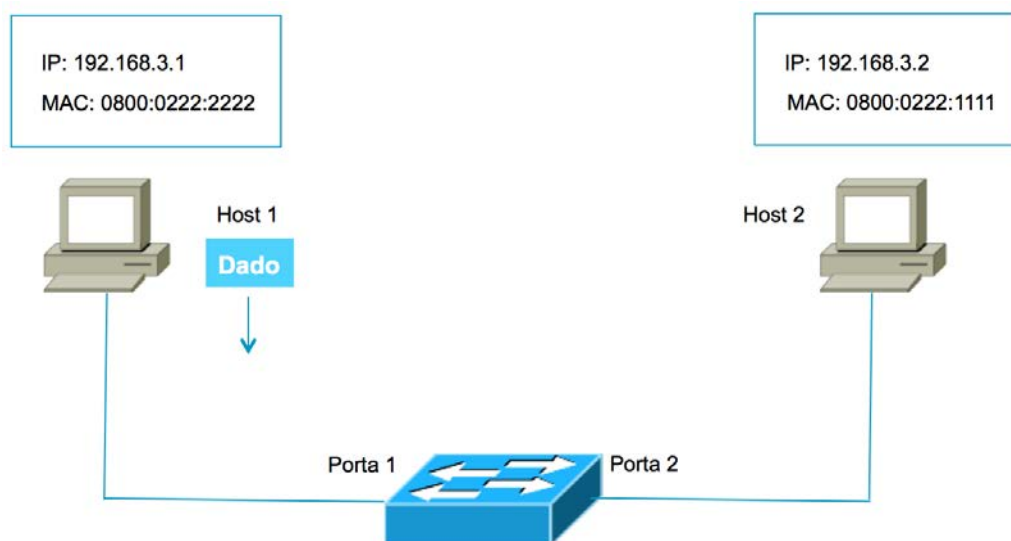
Porém, como um switch sabe quais os endereços MAC de todos os dispositivos conectados a ele? O que ocorre quando nenhum dos endereços de destino é encontrado pelo switch? O capítulo seguinte descreve de forma detalhada, empregando uma análise lógica, como uma determinada informação passa de um dispositivo a outra, passando pelo switch.

APÊNDICE A 1.5 - ENTREGA DE PACOTES HOST A HOST

A partir de agora, será explicado como um pacote trafega de um host a outro, passando pela análise do switch. Para isso, será necessário juntar e aplicar os conceitos de encapsulamento, endereçamento físico (MAC – camada dois) e endereçamento lógico (IP – camada três). Serão analisados os aspectos mais relevantes dessa comunicação, fazendo-se desnecessária a citação de alguns itens que não influenciam no cenário.

Supondo o seguinte cenário, como mostra a Figura 74, onde participam dois hosts e um switch, devidamente endereçados.

