UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ALEX CARDOSO DE JESUS

ESTUDO DE CASO PARA INSTALAÇÃO DE *HOTSPOTS* UTILIZANDO A TECNOLOGIA *POWER OVER ETHERNET* PARA FORNECIMENTO DE ENERGIA NOS DISPOSITIVOS WIRELESS

CRICIÚMA, JULHO DE 2008

ALEX CARDOSO DE JESUS

ESTUDO DE CASO PARA INSTALAÇÃO DE HOTSPOTS UTILIZANDO A TECNOLOGIA POWER OVER ETHERNET PARA FORNECIMENTO DE ENERGIA NOS DISPOSITIVOS WIRELESS

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. Esp. Arildo Sônego

CRICIÚMA, JULHO DE 2008

ALEX CARDOSO DE JESUS

ESTUDO DE CASO PARA INSTALAÇÃO DE HOTSPOTS UTILIZANDO A TECNOLOGIA POWER OVER ETHERNET PARA FORNECIMENTO DE ENERGIA NOS DISPOSITIVOS WIRELESS

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

_____

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

_____

PROF. ESP. ARILDO SÔNEGO (UNESC)
Orientador

_____

PROF. MSC. ROGÉRIO ANTÔNIO CASAGRANDE (UNESC)

_____

ESP. ADJANO SCARMAGNANI (UNESC)

A Deus, minha Família e ao Reaja.

AGRADECIMENTOS

Como não poderia deixar de ser, quero agradecer primeiramente a Deus e seu filho Jesus por ter dado a força necessária para que fosse possível chegar ao fim desta jornada nada fácil. Eles é que foram e deram a energia quando mais precisei em vários momentos no decorrer do curso. A Eles sou muito grato.

Tenho muito que agradecer a minha família por terem me dado o incentivo para iniciar a faculdade mesmo em meio às dificuldades, terem ajudado e suportado quando precisei. Mesmo em meio às tarefas, ocupações e tempo despendido para estudar sei que estavam de alguma forma me auxiliando e torcendo para que eu seguisse adiante com a realização de um sonho. Amo a todos incondicionalmente pelo papel individual que representam em minha vida. Pai, Mãe, Irmãos, Primos, Tios e Avós, amo vocês!

Reaja, minha segunda família a quem no decorrer do curso conheci e sou muito grato a Jesus por isso. Valeu pela força, conselhos, aprendizados, vida... Talvez sem eles eu fosse chegar no mesmo lugar em que estou, mas com eles a chegada se tornou muito mais fácil e feliz. Obrigado por terem um dia aparecido em minha vida e tornado-a mais simples, alegre, colorida e com um sentido a seguir.

Os agradecimentos especiais ficam por conta das pessoas que de me ajudaram a desenvolver o trabalho de conclusão de curso. Então, primeiro, ninguém mais justo do que meu orientador Arildo, que me ajudou em todos os detalhes a fazer um trabalho no qual muito me identifiquei e aprendi. Algumas vezes com puxões de orelha, principalmente por causa dos prazos, enfim, coisas que eram necessárias e construtivas. Obrigado Arildo pelo tempo e paciência oferecidos ao projeto para que o mesmo pudesse ser concluído.

Na etapa de desenvolvimento do estudo aplicado, algumas pessoas devo citar pela importância que tiveram para conclusão do mesmo. Ao meu tio João Batista de Jesus por ter me emprestado seu PDA para efetuar os testes necessários já que eu não tinha um equipamento semelhante para efetuar esta tarefa. Rodrigo Spillere, pelo tempo disponibilizado a me ensinar. Diego Piovesan Boschetto, por fim não foi necessário que me ajudasse, mas o agradeço por sua disponibilidade em fazê-lo. As pessoas que me apresentaram o local para os estudos de caso, especialmente Adjano Scarmagnani da UNESC e Allan Pantzier da E-Mix Lan-house, pessoas estas que abriram as portas, me ensinaram e forneceram os detalhes para que eu chegasse ao fim do estudo.

Outras pessoas a quem devo prestar homenagens são aquelas que passaram os últimos nove semestres na mesma luta e deixaram sua marca na história Edroaldo, Marlon, Dirceu, Leonardo, Fernando, Aline, Diego Machado, Lucélio, Luis Juventino e José Márcio. Cada um sabe o quanto valeu e vai valer a pena tê-los conhecido e participado querendo ou não um pouco ou muito em suas vidas, sejam elas professores ou estudantes do curso de computação ou a secretária, nossa querida ‘Marga’. Valeu galera!

“...muitas pessoas sonhavam com o dia em que entrariam em um escritório e magicamente seu notebook se conectaria à Internet.” **Andrew S. Tanenbaum**

RESUMO

Este trabalho apresenta um estudo de caso para a construção de um ambiente com acesso à Internet sem fio (*Hotspot*) utilizando a tecnologia *Power Over Ethernet* (PoE) para fornecer energia para a antena *wireless* por meio do cabo de comunicação de dados. Ambas as tecnologias foram pesquisadas e aplicadas no estudo de caso realizado na empresa Useall Software. No salão de festas da empresa foi implantado *o* projeto proposto, para disponibilizar aos seus colaboradores uma alternativa para acessar a Internet, pois havia somente uma máquina para este fim. O estudo apresenta detalhes a respeito da escolha do local, da configuração dos equipamentos e dos resultados obtidos.

Palavras-Chave: Redes de Computadores, Wireless, Hotspot, Power Over Ethernet

ABSTRACT

This paper presents a case study for building an environment with wireless Internet access (Hotspot) using the technology Power Over Ethernet (PoE) to provide energy for the wireless antenna through the cable for communication of data. Both technologies have been researched and applied in the case study conducted in the company Useall Software. In the hall of festivals of the company was implanted the proposed project, to provide their employees an alternative to access the Internet, since there were only a machine for this purpose. The study presents details about the choice of location, the configuration of equipment and results.

Key-Words: Computer Networks, Wireless, Hotspot, Power Over Ethernet

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encription Standard
ANS	Advanced Network and Services
AP	Access Point
ARPANET	Advanced Research Projects Agency Network
BSS	Basic Service Set
CRC-32	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA-CD	Carrier Sense Multiple Access With Collision Detection
DCF	Distributed Coordination Function
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
Gbps	Gigabit por segundo
GHz	Gigahertz
HR-DSSS	High Rate Direct Sequence Spread Spectrum
HTTP	HyperText Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization

Kbps	Kilobit por segundo
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
MAN	Metropolitan Area Network
Mbps	Megabit por segundo
MHz	Megahertz
NAV	Network Allocatiom Vector
OFDM	Orthogonal Frequency Division Modulation Method
PCF	Point Coordination Function
PD	Power Device
PDA	Personal Digital Assistant
PoE	Power Over Ethernet
POS	Point Of Sale
PSE	Power Sourcing Equipment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Route Coloniale 4
RM-OSI	Open Systems Interconnection Reference Model
RNP	Rede Nacional de Pesquisa
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Securitty

UDP	User Datagram Protocol
UNESC	Universidade do Extremo Sul Catarinense
V	Volts
VoIP	Voice over Internet Protocol
VPN	Rede Privada Virtual
W	Watts
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WPA	Wi-fi Protected Access
WPA2	Wi-fi Protected Access 2

SUMÁRIO

1 INTRODUÇÃO

As redes de computadores são utilizadas em locais distintos, como por exemplo, em ambientes comerciais, domésticos, instituições de ensino, entre outros e têm como objetivo interligar os componentes pertencentes a ela. Desta forma, muitas técnicas relacionadas à conectividade foram desenvolvidas para que de alguma forma algum processo ou serviço oferecido fosse aprimorado trazendo algum benefício. Este trabalho irá discorrer sobre duas destas técnicas, são elas: as Redes *Wireless* e a tecnologia *Power Over Ethernet* (PoE).

A Rede *Wireless* é uma forma de tornar a interligação dos computadores algo mais flexível por meio da mobilidade, pois não são utilizados fios para conectar os computadores, mas sim um dispositivo no computador e outro chamado de ponto de acesso, que irá fornecer a permissão e acesso deles na rede. Serão apresentadas características como padrões, segurança, métodos de acesso entre outros detalhes específicos desta tecnologia.

O *Power Over Ethernet* trata-se de uma tecnologia onde utiliza apenas um cabo para trafegar dados e energia. Ela faz o uso do cabo par-trançado que é o mais usado nas redes atuais. Serão apresentados os dispositivos PoE, seu funcionamento, arquitetura, vantagens e desvantagens, entre outros detalhes relacionados a ele.

A utilização dos ambientes *wi-fi* para conexão à Internet, chamados também de *Hotspot*, onde encontrá-los e qual a situação atual deste serviço no Brasil e no mundo estão descritos no trabalho juntamente com o objetivo prático de utilizá-lo em união com o PoE.

1.1 OBJETIVO GERAL

Realizar um estudo de caso para a instalação de um *hotspot* utilizando a tecnologia *power over ethernet* para fornecer energia para as antenas *wireless*. A aplicação será realizada em uma empresa de Criciúma.

1.2 OBJETIVOS ESPECÍFICOS

a) pesquisar conceitos relativos à redes de computadores;
b) conhecer a tecnologia *Power Over E*thernet e seus equipamentos;
c) pesquisar os padrões de redes sem fio 802.11a, 802.11b, 802.11g;
d) instalar um *Hotspot* baseado na tecnologia PoE;
e) demonstrar vantagens e desvantagens da rede *wireless* e PoE;
f) analisar o custo e viabilidade.

1.3 JUSTIFICATIVA

Na área de redes de computadores foi desenvolvida a tecnologia *Power Over Ethernet*, cujo objetivo é transmitir energia por meio do cabo par-trançado juntamente com os dados. Deste modo, há uma redução no volume de cabos e de gastos em geral com a instalação elétrica. Por enquanto a tensão máxima fornecida pelo PoE é de 48V, por isso, nem todos os equipamentos podem ser alimentados por ele. Dentre os quais apresentam esta possibilidade pode-se citar a antena *wireless* que é utilizada para prover sinal de internet por meio do ar.