Figura 74 - Cenário de Comunicação host-to-host

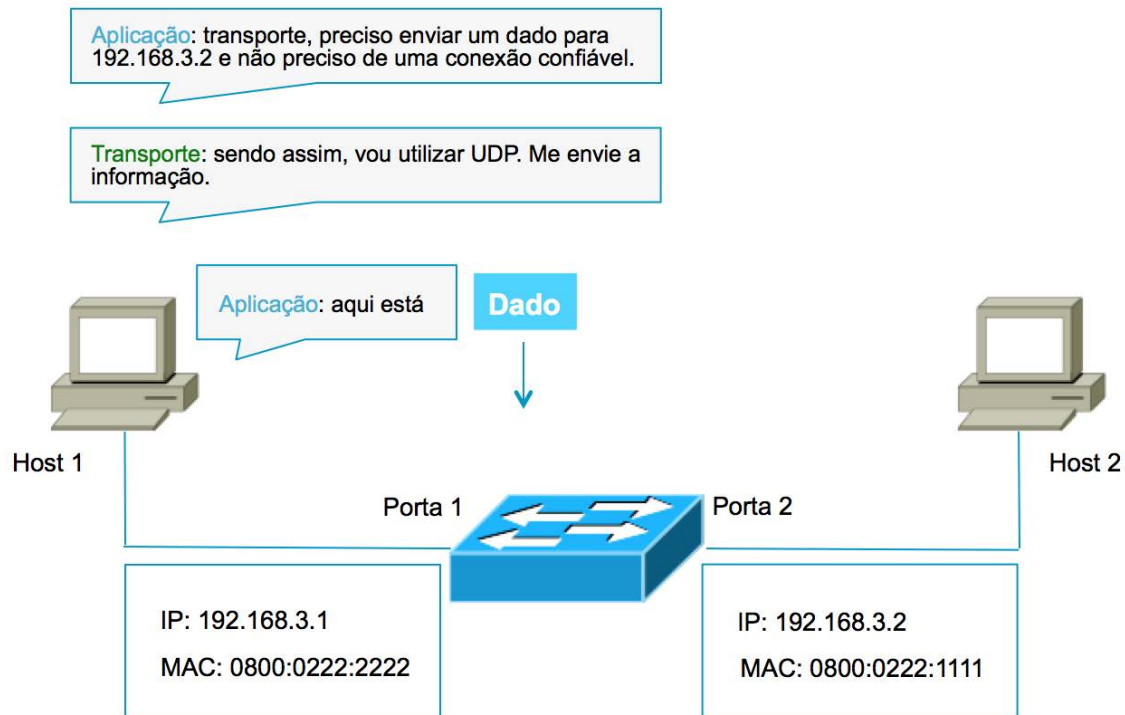


Fonte: (Autor, 2013)

Passo 1

Nesta primeira etapa, o host 1 deseja enviar uma informação para o host 2 cujo endereço IP é 192.168.3.2. Uma vez que a aplicação não necessita de uma conexão confiável, é utilizado o UDP. Assim, a camada de aplicação envia a informação para a camada de transporte que irá cuidar do resto do processo, como ilustra a Figura 75.

Figura 75 - Passo 1 da Comunicação host-to-host

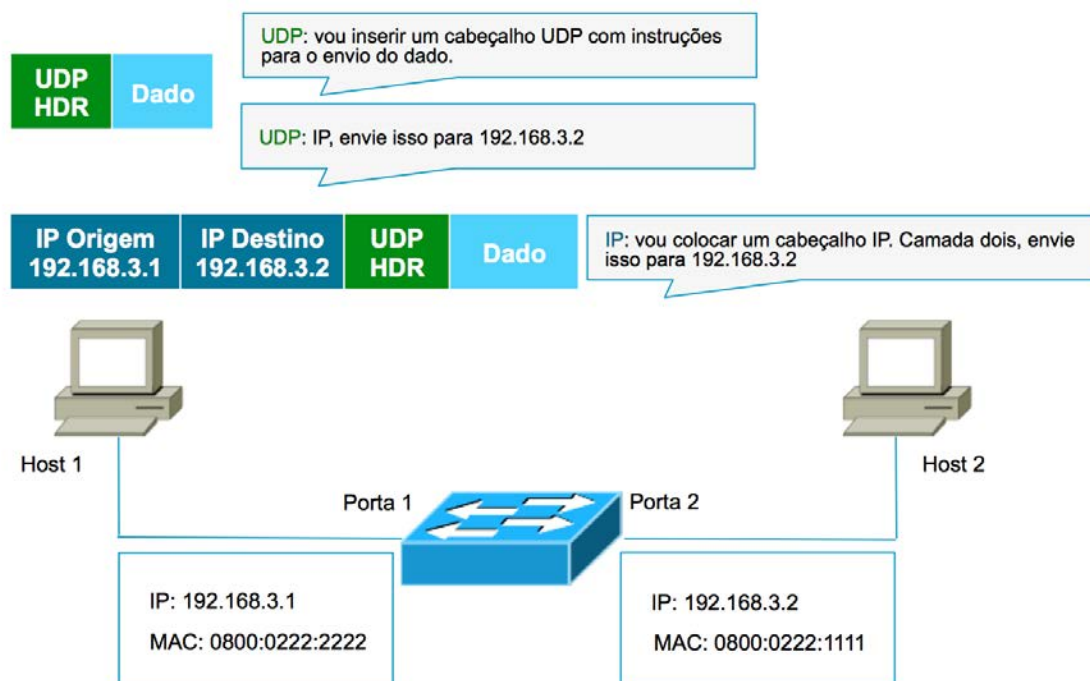


Fonte: (Autor, 2013)

Passo 2

Uma vez que não há a necessidade de estabelecer uma conexão, o UDP (camada quatro) pode começar a enviar o dado. Sendo assim, ele insere um cabeçalho UDP, com instruções para enviar para 192.168.3.2, no dado e transfere para o protocolo IP, que pertence a camada três. Da mesma maneira, o IP encapsula mais um cabeçalho e passa para a camada dois, conforme ilustra a Figura 76.