Tradicionalmente os computadores são conectados na rede por meio de um cabo para acessarem a *web*, mas a antena *wireless* que também é conhecida como *access point*, possui a vantagem de não utilizar este meio, tornando assim, o fator mobilidade seu ponto forte.

O *wireless* é uma boa opção, pois em qualquer área com sinal de internet disponível é possível conectar-se, sendo que atualmente ela é indispensável no cotidiano de muitas pessoas. Estes locais são conhecidos como *Hotspot* e são construídos em locais públicos como aeroportos, *cyber-cafés*, *shoppings*, entre outros, tornando-os um atrativo para as pessoas que estão muitas vezes de passagem rápida ou que procuram estes lugares devido a sua comodidade (GREGO, 2006).

A união das duas tecnologias irá resolver um problema que ocorre na Useall Software, uma empresa situada em Criciúma, onde o salão de festas que é utilizado também para palestras, reuniões com os clientes, demonstrações dos produtos e nos horários de folga durante o expediente os colaboradores que têm notebook se reúnem e aproveitam o tempo para entretenimento.

Este local fica na cobertura do prédio e não há nenhum ponto de rede, por isso será utilizada a tecnologia *Power Over Ethernet* e um ponto de acesso que forneça acesso à internet e à rede local como solução para os problemas ocasionados pelos itens supracitados referentes ao salão de festas.

1.4 ESTRUTURA DO TRABALHO

Tendo em vista os objetivos deste trabalho de pesquisa, os objetos de estudo durante a elaboração estão descritos em oito capítulos, já incluso introdução, o trabalho

e a conclusão. Os objetos de pesquisa são: Redes de Computadores, Wireless Fidelity, Power Over Ethernet e Hotspot. Por fim são realizados alguns estudos de caso teórico e práticos utilizando estas tecnologias em conjunto.

As Redes de Computadores são estudadas no Capítulo 02. Nele são abordadas as topologias, o protocolo de rede, as principais arquiteturas e apresentado os padrões do IEEE que serão estudados a seguir.

O Wireless Fidelity está presente no Capítulo 03, nele pode-se encontrar um breve histórico de sua origem, os principais padrões e mais utilizados, topologias, as frequências na qual opera e técnicas de transmissão, protocolos e pelo fato de ser um padrão que utiliza o ar para trafegar os dados é discutido suscintamente sobre alguns padrões de segurança.

No Capítulo 04 é descrito sobre a tecnologia Power Over Ethernet, onde é possível encontrar sobre o seu funcionamento, objetivos, equipamentos, vantagem e desvantagem e quando utilizá-la.

Para complementar o assunto sobre Wireless Fidelity, no Capítulo 05 é descrito sobre *Hotspot*, locais com acesso à Internet sem fio. Trabalhos correlatos são apresentados no Capítulo 06 e por fim no Capítulo 07 é apresentado o estudo de caso teórico e prático. No Capítulo seguinte é descrito por fim, a conclusão do estudo realizado e em seguida as referências utilizadas.

2 REDES DE COMPUTADORES

Segundo Hayden (1999) as redes estão por toda parte. Ao comprar um carro novo em uma concessionária, utilizar os correios ou até mesmo ao ligar a televisão, de alguma forma está sendo utilizada uma rede. No momento em que um cartão de crédito é utilizado, uma chamada telefônica é realizada ou se a Internet for acessada, estará sendo utilizada uma rede de computadores.

Uma rede de computadores é um conjunto de módulos processadores que se conectam entre si por meio de um sistema de comunicação, cujo objetivo é trocar informações e compartilhar recursos (SOARES; LEMOS; COLCHER, 1995). Um exemplo disso está presente na Figura 1.

O sistema de comunicação trata de como os computadores estão dispostos em rede (topologia), quais os meios físicos que serão utilizados para que eles se comuniquem e quais as regras utilizadas para que a comunicação seja organizada (TANENBAUM, 2003).

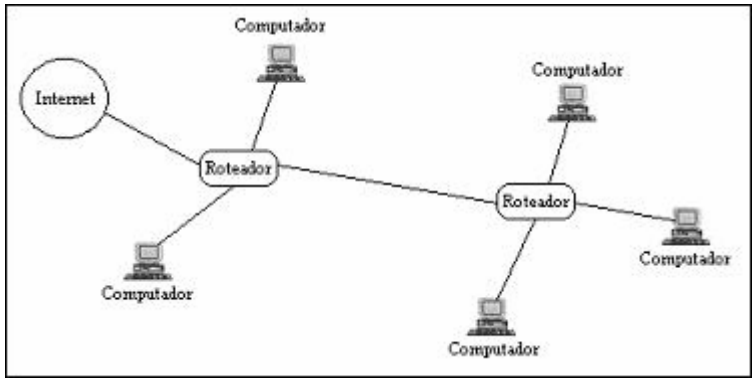

Figura 1. Exemplo de uma rede de computadores
Fonte: Adaptado de LIMA JÚNIOR, A. (2002)

2.1 TOPOLOGIAS

Como já explicado anteriormente, dependendo de como os computadores estão interligados, eles formam um tipo de topologia. De acordo com Soares, Lemos e Colcher (1995) algumas topologias utilizadas em redes são:

a) **estrela**: Todos os computadores são ligados em um outro computador central, por onde todas as mensagens devem passar. Há um exemplo na Figura 2. Ele é quem controla a rede, pois é por meio dele que todos os outros se comunicam entre si (ZACKER; DOYLE, 2000);

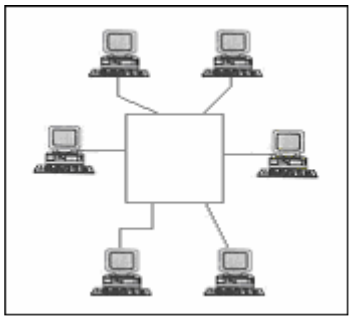

Figura 2. Topologia em estrela
Fonte: SOARES, L.; LEMOS, G.; COLCHER, S. (1995)

b) **anel**: Os computadores estão conectados por meio de um caminho fechado, dando a idéia de um anel, conforme a Figura 3. A informação é lançada no meio físico e transmitida de forma seqüencial até que chegue ao seu destino (SOARES; LEMOS; COLCHER, 1995);

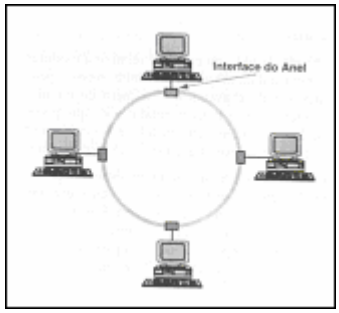

Figura 3. Topologia em anel
Fonte: SOARES, L.; LEMOS, G.; COLCHER, S. (1995)

c) **barra**: Na Figura 4 pode-se verificar que os computadores têm em comum o mesmo meio físico de transmissão das mensagens (TANENBAUM, 2003).

Figura 4. Topologia em barra
Fonte: SOARES, L.; LEMOS, G.; COLCHER, S. (1995)

Algumas características como topologia, tamanho, meios de transmissão, entre outros, influenciam diretamente na classificação do tipo a qual a rede pertence, que pode ser uma *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) e *Wide Area Network* (WAN), que serão analisados no próximo tópico (TANENBAUM, 2003).

2.2 ABRANGÊNCIA

Segundo Tanenbaum (2003) as redes locais, também conhecidas como LAN's, normalmente são de propriedade privada que se encontram em um espaço físico fechado como o de um prédio ou de um campus cuja extensão é pequena. Este tipo de rede é utilizado em larga escala para conectar computadores em locais como escritórios, indústrias, universidades, cujo objetivo é rapidez na troca de informações e compartilhamento de recursos disponíveis. Outros pontos que se pode ressaltar são as baixas taxas de erro, podem ser construídas utilizando qualquer topologia e a alta taxa de transmissão de dados que tradicionalmente é de 10 a 100Mbps, mas nas mais atuais pode chegar até a 10Gbps. Uma rede um pouco maior são as redes metropolitanas ou

MAN’s.

As MAN’s são semelhantes as LAN’s, a diferença básica entre elas é a distância na qual podem transferir as informações entre os computadores. Como o próprio nome diz, metropolitana, abrange a área de uma cidade sendo sua velocidade superior a de uma LAN (SOARES; LEMOS; COLCHER, 1995).

Ainda relacionado à abrangência das redes, há a rede geograficamente distribuída ou WAN. Neste tipo, os computadores estão ligados a uma sub-rede (formada por linhas de comunicação e equipamentos que gerenciam o tráfego de informações) que normalmente é de propriedade de alguma companhia telefônica ou provedor de serviços da Internet, que são os responsáveis por transmitir os dados entre eles (TANENBAUM, 2003).

2.3 PROTOCOLO DE REDE

Segundo Thomas (1997) os protocolos de rede, podem ser comparados com a comunicação entre os seres humanos por meio da fala. Isto porque, para um entender o outro, é necessário ser capaz de atender a alguns requisitos, sendo que o essencial deles é que conversem no mesmo idioma. Assim como os humanos, os computadores têm que obedecer a um conjunto de padrões e regras (protocolo de rede), para que possam se comunicar entre si.

Considerando então as informações anteriores, pode-se concluir que todo computador precisa de um protocolo de comunicação para conectar-se à rede (ZACKER; DOYLE, 2000). Como exemplo de protocolo pode-se citar o TCP/IP, que será comentado no item 2.5.