Figura 76 - Passo 2 da Comunicação host-to-host

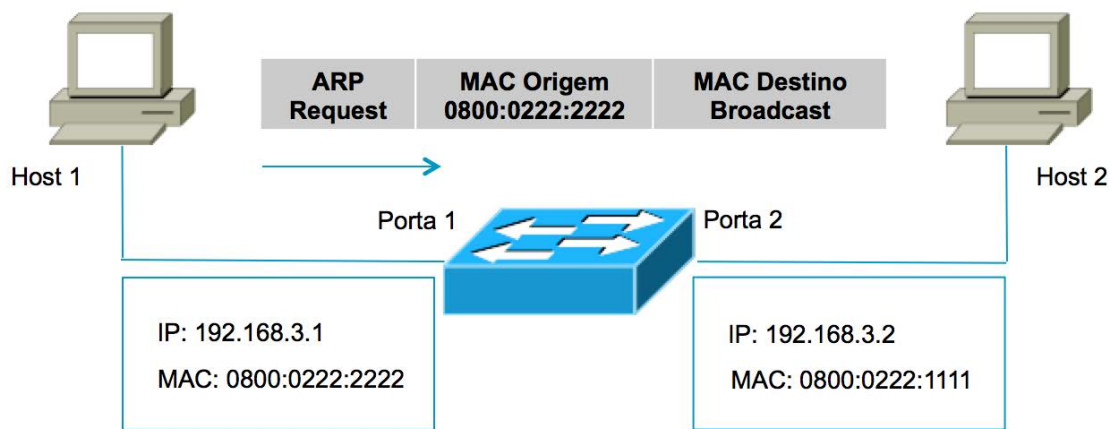


Fonte: (Autor, 2013)

Passo 3

Neste passo, ocorre um processo de extrema importância para o funcionamento das redes de computadores. Antes de o dado e seus cabeçalhos serem enviados ao switch, a camada dois deve adicionar um cabeçalho contendo as informações referentes ao endereçamento de camada dois (endereço de origem e destino), o endereço MAC. Porém, o host 1 ainda não sabe o endereço MAC do destino, o host 2. Para isso, entra em funcionamento o ARP (*Address Resolution Protocol*). Este protocolo mantém armazenado uma tabela chamada de Tabela ARP. Essa tabela guarda registros de relações IP-Endereço MAC. Ou seja, para um determinado IP, sabe-se através da tabela ARP qual é o MAC correspondente. Sendo assim, a camada dois solicita o MAC de um determinado IP para essa tabela e insere esse MAC no cabeçalho antes de enviar o frame. Porém, o que acontece quando não existe o registro do MAC para um determinado IP? Quando isso ocorre, um host envia uma requisição ARP, que nada mais é que uma mensagem broadcast, contendo o endereço MAC de origem. A Figura 77 ilustra a composição de um frame de requisição ARP, enviado pelo Host 1 para obter o endereço MAC do Host 2:

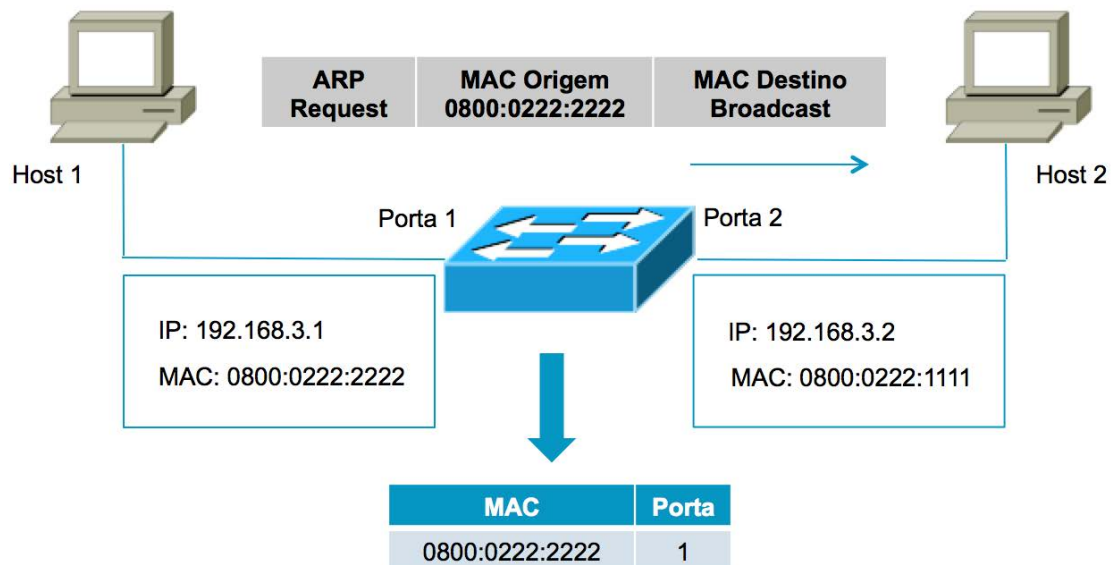
Figura 77 - ARP Request



Fonte: (Autor, 2013)

Ao chegar ao switch, por ser um broadcast, este enviará a requisição para todas as suas portas, exceto para a porta por onde chegou a requisição. Além disso, ao receber o frame, o switch já adiciona o endereço MAC do Host 1 em sua tabela de endereços MAC que associa um MAC com uma determinada porta do switch. A Figura 78 mostra esse processo:

Figura 78 - ARP Request Continuação

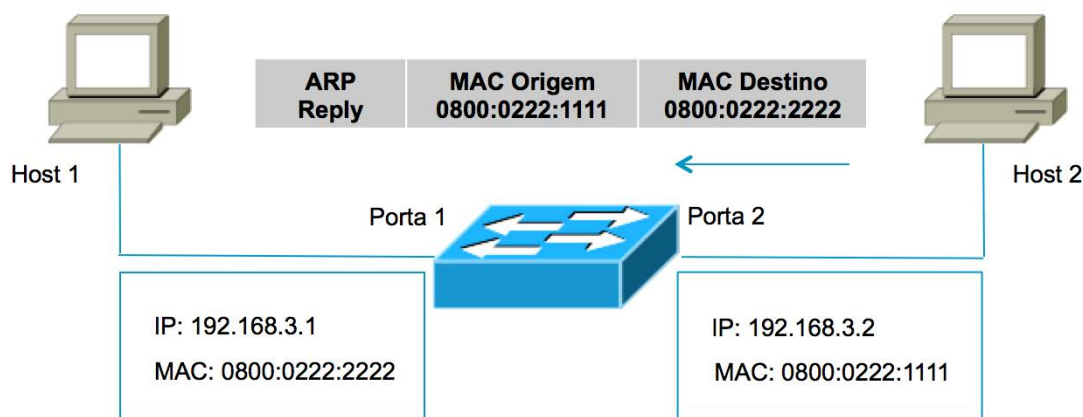


Fonte: (Autor, 2013)

Essa tabela armazenada pelo switch é utilizada quando ele já possui o endereço MAC de destino e a utiliza para saber para qual porta enviar o dado.

A requisição ARP chega então ao Host 2, que identifica a requisição e responde através de uma resposta ARP. A Figura 79 mostra o Host 2 enviando uma resposta ARP (ARP Reply):