2.4 MODELO RM-OSI

O modelo RM-OSI foi criado nos anos 80 pelo grupo *International Standards Organization* (ISO), com o objetivo de padronizar os protocolos existentes entre as camadas que o compõe. O modelo é constituído por sete camadas, as quais são explicadas a seguir (TANENBAUM, 2003):

a) **camada física**: É o meio de comunicação no qual trafegam os *bits* de um computador para o outro. Deve constar no projeto deste protocolo como realizar o reconhecimento do bit 1 e do bit 0, se a transmissão desses sinais será *half* ou *full-duplex*[1], como é iniciada e encerrada a conexão e outros detalhes elétricos e mecânicos (SOARES; LEMOS; COLCHER, 1995);

b) **camada de enlace**: Recebe os *bits* da camada física em quadros, isto é, uma parte da cadeia de *bits* e verifica se há algum erro, não necessariamente efetuará a sua correção. Normalmente, neste nível são utilizado *bits* de redundância nos quadros enviados para a detecção de erros, mas não para corrigi-los. Outra função é garantir que o transmissor não enviará mais dados que o receptor pode processar (TORRES, 2001);

c) **camada de rede**: É a responsável por definir as rotas que os pacotes devem seguir da sua origem até o destino, serviço este que é semelhante ao dos correios, onde são fornecidas algumas informações

[1] Half Duplex permite a transmissão em dois sentidos, mas apenas um de cada vez e a Full Duplex permite a transmissão em dois sentidos simultaneamente (COMER; STEVENS, 1999).

na correspondência que garantirão a sua entrega no local certo (HAYDEN, 1999);

d) **camada de transporte**: A entrega confiável dos pacotes é realizado nesta camada. Ela irá notificar qualquer erro na transmissão dos pacotes para a camada emitente solicitando assim um novo pacote, desta forma corrigindo o erro. Há basicamente duas formas de transmissão, uma garantirá que os pacotes cheguem em ordem, já a outra não irá garantir que todos os pacotes cheguem na mesma ordem, mas a taxa de erros é considerada baixa e por isso ignorada na prática (TANENBAUM, 2003);

e) **camada de sessão**: Usuários de diferentes computadores estabelecem uma sessão para a transferência de dados. Esta camada disponibiliza os serviços que permitem saber quem detém a permissão para enviar algo, impede que sejam executadas operações críticas iguais ao mesmo tempo e a sincronização que inicia a sessão do ponto em que foi interrompida. Esta interrupção pode ter sido planejada ou não (TORRES, 2001);

f) **camada de apresentação**: Para melhor compreender, Hayden (1999) exemplifica esta camada como alguém que traduz um texto antes de ser enviado e compreendido posteriormente do outro lado. Os serviços oferecidos por esta camada são a seleção de sintaxes e estabelecimentos, transformação e formatação de dados e manutenção de conexões de apresentação (SOARES; LEMOS; COLCHER, 1995);

g) **camada de aplicação**: O próprio nome já o define, isto é, são os

aplicativos utilizados para acessar e transferir arquivos como o navegador, programa para envio de e-mail's, entre outros. Esta camada é quem fornece a comunicação entre os aplicativos e o modelo de comunicação RM-OSI (SOARES; LEMOS; COLCHER, 1995).

Figura 5. Modelo RM-OSI
Fonte: MURHAMMER, M. et. Al, (2000)

O modelo presente na Figura 5 é bem divido e alcança o objetivo de modo satisfatório, embora não tenha sido implementado como protocolo de rede (HAYDEN, 2001).

2.5 ARQUITETURA TCP/IP

Quando foram criadas as redes de rádio e satélite, haviam alguns problemas com os protocolos existentes. Para resolver isto, em meados dos anos setenta desenvolveu-se o protocolo TCP/IP. Tem como uma das principais metas a interconexão de computadores pertencentes à rede diferentes. Ele foi dividido em quatro camadas, que podem ser visualizadas na Figura 6 (TANENBAUM, 2003):

Figura 6. Modelo TCP/IP
Fonte: MURHAMMER, M. et. Al, (2000)

a) a **camada de aplicação** é responsável por comunicar os aplicativos com a camada inferior, neste caso a de transporte. Alguns serviços oferecidos nesta camada são o SMTP, HTTP, FTP entre outros. A conexão para que ocorra este serviço, é por meio de portas. As portas são números padrões para cada aplicativo padrão. Deste modo, o protocolo sabe que tipo de dado está sendo enviado, e no destino ele sabe para qual protocolo de aplicação enviar a informação (TORRES, 2001);

b) a **camada de transporte** tem a função de dividir os dados da aplicação em pacotes a serem entregues para a camada de inter-rede. Quando o pacote é recebido, é ele quem faz a reorganização, pois eles podem chegar na ordem diferente de quando saíram. Se estiver faltando algum é feita uma solicitação de reenvio do pacote. Este é o primeiro protocolo o TCP. O *User Datagram Protocol* (UDP) é o segundo protocolo, sendo que este não verifica se o pacote chegou ou não no destino (TORRES, 2001);

c) a **camada de inter-rede** deve fazer com que os pacotes recebidos sejam inseridos em qualquer rede e trafegarão até que chegue no seu

destino. O protocolo mais utilizado nesta camada é o IP, que define o tipo de pacote. Estes são entregues ao destino por meio do roteamento, que é uma função específica desta camada, sendo que ela deve também evitar o tráfego intensivo (TANENBAUM, 2003);

d) não importa qual a rede utilizada para formar a inter-rede, contanto que a sua interface compreenda o datagrama[2] IP para trafegá-lo (SOARES, LEMOS E COLCHER, 1995).

2.6 IEEE 802

Em 1980, foi criado um grupo no IEEE que ficou responsável de estudar e criar um padrão para as redes locais. Este é o padrão IEEE 802 que inicialmente era somente usado nos Estados Unidos, mas em seguida foi revisto e publicado novamente, desta vez pela ISO, e considerado um padrão internacional (SOARES; LEMOS; COLCHER, 1995).

O IEEE 802 foi dividido em três camadas, sendo que ao compará-lo com o modelo RM-OSI, ele se refere às camadas Física e de Enlace. A Figura 7 mostra a relação entre eles:

[2] Pacote de informação contendo os dados que trafegam pela rede.

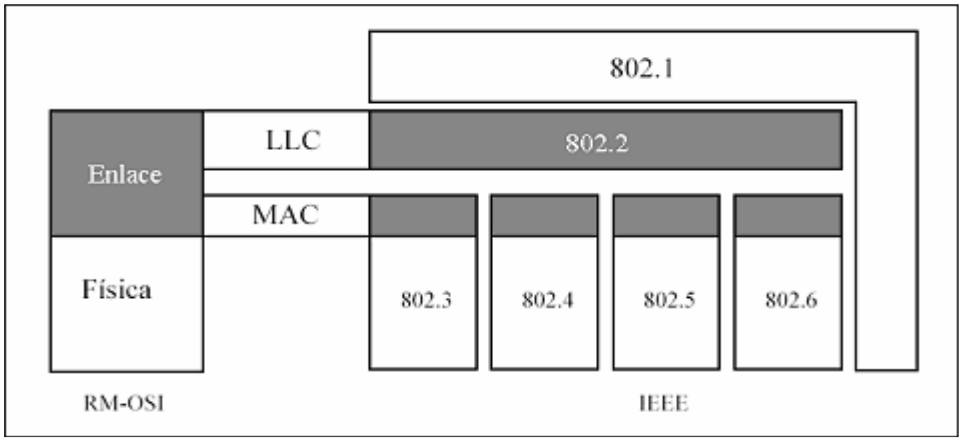

Figura 7. Relação entre RM-OSI e IEEE 802
Fonte: SOARES, L.; LEMOS, G.; COLCHER, S. (1995)

A primeira camada trata-se do IEEE 802.1, que nada mais é do que um documento criado com o objetivo de fazer uma relação entre os padrões 802, bem como o deles com o modelo de referência RM-OSI. A segunda camada, isto é, IEEE 802.2 é descrito sobre o nível superior da camada de enlace, que se refere ao protocolo *Logical Link Control* (LLC). Na terceira e última camada, são as diversas opções de nível físico e protocolos da camada inferior do *Medium Access Control* (MAC). Abaixo destes níveis encontram-se as funções utilizadas na camada Física (SOARES; LEMOS; COLCHER, 1995).

Para a realização deste trabalho, o foco desta pesquisa são os padrões da terceira camada 802.11 e 802.3af, que serão discutidos mais detalhadamente nos capítulos a seguir.

2.7 IEEE 802.3

O estudo deste padrão iniciou-se no ano de 1976 com os pesquisadores Metcalfe e Boggs no centro de pesquisas da Xerox. O seu objetivo é interligar os computadores pessoais – invenção naquela época recente e originalmente também da

Xerox – por meio de um único cabo (SPURGEON, 2000).

A utilização do cabo permitiu que fosse criado o método *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD), isto é, o computador verifica se há alguém transmitindo informação na rede, se houver, ele espera até que o meio fique livre para poder enviar informação. Caso ocorra alguma colisão, isto é, dois computadores enviarem informações ao mesmo tempo, eles esperarão um tempo aleatório, que se tornará exponencial caso ocorra outras vezes para o envio dos dados (LIMA JÚNIOR, 2002).

A velocidade inicial deste sistema era de 2,94Mbps por meio do cabo coaxial grosso. Posteriormente foi aprimorado por outras empresas e finalmente padronizado pelo IEEE na década de 80. Atualmente sua velocidade opera na casa dos gigabits e os cabos que podem ser utilizados são o coaxial fino, par-trançado e fibra óptica (TANENBAUM, 2003). Este trabalho destina-se ao uso do cabo par-trançado pelo fato da tecnologia *Power Over Ethernet* (PoE), que será abordada em detalhes no Capítulo 4, ter sido implementada utilizando-o como meio de transmissão.

2.8 IEEE 802.11

Segundo Rufino (2005) este padrão foi criado e desenvolvido pelo IEEE, que o apresentou no ano de 1997. Ele deveria fazer com que os computadores se interconectassem por meio do ar e não mais utilizando a estrutura física de cabos. Suas características principais são a velocidade de no máximo 2Mbps, que se for comparada com as atuais é muito baixa, a utilização da freqüência na faixa de 2,4GHz, o modo de operação em que irá estabelecer conexão, que pode ser ponto-a-ponto ou infra-estrutura

e o protocolo de segurança *Wired Equivalent Privacy* (WEP).

Os aspectos que serão pesquisados neste trabalho com mais detalhes no próximo Capítulo são as derivações deste padrão e suas particularidades, as topologias, freqüências e protocolos disponíveis, assim como os principais métodos de segurança existente para este tipo de rede.

2.9 INTERNET

No inicio dos anos 60, a Guerra Fria entre os Estados Unidos e a União Soviética estava atingindo o seu clímax. Em meio à guerra, inicia-se nos centros militares de pesquisa norte-americanos uma forma de conectar seus computadores, de modo que se algum deles fosse desligado ou destruído, os demais continuariam operando. Esta rede foi denominada de *Advanced Research Projects Agency Network* (ARPANET), que posteriormente deu origem à Internet (ERCÍLIA, 2000).

Na década de 70 é desenvolvido o TCP/IP, que hoje é o principal protocolo utilizado na Internet. No ano de 1980 a até então ARPANET se une com outros centros de pesquisa. No inicio dos anos 90 a *Advanced Network and Services* (ANS) desenvolve o principal *backbone* (espinha-dorsal) da Internet e em paralelo desenvolvia-se outro na Europa (CYCLADES, 1997).

Segundo Vieira (2003) o primeiro contato com a Internet no Brasil foi no ano de 1988, quando dois professores da Universidade de São Paulo fizeram uma conexão com um centro de pesquisa nos Estados Unidos. Em 1992, o governo brasileiro cria a Rede Nacional de Pesquisa (RNP) que se torna o responsável por criar um *backbone* para receber a conexão internacional.

A princípio a conexão foi liberada para universidades, centros de pesquisa e órgãos do governo que se encontraram distribuídos pelo país (VIEIRA, 2003). Guizzo (2002) complementa que a Internet no Brasil decolou realmente no ano de 1996. Ano em que os serviços oferecidos melhoraram e o numero de usuários e provedores aumentaram.

Guizzo (2002) explica que é impossível descrever todas as operações que podem ser realizadas por meio da Internet. Ele salienta que ela é um canal por onde pode-se disseminar informação, oferecer serviços e entretenimento sendo que ela traz novas formas de trabalho e comunicação.

Com base nisto, pode-se concluir que ela tem uma influência e implicações consideráveis na pesquisa, transações relacionadas ao comércio, entretenimento, trabalho, entre outros campos que podem de alguma maneira se beneficiar com o seu uso.

Com o passar dos anos a internet se tornou cada vez mais utilizada e necessária no cotidiano tanto de pessoas quanto para fins empresariais. É possível conectar-se à ela por meio do ar, bastando que se tenha os equipamentos necessários e permissão para acessá-la. Esta forma de conectar-se à rede rede mundial dos computadores é conhecida também como *Hotspot*, muito utilizado em restaurantes, shopping, hotéis, entre outros que serão vistos com mais detalhes no Capítulo 5 que trata especificamente desta modalidade.

3 WIRELESS FIDELITY

Com a evolução da informática e a utilização dos notebooks no início dos anos 90, seria mais fácil para os usuários destes aparelhos se chegassem em seus locais de trabalho ou em qualquer outro local e pudessem integrar seus computadores à rede sem ter de conectá-los por meio de algum cabo. Com este objetivo, muitos fabricantes desenvolveram um meio de fazer com que estes aparelhos se estabelecessem na rede utilizando alguns transmissores e receptores que trocassem informações pelo ar, por meio de ondas de rádio (GRÜNEWALD, 2005).

O problema é que esta tecnologia não era padrão. Deste modo um computador conectado em uma empresa poderia não se conectar em um campus de alguma universidade, porque as tecnologias empregadas eram diferentes. Para isso foi necessário que alguém tomasse à frente dos estudos e desenvolvesse algo que pudesse tornar padrão o método de trocar informações por meio do ar, atividade esta que ficou por conta do IEEE (TANENBAUM, 2003).

No início do projeto, o objetivo era fazer que as redes sem fio se conectassem com a rede *Ethernet* – rede cabeada. Foi criado então o padrão IEEE 802.11 e divulgado em 1997, que trata das redes sem fio ou *Wi-Fi* (*Wireless Fidelity*). A maior dificuldade deste padrão era o fato de sua velocidade ser de no máximo 2Mbps. O próximo passo seria criar um novo padrão, porém mais veloz. Dois anos depois são apresentados os padrões 802.11b e 802.11a que possuem uma velocidade maior (GRÜNEWALD, 2005). Outros padrões, que trazem novas implementações foram criados após estes.

3.1 PADRÕES

Conforme já visto no tópico anterior, as redes *Wi-Fi* foram aprimoradas de modo que pudessem alcançar uma velocidade maior do que a oferecida no projeto inicial que é de no máximo 2Mbps. Os padrões mais utilizados atualmente serão apresentados nos tópicos a seguir.

3.1.1 802.11b

Ratificado no ano de 1999, foi o primeiro sub-padrão a ser apresentado pelo IEEE, permitindo velocidades de transmissão máximas de 11Mbps, sendo que opera também nas velocidades de 5,5Mbps, 2Mbps ou ainda 1Mbps. Para a transmissão dos dados, a freqüência é de 2,4GHz. Alguns equipamentos eletro-eletrônicos utilizam esta mesma freqüência (celulares, forno de microondas, entre outros), por este motivo poderá haver interferências e ruídos na transmissão do sinal. Comporta no máximo 32 computadores conectados em um determinado ponto de acesso ao mesmo tempo. Apesar desta limitação ele é o padrão mais utilizado atualmente. Outras características são o fato de possuir o maior numero de ferramentas disponíveis para sua administração e possui um baixo custo, devido ao fato de utilizar uma freqüência gratuita (DUNCAN, 2006).

3.1.2 802.11a

Este padrão foi desenvolvido para melhorar a velocidade dos padrões sem

fio. Opera a uma velocidade teórica de 54Mbps (pode atingir até 108Mbps no modo *full-duplex*) na faixa de freqüência de 5GHz. As suas principais vantagens se comparado ao padrão 802.11b são o fato de ter sua velocidade superior (sendo quase quatro vezes mais rápido) operar em uma freqüência pouco utilizada e suportar até 64 usuários conectados no mesmo ponto de acesso. Pode-se citar como alguns pontos negativos, ainda comparado ao padrão 802.11b, o fato de não alcançar uma distância muito longa, pois alcança teoricamente a metade da distância que o outro. Desta forma, é necessário utilizar mais pontos de acesso para cobrir a mesma área que a do outro, assim os custos irão aumentar. É pouco utilizado, pois não é compatível com o outro padrão que hoje em dia está na maioria dos locais, por isso é mais difícil disseminá-lo (GRÜNEWALD, 2005).

3.1.3 802.11g

Padrão desenvolvido no ano de 2001 une as vantagens do padrão 802.11b com o 802.11a. Funciona na freqüência de 2,4GHz, que é gratuita, possibilitando assim a interoperabilidade com o padrão mais utilizado, sendo portanto mais fácil de implantá-la em um dado ambiente. A velocidade que pode atingir é de 54Mbps (atinge 108Mbps no modo *full-duplex*), mesma que a do padrão 802.11a. Considerando que haja algum equipamento referente à tecnologia 802.11b e outro 802.11g na rede, apesar da haver a comunicação entre eles, a velocidade será de 11Mbps (MATOS, 2005).

3.1.4 Outros Padrões

É importante comentar que Rufino (2005) ressalta outros padrões para a tecnologia *Wi-Fi*, bem como o padrão 802.11i que possui como objetivo principal o quesito de segurança. O 802.11n que foi desenvolvido de modo que possa operar em velocidades de até 500Mbps sendo compatível com os padrões utilizados atualmente. Por fim é mostrado o padrão 802.1X que não é especificamente para as redes *Wireless*, mas pode também ser empregado nela, pois trata de autenticação do usuário na rede. Ele possui alguns métodos que controlam esse mecanismo de acesso, permitindo assim um pouco mais de segurança para a rede. Grünewald (2005) acrescenta a existência dos padrões 802.11d, 802.11e, 802.11f, 802.11h, 802.11k, 802.11r e 802.11s.

3.2 TOPOLOGIAS

As topologias encontradas para as redes *Wireless* são dispostas basicamente de duas maneiras ponto-a-ponto, onde os dispositivos conectam-se entre si e infra-estrutura, em que eles utilizam um ponto de acesso em comum para se comunicarem (TANENBAUM, 2003).

3.2.1 Ponto-a-Ponto

Este modo permite que um dispositivo troque informações diretamente com outro dispositivo, como visualizado na Figura 8, isto é, não utilizam um ponto de acesso para conectá-los. Deste modo não há um controle centralizado, por isso é utilizado

comumente para uma rápida troca de informações ou criar pequenas redes, o que envolve aproximadamente cinco computadores (DUNCAN, 2006).

Quando comparado o *Wi-Fi* com a topologia em barra da rede cabeada, nota-se uma vantagem, pois se um computador deixar de funcionar não irá interferir na comunicação dos outros, enquanto que na outra se um não funciona, o restante também pára de funcionar (RUFINO, 2005).