Figura 79 - ARP Reply

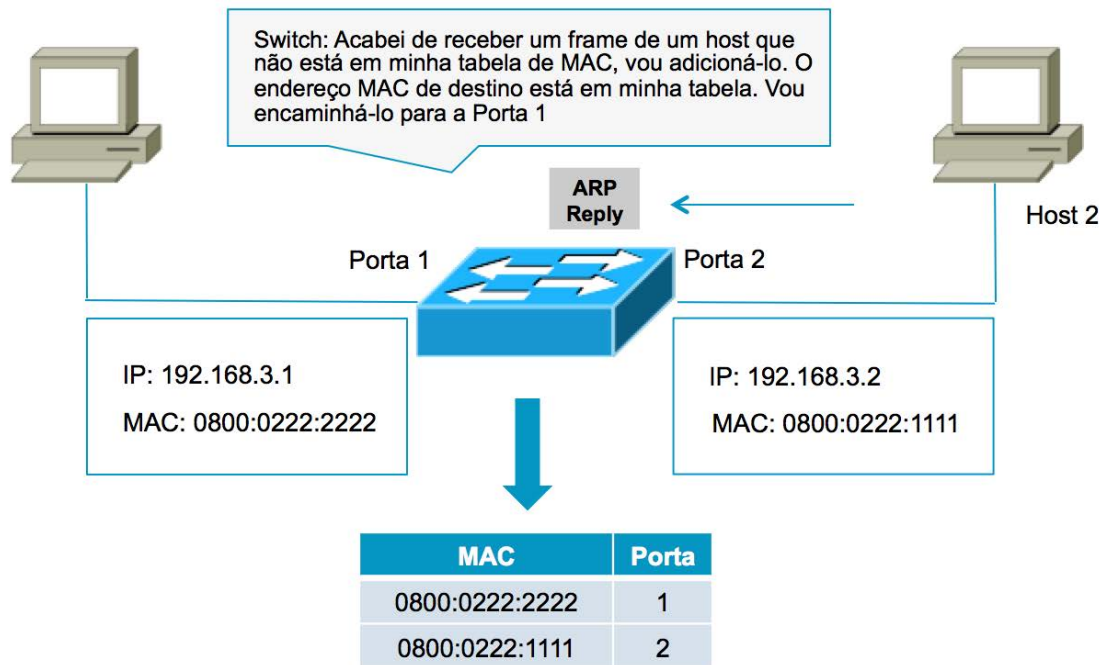


Fonte: (Autor, 2013)

É importante evidenciar que agora o MAC de origem mudou para o MAC do Host 2 e o MAC de destino para o MAC do host 1.

Agora, quando a resposta chega ao switch, ocorre algo bastante interessante. Primeiro, o switch detecta um dado vindo de sua porta 2 cujo endereço físico de origem é 0800:0222:1111. Isso faz com que o switch adicione essa entrada em sua tabela de endereços MAC para usos futuros. Além disso, ele analisa qual é o endereço MAC de destino para procurar em sua tabela de endereços e saber para qual porta encaminhar o dado. Neste exemplo, o endereço é 0800:0222:2222 (Host 1) e a porta é a Porta 1, como mostra a nova tabela de MAC do switch na Figura 80:

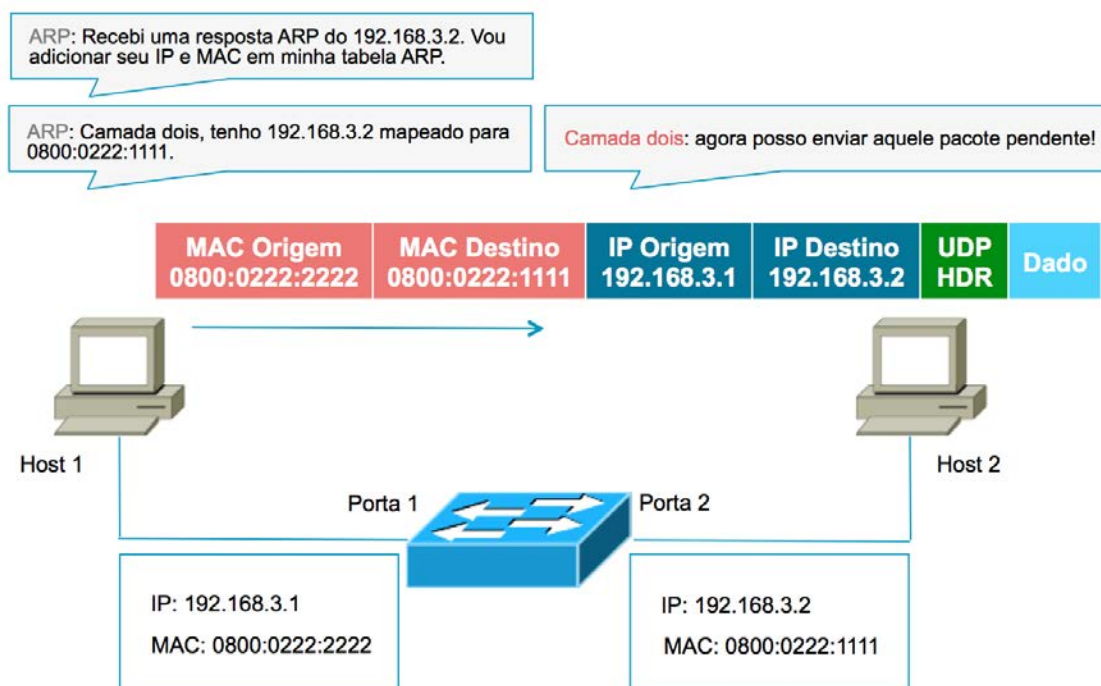
Figura 80 - ARP Reply Continuação



Fonte: (Autor, 2013)