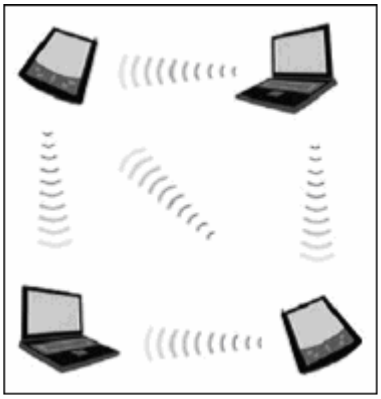

Figura 8. Topologia de rede no modo ponto-a-ponto
Fonte: RUFINO, N. (2005)

3.2.2 Infra-Estrutura

Rufino (2005) explica que neste modo de operação o ponto de acesso é o equipamento chave para que esta topologia funcione, já que todos os dispositivos ‘conversam’ entre si por meio dele. Neste modo é mais simples e fácil controlar a rede, porque todas as conexões são realizadas somente em um ponto, desta forma há um nível de segurança maior. Outro ponto importante é que a abrangência da área alcançada neste modo torna-se mais ampla e a comunicação com a rede cabeada ou o acesso à Internet facilitada.

Segundo Fernandes (2006) os dispositivos que se conectam através de um ponto de acesso, obedecem a algumas configurações como:

a) modo *Basic Service Set* (BSS): área de abrangência de um único ponto de acesso (célula), conforme exemplo na Figura 9;

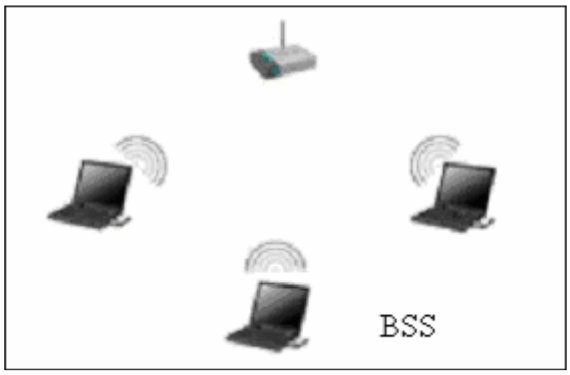

Figura 9. Modo BSS
Fonte: FERNANDES, M. (2006)

b) modo *Extended Service Set* (ESS): Áreas distintas de abrangência sendo conectadas por diferentes pontos de acesso conforme apresentado na Figura 10.

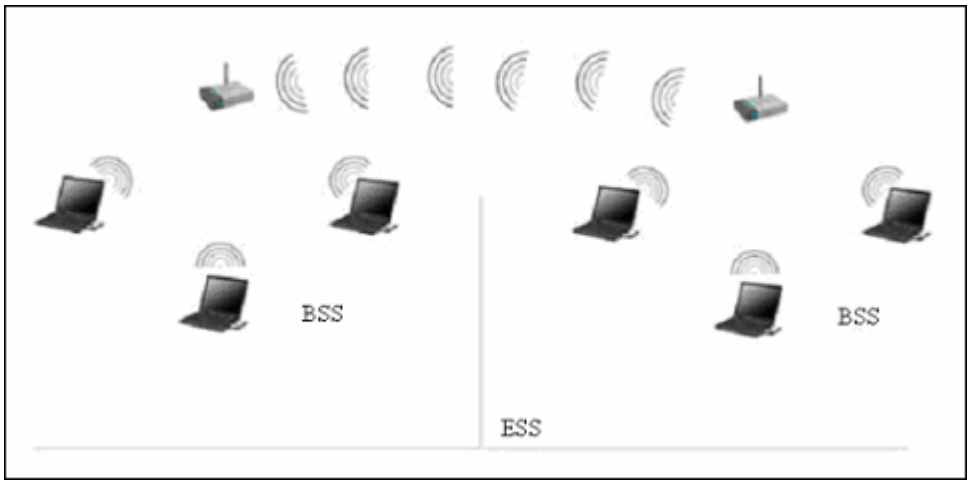

Figura 10. Modo ESS
Fonte: FERNANDES, M. (2006)

3.3 FREQÜÊNCIA

Quando o assunto é freqüência de rádio, faz-se necessário ressaltar que isto

nada mais é do que um sinal que se propaga por meio do espaço em uma distância que está relacionada à sua freqüência, isto é, quanto maior a freqüência menor será o seu alcance. Muitos serviços utilizam radiofreqüência como estações de rádio e TV's, operadoras de telefone móvel, entre outros. Um dos problemas pertinentes a este assunto é o fato destes serviços não serem padronizados a nível internacional, deste modo a freqüência utilizada para ouvir a rádio em um país pode não ser a mesma em outro. Isto pode gerar um certo transtorno na comercialização de alguns serviços (RUFINO, 2005).

3.3.1 Canais

Um sinal de freqüência é subdividido em canais. Estes são utilizados em paralelo com outros canais na mesma faixa para transmitir sinais diferentes. Para ilustrar melhor o conceito de canais, pode-se utilizar como exemplo do seu uso as televisões que possuem sintonia fina. Por meio desta é possível visualizar o conteúdo de um determinado canal nos seus canais adjacentes. Portanto, pode-se concluir que canais muito próximos podem provocar interferência um no outro (RUFINO, 2005).

3.3.2 Técnicas de Transmissão da Camada Física

A seguir serão apresentadas as técnicas utilizadas pela tecnologia *Wi-Fi* para transmitir os dados por meio da camada física de um computador para outro. Os pontos principais em que elas se diferem são a velocidade e a distancia na qual podem alcançar para transmitir os dados.

3.3.2.1 Infravermelho

Este método de transmissão possui um alcance de aproximadamente cinco metros, sendo que para haver comunicação e conseqüentemente troca de informações, os dispositivos precisam estar alinhados e podem alcançar a velocidade de até 2Mbps. O sinal disponibilizado não consegue atravessar uma parede, possibilitando assim o isolamento total de uma sala para outra (GRÜNEWALD, 2005). Este tipo de sinal é comum em controles remoto, *mouse* de computador, entre outros, sendo que se encontra também nos computadores e outros dispositivos móveis para que troquem dados sem a utilização de uma antena.

3.3.2.2 FHSS

O *Frequency Hopping Spread Spectrum* ou Espectro de Dispersão de Saltos de Freqüência utiliza a banda de 2,4GHz subdividida em 75 canais, cada um com 1MHz de largura. Toda a informação trafega por estes 75 canais, saltando de um para o outro várias vezes por segundo, o que acarreta em uma velocidade de transmissão baixa, aproximadamente 2Mbps. A origem e o destino utilizam um mesmo padrão de saltos sincronizados, que define a ordem na qual serão utilizados os diferentes canais. Desta maneira, o sinal só é reconhecido por quem conhece o padrão, chegando como ruído para quem não o conhece (RUFINO, 2005).

Rufino (2005) completa que pode haver mais de um par origem-destino ao mesmo tempo, pois eles estarão utilizando padrões diferentes em tempos diferentes. Se acontecer algum conflito, a origem reenvia a informação e fica no aguardo de uma

confirmação de recebimento por parte do destino.

3.3.2.3 DSSS

Esta técnica chamada de *Direct Sequence Spread Spectrum* (Espectro de Dispersão de Seqüência Direta) utiliza o método conhecido como Seqüência 11-*chip* de Barker. Este método separa cada bit em onze subbits e os transfere redundantemente por um canal cuja banda é de 2,4GHz, e que pode ser dividida em três canais. Ao enviar uma informação, o DSSS encaminha também uma mensagem para verificar se o receptor consegue compreender o que ela quer dizer. A taxa de transmissão é de aproximadamente 11Mbps, mas opera também com velocidades menores (TANENBAUM, 2003).

3.3.2.4 OFDM

O Orthogonal Frequency Division Multiplexing (Multiplexação Ortogonal por Divisão de Freqüência) têm a capacidade de transmitir os dados a uma velocidade de até 54Mbps na banda de 5GHz, para isto é utilizado um total de cinqüenta e duas freqüências, onde quarenta e oito transmite os dados e as outras quatro têm a função de sincroniza-los. O sinal dividido em várias bandas estreitas e permite algumas vantagens como melhora na imunidade à interferência de banda estreita e a utilização de bandas não contíguas (GRÉGIO, 2005).

3.3.2.5 HR-DSSS

A *High Rate Direct Sequence Spread Spectrum* (Espectro de Dispersão de Seqüência Direta de Alta Velocidade), possui taxa de transmissão de aproximadamente 11Mbps, sendo que opera também a 1Mbps, 2Mbps e 5,5Mbps na banda de 2,4GHz. Ela pode adaptar-se a taxa dinamicamente dependendo das condições de carga e ruído, de modo que a velocidade alcançada seja a melhor possível - geralmente opera em 11Mbps (GRÉGIO, 2005).

3.4 PROTOCOLOS

Como já citado no item 2.3 os protocolos são regras estabelecidas que permitem que um computador entenda o que o outro está ‘falando’. Os protocolos utilizados pelo padrão 802 possuem suas estruturas muito semelhantes uns dos outros. A Figura 11 ilustra o protocolo parcial 802.11. Se comparado ao modelo OSI, este protocolo é bastante semelhante no que se refere à camada física, mas se subdivide na camada de enlace.

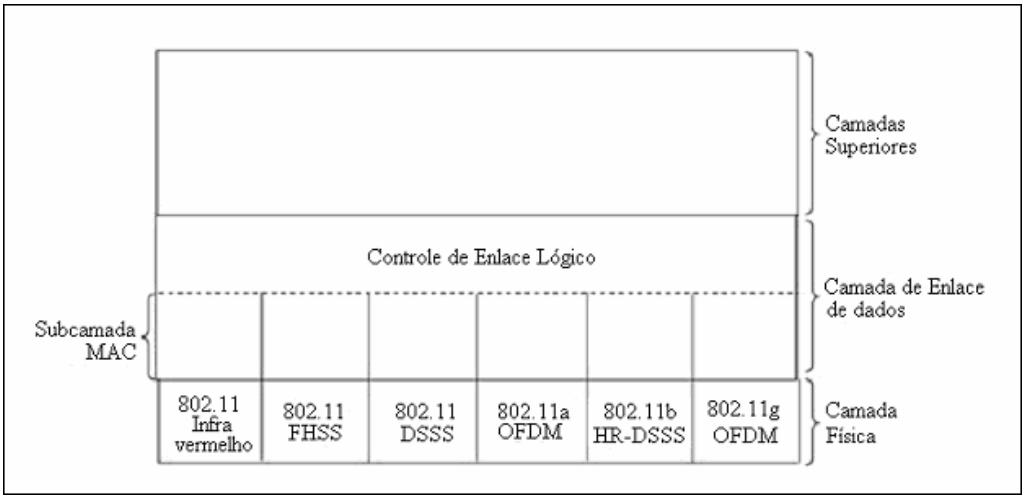

Figura 11. Pilha de Protocolos 802.11
Fonte: TANENBAUM, A. (2003)

A primeira subcamada do enlace é a LLC, responsável por tornar o acesso à rede de forma transparente, mesmo quando a comunicação acontece entre variações diferentes do padrão 802. A camada abaixo desta é a MAC, que possui a função de determinar de quem é a vez para o envio da informação na rede (TANENBAUM, 2003).

3.4.1 Problema da Estação Oculta e Exposta

Para exemplificar esta situação, pode-se considerar o seguinte caso: o computador A pode transmitir algum dado para o computador B, e neste mesmo instante o computador C, que não reconhece o computador A, tenta transmitir algum dado para o computador B. Poderá ocorrer algum erro. Este é conhecido como o problema da estação oculta, isto é, quando dois computadores que estão fora de alcance um do outro tentam transmitir algo para o mesmo computador. Em contra-partida, há o problema da estação exposta, que é quando o computador B envia dados para o computador C, mas ao mesmo tempo o computador A quer enviar dados para o computador D (não está na figura), como já há alguém transmitindo ele não continua a operação, mas poderia ser

realizada sem nenhum problema já que uma troca não irá interferir na outra (TANENBAUM, 2003). A Figura 12 ilustra os problemas supracitados:

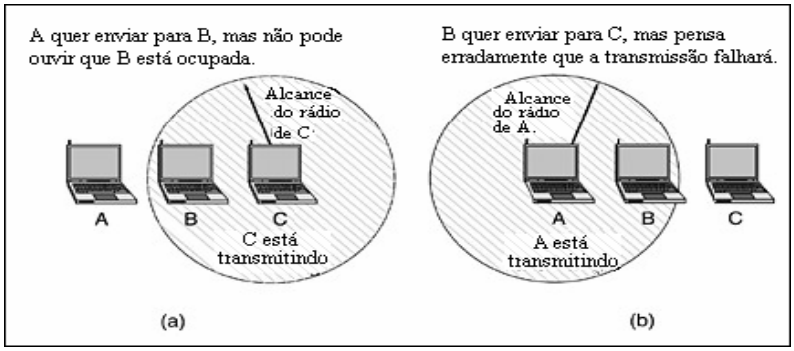

Figura 12. (a) Problema da estação oculta. (b) Problema da estação exposta
Fonte: TANENBAUM, A. (2003).

Para resolver este problema o padrão 802.11 utiliza dois métodos, sendo o primeiro o *Distributed Coordination Function* (DCF - Função de Coordenação Distribuída), que não utiliza nenhum ponto de acesso para controlar o acesso e o segundo que é o *Point Coordination Function* (PCF - Função de Coordenação de Ponto), este utiliza algum dispositivo para controlar a atividade que está acontecendo na célula.

3.4.1.1 DCF e PCF

Este método utiliza o protocolo *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). Ele utiliza duas funções para ouvir o canal. Na primeira se estiver ocioso irá transmitir o quadro com os dados por completo, sendo que enquanto ele está sendo enviado não será feita nenhuma verificação no canal, podendo assim ser destruído no receptor devido às interferências. Se o canal estiver sendo utilizado, então a estação irá aguardar até o momento em que ele fique desocupado para transmitir. No caso de uma colisão, as estações irão esperar um tempo aleatório para

retransmitir os dados (BARCELOS; GONÇALVES; ALVES JÚNIOR, 2003).

A segunda baseia-se em um método de detecção do canal virtual, que está ilustrado na Figura 13. Neste caso, considera-se que o computador A deseja enviar dados para o computador B. Há ainda o computador C que reconhece o B e A e também o computador D que reconhece apenas o B e o C. Neste instante, A pergunta para B se pode ou não encaminhar o quadro. Se B permitir, ele irá retornar uma resposta afirmativa para A. Assim que A receber o 'sim', ele irá enviar o quadro de dados. Após B ter recebido o quadro por completo, ele responderá para A que foi recebido com sucesso, caso contrário o processo será executado outra vez (TANENBAUM, 2003).

Para os computadores C e D este processo ocorre da seguinte maneira: C reconhece A, quando A faz a pergunta para B, C também irá recebe-lo, desta maneira ele não irá enviar nenhuma informação, mas solicitará um canal virtual que ele mesmo irá ocupar. Este canal virtual é conhecido como *Network Allocatiom Vector* (NAV – Vetor de Alocação de Rede). O canal não é transmitido, mas serve como uma espécie de aviso, que se mantém inativo até o momento em que acabar a transmissão de A para B. Da mesma forma ocorre com o D, embora ele não escute a pergunta do A, ele ouvirá a resposta do computador B, então solicitará também um NAV, para que depois de terminado o tempo possa estar enviando seus quadros de informações (TANENBAUM, 2003).

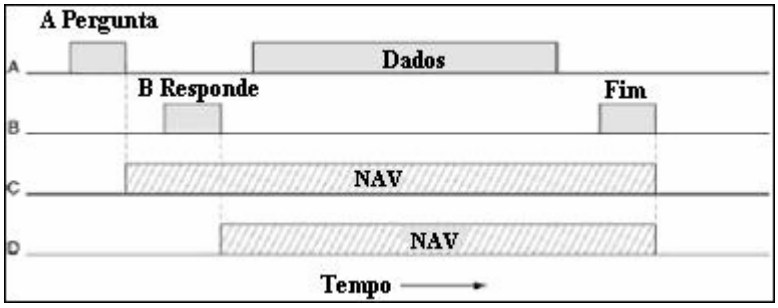

Figura 13. Detecção do Canal Virtual - CSMA/CA
Fonte: Adaptado de TANENBAUM, A. (2003)

Conforme já explicado no item 3.4.1, o método PCF utiliza um ponto de acesso para controlar o acesso de um dado dispositivo na célula. Deste modo, ele pergunta às estações se há algo que deve ser enviado e o adiciona no *pooling*, por isso neste método não ocorre o problema de colisão (BARCELOS; GONÇALVES; ALVES JÚNIOR, 2003).

3.5 SEGURANÇA

Juntamente com o crescente aumento da utilização do ambiente *Wi-Fi*, vem a preocupação com a segurança do mesmo. Pelo fato dos dados serem transmitidos por meio do ar, é mais fácil um invasor ter acesso à rede e, sua presença no ambiente pode ser imperceptível, dependendo do alcance do sinal dos transmissores. Deste modo, os fabricantes destes dispositivos têm procurado desenvolver algo seguro e eficaz na transmissão e recepção dos dados (AMARAL; MAESTRELLI, 2004).

A criptografia é um método utilizado para fornecer segurança aos dados que são trafegados na rede. Ela impede que invasores tenham o conhecimento por meio de técnicas que transfiguram os dados, isto é, faz com que eles não sejam entendidos por quem não tem permissão ao acesso a eles (MORENO; PEREIRA; CHIARAMONTE, 2005).

3.5.1 Wired Equivalent Privacy (WEP)

Este método de criptografar os dados foi desenvolvido e utilizado primeiramente nas redes *Wi-Fi* 802.11. Ele foi escolhido porque atende a alguns quesitos necessários para se ter um mínimo de segurança no ambiente, tais como (BARCELOS; GONÇALVES; ALVES JÚNIOR, 2003):

a) razoavelmente forte: Para que seja utilizado ele deve oferecer algum nível de segurança para o usuário (GRÜNEWALD, 2005);

b) auto sincronizável: Assim que encontrar algum sinal disponível e que possa se conectar ao ambiente, ele deve fazer este processo de forma automática, isto é, o usuário não deve se preocupar em fazer qualquer configuração que seja de forma manual (AMARAL; MAESTRELLI, 2004);

c) computacionalmente eficiente: Pode ser implementado por algum software ou hardware e dispositivos que tenham pequena capacidade de processamento (AMARAL; MAESTRELLI, 2004);

d) exportável: Não deve se limitar a um único país ou local, mas deve ser disseminado por todo o globo terrestre (GRÜNEWALD, 2005);

e) opcional: Se o usuário desejar ele pode habilitá-lo ou não (JUNIOR; BRABO; AMORAS, 2004).

Opera na camada de enlace de dados e utiliza o método de criptografia *Route Coloniale* 4 (RC4)[3] e o *Cyclic Redundancy Check* (CRC-32) para garantir a integridade dos dados (GIMENES, 2005).

Rufino (2005) explica que este método de criptografia pode ser quebrado com alguns programas disponíveis no mercado, bastando apenas que o tráfego da rede seja monitorado por algum tempo até que se descubra qual a chave utilizada e então usufruí-la do modo que desejar, pois a chave é estática, portanto uma vez descoberta, a rede ficará vulnerável até que ela seja trocada.

3.5.2 Wi-fi Protected Access (WPA)

Este método foi criado após o WEP e possui alguns modelos de segurança, os quais são empregados dependendo da necessidade do usuário. Por exemplo, no modo ponto-a-ponto pode-se optar por utilizar uma chave de criptografia compartilhada, semelhante à que é fornecida no WEP, porém utiliza o protocolo conhecido como *Temporal Key Integrity Protocol* (TKIP), que é o responsável por efetuar a troca dinâmica das chaves com um vetor inicial de 48 *bits*. Já no modo infra-estrutura, um servidor para autenticação dos usuários possuirá uma maior segurança do que apenas a chave compartilhada (RUFINO, 2005).