Quando o Host 1 recebe a resposta ARP, ele salva em sua tabela ARP um registro que identifica que o IP 192.168.3.2 está mapeado para o MAC 0800:0222:1111. Agora a camada dois do Host 1 tem, finalmente, todas as informações necessárias para enviar aquele dado inicial para o Host 2, como mostra a Figura 81:

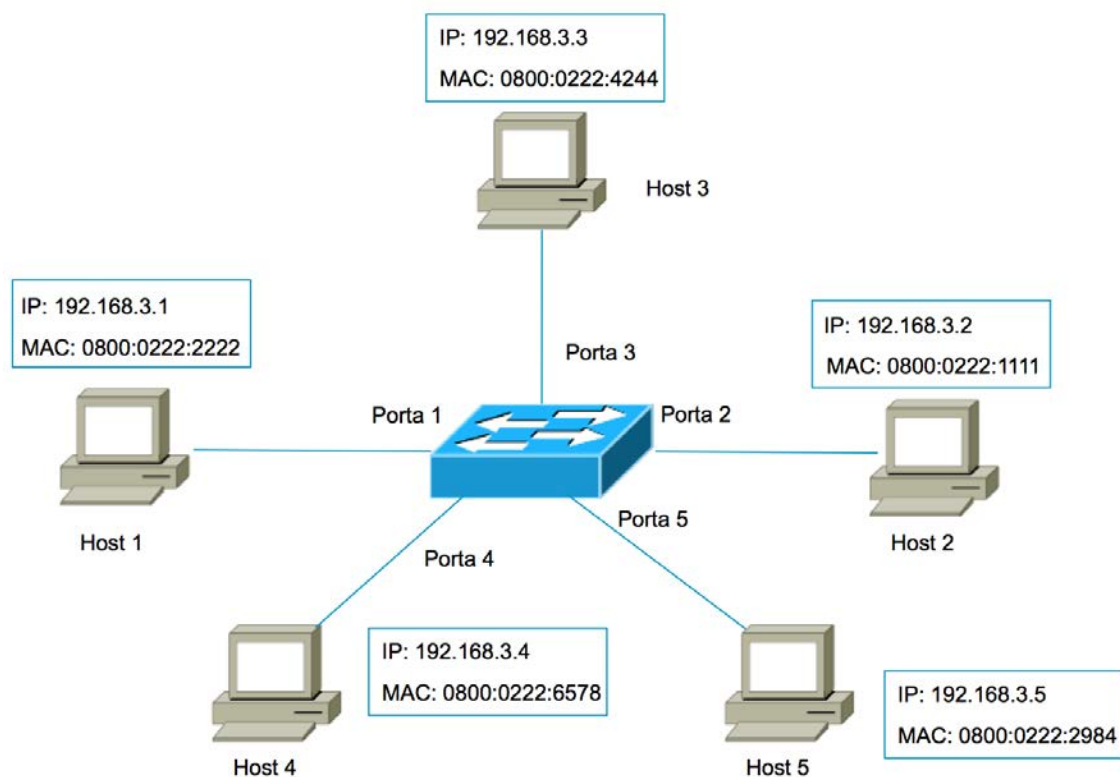
Figura 81 - Enviando o dado



Fonte: (Autor, 2013)

Através deste exemplo foi possível perceber que o switch faz a interface entre diversos equipamentos em uma mesma LAN. Dentre suas funções está o direcionamento de frames baseado no endereço MAC, evitando enviar uma determinada informação para todos os hosts desnecessariamente e aumentando a eficiência da rede. Neste exemplo foram utilizados somente dois computadores, porém um switch pode conectar diversos computadores. Existem modelos de 8, 24, 48 ou mais portas que são utilizados dependendo das necessidades de uma empresa. Essas vantagens do switch citadas acima fazem com que ele seja um dos equipamentos de redes mais utilizados hoje em dia, onde ele é, na maioria das vezes, conectado em estrela, como mostra a Figura 82:

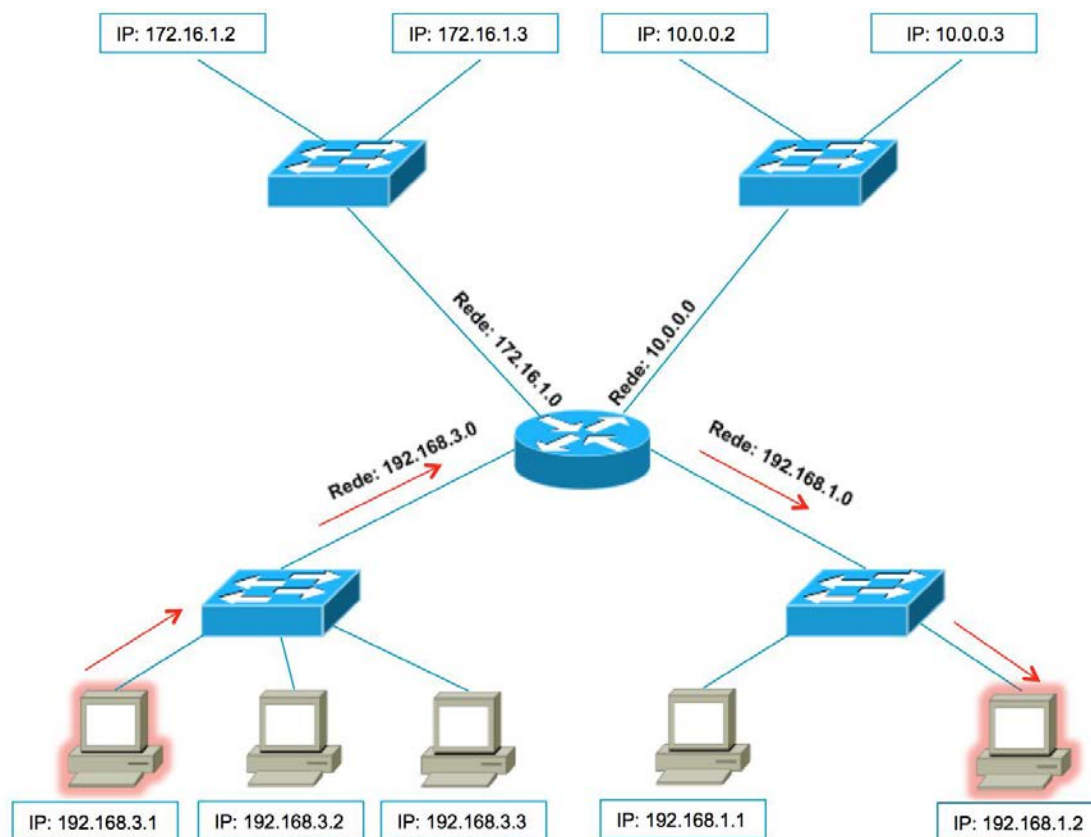
Figura 82 - Conexão em estrela com um switch



Fonte: (Autor, 2013)

E se ao invés do endereço de destino for 192.168.3.2 fosse 192.168.1.2? Sabe-se que este é um endereço IP de Classe C e por isso, os 24 primeiros bits indicam a rede. Desse modo, observa-se que o IP 192.168.3.2 pertence a rede 192.168.3.0 e o IP 192.168.1.2 pertence a rede 192.168.1.0. Assim o endereço do Host 1, que é 192.168.3.1, também situado na rede 192.168.3.0, também pertence a uma rede diferente a 192.168.1.0. Sendo assim, o Host 1 deseja enviar um pacote para um outro Host que está localizado em uma rede diferente. Pode-se imaginar uma topologia como mostra a Figura 83:

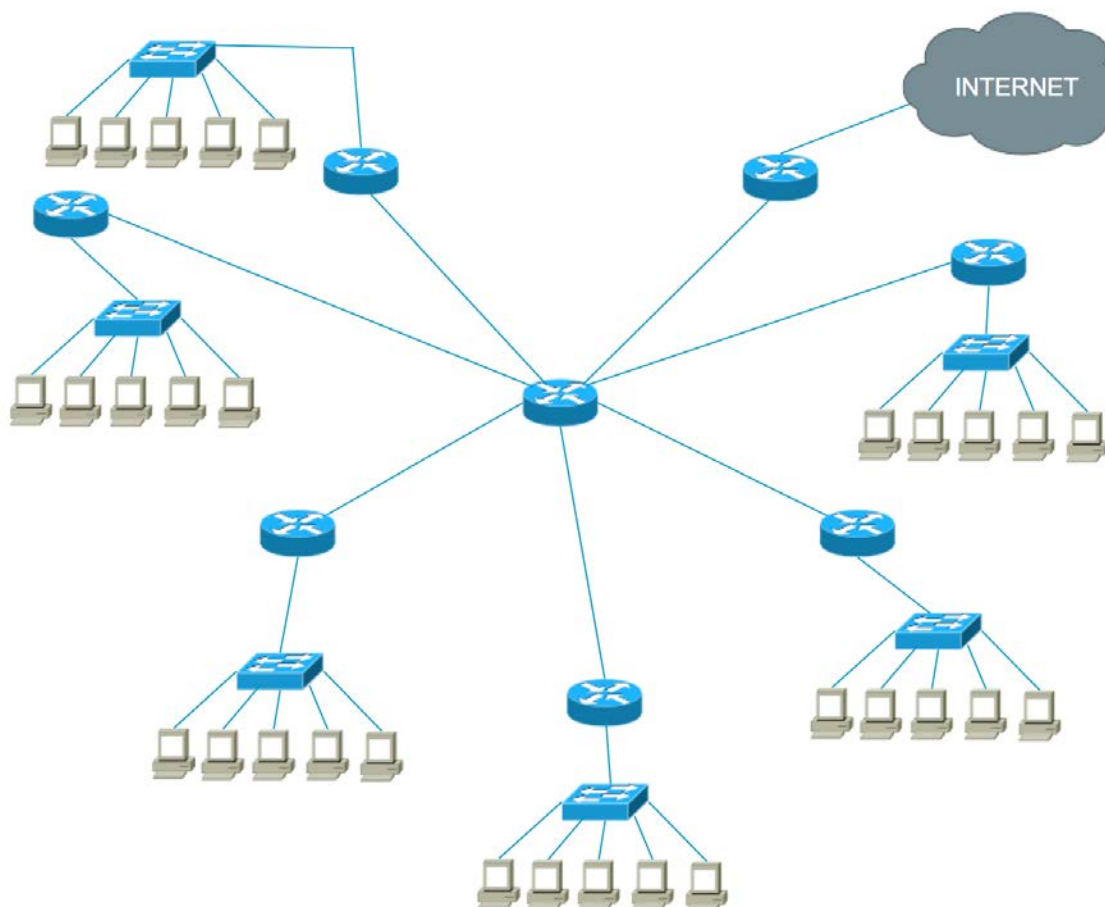
Figura 83 - Host em outra rede



Fonte: (Autor, 2013)

Quando se deseja enviar um pacote para uma rede diferente, um roteador tem que estar presente na topologia, já que é ele quem faz o roteamento de pacotes baseado em endereço IP. O roteador sabe para qual porta enviar um pacote com base em sua tabela de roteamento, que faz o mapeamento IP-Porta, assim como o switch faz o mapeamento MAC-Porta. Cada porta do roteador está conectada a uma rede diferente e cada rede possui seus switches e host. Quando o switch recebe um pacote com IP de destino pertencente a outra rede, ele envia esse pacote para um endereço IP chamado de Default Gateway. Esse endereço é utilizado por equipamentos quando se quer enviar um pacote para uma rede que não é a sua. Geralmente, o endereço Default Gateway geralmente é a de um roteador, já que é ele quem vai saber para onde mandar um determinado pacote com base no IP. Uma vez que um roteador interconecta diferentes redes, pode-se então conectar diversos roteadores entre si, como mostra a Figura 84 a seguir:

Figura 84 - Conexão com vários roteadores



Fonte: (Autor, 2013)

Cada roteador possui armazenado em sua tabela de roteamento qual é o melhor caminho para chegar a uma determinada rede. Caso não exista um caminho em sua tabela para uma determinada rede, ele o envia para o seu Default Gateway, que é algum outro roteador conectado a ele. Talvez, este saiba o melhor caminho para aquela rede, mas em caso negativo, este também direciona o pacote para o seu respectivo Default Gateway, e esse procedimento se repete até o pacote chegar a um roteador que saiba qual é o melhor caminho para chegar aquela rede.

Então, conclui-se que a internet, representada por uma nuvem no desenho anterior, nada mais é do que milhares ou até milhões de roteadores interconectados fazendo com que seja possível enviar pacotes de um lugar para o outro lado do planeta.