Para se tornar mais seguro, algumas implementações de autenticação de usuários foram adotadas no WPA, métodos estes que não existem no WEP.

---

[3] Inicia com um vetor de 24 *bits* e, após isso se une com uma chave de 40 ou 104 *bits* para formar a chave de proteção da rede, com um total de 64 ou 128 *bits* (GIMENES, 2005).

3.5.2.1 Remote Authentication Dial-In User Service (RADIUS)

Nesta etapa, um usuário qualquer deseja se conectar à rede. Ele encaminha uma mensagem para um cliente RADIUS com as informações referentes ao seu login e senha. O cliente encaminha estes dados para o servidor RADIUS, que verificará primeiramente se ele é válido ou não. Ao verificar que o cliente é verdadeiro, o *login*, senha e porta utilizada por ele serão validadas. Assim que estes dados tiverem sido validados, o servidor RADIUS encaminhará uma resposta ao cliente informando quais as permissões que o usuário possui ou não na rede (GIMENES, 2005).

3.5.2.2 Extensible Authentication Protocol (EAP)

São vários métodos de criptografia utilizados pelo padrão 802.1X para autenticar o usuário na rede, objetivando maior segurança na mesma, os quais se pode citar (BARCELOS; GONÇALVES; ALVES JÚNIOR, 2003):

a) *message digest* 5: É baseado na utilização de senhas (AMARAL; MAESTRELLI, 2004);

b) *lightweight extensible authentication protocol*: Utiliza a autenticação de senhas no servidor RADIUS e altera constantemente a chave criptográfica, de modo que proteja ainda mais de possíveis invasores (AMARAL; MAESTRELLI, 2004);

c) transport layer securitty (TLS): É considerado complexo de configurar, mas que é válido pela segurança oferecida. Utiliza o servidor RADIUS e certificado digital na estação e servidor

(AMARAL; MAESTRELLI, 2004);

d) *tunneled*-TLS/*protect* EAP: O servidor utiliza o certificado digital para se identificar com o usuário, mas o usuário em contra-partida faz o uso de apenas seu *login* e senha para se identificar com o servidor por meio de um ‘túnel’, o que torna a conexão entre ambos mais segura (AMARAL; MAESTRELLI, 2004).

3.5.3 Wi-fi Protected Access 2 (WPA2)

Este padrão foi disponibilizado pela *Wi-Fi Alliance*[4] e ratificado por meio do grupo IEEE no ano de 2004. Sua diferença principal em relação ao padrão WAP é o método utilizado para criptografar os dados que serão trafegados na rede sem fio. Para maior segurança se comparado com o WEP, o WPA utiliza-se do método TKIP e RC4. Em contra-partida, o WPA2 sugere a implementação do algoritmo *Advanced Encription Standard* (AES), que é mais seguro ainda do que o WPA, uma vez que a chave criptográfica juntamente com o TKIP é de 256 *bits* e no anterior é de apenas 48 *bits*. Ele opera também com chaves criptográficas menores como 128 e 192 *bits*, embora o padrão seja de 256 *bits* (LACERDA, 2007).

3.5.4 VPN

Tecnologia utilizada para prover um maior grau de segurança na transmissão dos pacotes de dados nas redes públicas. Isto porque ele utiliza por meio de

[4] Associação internacional responsável por certificar a interoperabilidade de produtos *Wi-Fi*.

um túnel[5], a conexão entre a origem e o destino, garantindo assim que eles troquem informações entre si. Os pacotes com estas informações são criptografados na origem de modo que não sejam interceptados até que cheguem ao seu destino, que irá fazer com que os dados sejam descriptografados e fiquem em seu formato original (JUNIOR; BRABO; AMORAS, 2004).

Sua aplicação ocorre na camada de rede do modelo RM-OSI, podendo assim ser aplicado juntamente com o WEP, por exemplo. A Figura 14 apresenta um método de sua utilização, com o objetivo de fornecer um nível maior de segurança. Algumas VPN's fazem o uso do protocolo *Internet Protocol Security* (IPSec), que provê algumas proteções adicionais bem como privacidade, autenticação da informação de origem, autenticação do usuário por meio de *login* e senha - podendo esta ser realizada por um servidor RADIUS, entre outros (AMARAL; MAESTRELLI, 2004).

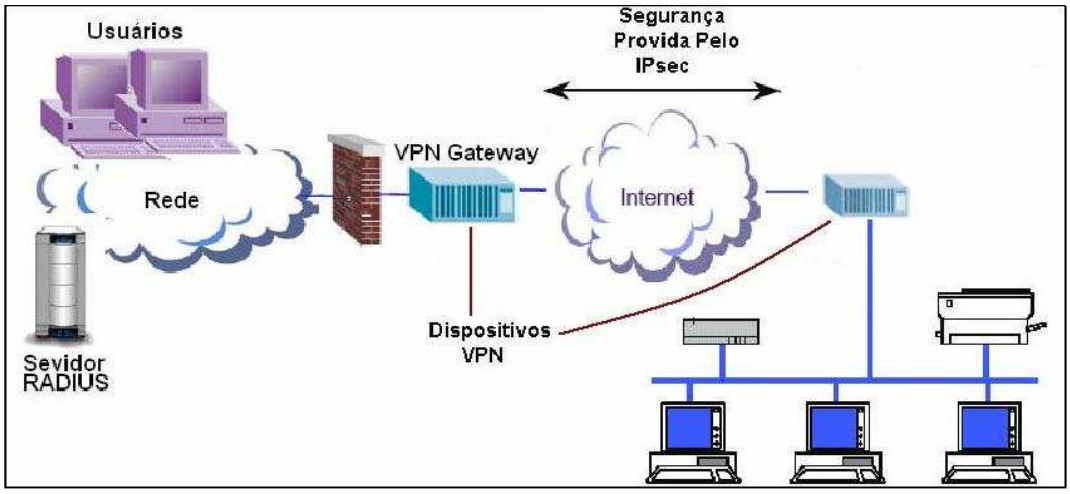

Figura 14. VPN
Fonte: Adaptado de AMARAL, B. M.; MAESTRELLI, M. (2004)

Com o estudo deste Capítulo pode-se concluir que as redes *wi-fi*, possuem algumas vantagens quando comparadas às redes cabeadas, por exemplo, a mobilidade oferecida pelo fato de não utilizar cabos para interconectar os computadores, diferencial

[5] Encapsulamento de um protocolo dentro de outro.

que estabelecimentos como *cyber*-cafés, shoppings, entre outros, podem oferecer como atrativo e aumentar a clientela.

Foram apresentados os principais padrões existentes e suas características diferenciais um do outro. Estes padrões não são imunes a ataques, isto é, se alguém tentar invadir o ambiente será necessário que ele ofereça algum tipo de segurança para seus usuários. Desta forma, os métodos mais importantes e utilizados atualmente nesta área foram discutidos para exprimir a sua relevância neste tipo de rede.

4 POWER OVER ETHERNET

Este modelo teve início no ano de 1999. Ele foi conceituado e desenvolvido pelo grupo IEEE, denominado de IEEE 802.3af, que é uma extensão do padrão IEEE 802.3. Inicialmente os principais interessados foram as empresas 3Com, Intel, PowerDsine, Nortel, entre outros, porque reconheciam que havia uma necessidade de fornecer energia sobre o cabo *Ethernet*. Houveram outras implementações relacionadas, mas a falta de um padrão fez com que o mercado continuasse sem avanços (POWER OVER ETHERNET, 2003, tradução nossa).

O padrão envolveu muitos especialistas de empresas diferentes, o que de certa forma o beneficiou, porque era estudado sob diversas perspectivas diferentes. O IEEE 802.3af foi aprovado e surgiu formalmente no mês de junho do ano de 2003 (POWER OVER ETHERNET, 2003, tradução nossa).

Com o surgimento e a comum utilização deste padrão, a ascensão no mercado dos dispositivos resultantes desta tecnologia tende a crescer. Isto, porque o custo de adquirir e empregar equipamentos PoE para determinada solução deverá reduzir à medida que o tempo passa e a tecnologia evolui (POWER OVER ETHERNET, 2003, tradução nossa).

A Figura 15 exemplifica algumas formas de utilizar o *Power over Ethernet*. Ele está presente principalmente em telefones *Voice over Internet Protocol* (VoIP), pontos de acesso *wireless* e outras aplicações que podem obter sua fonte de alimentação elétrica por meio do cabo *Ethernet*, que é comumente utilizado nas redes LAN, sem que seja necessário modificar a infraestrutura existente (POWER OVER ETHERNET, 2003, tradução nossa).

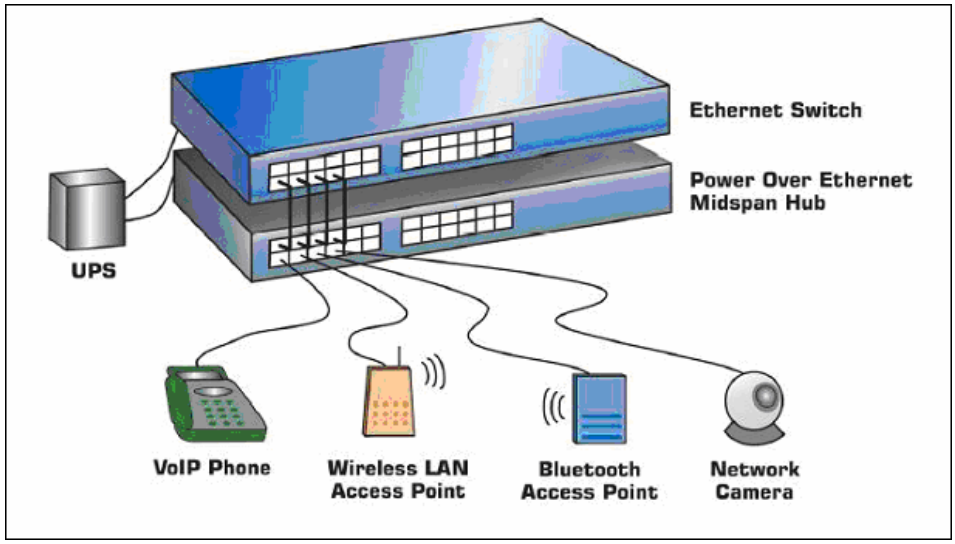

Figura 15. Aplicações PoE
Fonte: POWER OVER ETHERNET, 2003

4.1 FUNCIONAMENTO

Conforme descrito na seção anterior, a energia irá ser transmitida por meio do cabo *Ethernet*, mais precisamente pelo par-trançado 10/100BaseT[6]. Este cabo quando utilizado para montar a rede, apenas dois pares deles trafegam dados (1,2 e 3,6) e os outros dois (4,5 e 7,8) são utilizados somente em redes cuja velocidade está na casa do gigabit. A tecnologia PoE se aproveita dos pares que não são utilizados para fornecer a energia que irá alimentar os dispositivos que suportam esta técnica (IEEE, 2003).

4.2 OBJETIVOS DA TECNOLOGIA

Assim como os dispositivos presentes na Figura 15, há outros equipamentos que também utilizam os dados da rede e que para serem ligados precisam de energia provenientes da rede elétrica. Com isso, alguns dos benefícios resultantes deste padrão

[6] Padrão que define as características do cabo, por exemplo, comprimento, conectores, topologia, entre outros.

que se pode citar são (POWER OVER ETHERNET, 2003, tradução nossa):

a) o uso de apenas um cabo para efetuar duas tarefas reduz o custo com a aquisição do mesmo e economiza espaço;

b) não há a necessidade de um eletricista, desta forma não será necessário pagar pelo serviço prestado por ele e também ficar esperando para que seja atendido;

c) o dispositivo pode ser movido de maneira fácil e rápida para qualquer outro local da rede, desde que haja uma fonte de alimentação e esteja dentro do alcance permitido;

d) a transmissão dos dados se dá de forma mais segura, porque não há uma tensão capaz de prejudicar o envio do mesmo;

e) um equipamento externo, como um *no-break*[7] por exemplo, pode garantir o fornecimento de energia ao dispositivo PoE, quando por algum motivo houver a falta da mesma e consequentemente manter ligado aquele que está sendo alimentado por ele;

f) os dispositivos podem ser reiniciados à distância, isto é, basta desconectar o cabo que está ligado no equipamento fornecedor de energia e dados.

Com base nestes aspectos se pode concluir que eles é que nortearam e foram os focos da implementação para as aplicações que fazem o uso deste padrão. Da mesma forma, foi necessário que houvesse o estudo para definir como os equipamentos iriam ser desenvolvidos e utilizados.

---

[7] Na Figura 14 a representação deste, é dado pelo equipamento *Uninterruptable Power Supply* (UPS).

4.3 HARDWARE

Os equipamentos PoE podem ser classificados em duas categorias. A primeira é o chamado *Power Sourcing Equipment* (PSE). Este dispositivo é responsável por fornecer a alimentação de energia aos outros. A segunda categoria é o *Power Device* (PD), que conseqüentemente será o receptor da energia proveniente do PSE (IEEE, 2003).

4.3.1 *Power Sourcing Equipment*

Conforme já explicado, estes equipamentos são os fornecedores de energia para outros dispositivos por meio do mesmo cabo que trafega os dados. Os principais componentes deste grupo são:

a) *switch*: Ele é utilizado para trafegar os dados por meio de uma conexão direta entre origem e destino (SPURGEON, 2000);

b) *splitter*: Recebe dados e energia diretamente de um dispositivo PoE para em seguida separa-los e encaminha-los aos dispositivos que não suportam esta tecnologia (TRENDNET SPLITTER, 2005, tradução nossa);

c) *injetor*: Faz o processo contrário ao *splitter*. Neste caso, ele recebe os dados e energia de equipamentos distintos para transferi-los por meio de um único cabo para o dispositivo final (TRENDNET INJECTOR, 2005, tradução nossa).

A potência de no máximo 15,4W e a identificação dos *powered devices*

são algumas das características comuns entre estes três equipamentos.

Os dois últimos equipamentos citados são utilizados para conectar um dispositivo PoE com outro que não suporta esta tecnologia e assim ser possível trocarem informações. Na Figura 16 pode-se visualizar a utilização destes equipamentos em uma única aplicação. Não necessariamente serão utilizados o splitter e injetor ao mesmo tempo. Por exemplo, considerando na Figura 16 que o dispositivo representado pela antena *wireless* fosse PoE, não seria necessário a utilização do splitter. Ou ainda, se o *switch* suportasse a tecnologia 802.3af não seria necessário a utilização do injetor. Pode ocorrer também que o *switch* e a antena *wireless* sejam PoE, esta é a melhor situação, principalmente porque não haverá gastos com os equipamentos intermediários.

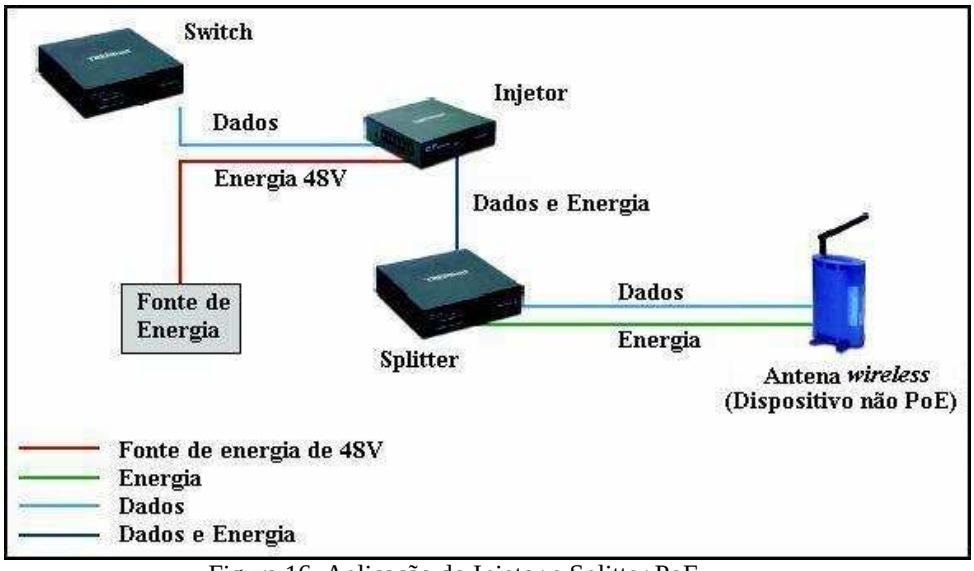

Figura 16. Aplicação do Injetor e Splitter PoE
Fonte: TRENDNET INJECTOR, (2005)

4.3.2 Power Device

Estes são os dispositivos receptores da energia provida pelo PSE por meio do cabo *Ethernet*. Analisando a Figura 16, pode-se deduzir que normalmente eles serão

os equipamentos terminais utilizados em determinada aplicação. No exemplo anterior, a antena *wireless* representa um *power device*, mas há muitos outros que também são denominados desta maneira como o telefone VoIP, câmeras de segurança, terminal *Point Of Sale* (POS), entre outros (IEEE, 2003).

Vantagens:

a) Utilização de um único cabo.
b) Redução de custos com a fiação elétrica
c) Fácil mobilidade por meio da rede de computadores
d) Reinício à distância

Desvantagens:

a) Alimentação ainda é baixa, em torno de 44 à 57V.
b) Nem todo equipamento que possui a tomada RJ-45 pode ser alimentado pelo PoE.

O objetivo do Capítulo não é detalhar os conceitos técnicos desta tecnologia, pois não é este o foco, mas sim a sua pesquisa e conhecimento em geral. Quem a implementou foi o IEEE com o objetivo de transmitir energia por meio do cabo *Ethernet* que até então trafegava somente dados em suas aplicações. Com base neste Capítulo pode-se concluir quais as suas principais vantagens e quando utilizá-lo.

Os equipamentos beneficiados com este padrão não estão presentes somente nas redes LAN, mas também há outras situações em que eles podem ser aplicados.

5 *HOTSPOT*

A tradução literal do ingês para o português do termo *Hotspot* pode ser entendido como “Ponto Quente”. Ele pode ser descrito como uma área ou local qualquer com acesso à tecnologia sem fio. Comumente estes locais são *cyber-cafés*, hotéis, aeroportos, shopping, entre outros. O motivo de ter disponível nesses ambientes este tipo de serviço é um diferencial que proporcionará aos seus frequentadores estarem conectados na rede mundial de computadores de modo confortável e de fácil acesso devido à sua mobilidade (GREGO, 2006).

Kurose e Ross (2006) reforçam a idéia de que o sistema sem fio de comunicação irá se expandir e cada vez mais ganhar espaço, devido a mobilidade e outros benefícios que oferecem.

5.1 LOCALIZANDO *HOTSPOTS*

Leal (2007) explica que os *Hotspots* podem ser encontrados principalmente de duas formas, sendo a primeira por meio de dispositivos que verificam no local se há algum sinal de conectividade disponível e a outra é utilizando uma ferramenta, seja ela um site ou algum software específico para tal finalidade. Leal (2007) finaliza com uma lista de sites Localizadores de *Hotspots* e explicando que os notebooks mais recentes e PDA’s já têm os dispositivos localizadores embutidos. Uma outra maneira, diferente das duas citadas anteriormente está exemplificada na Figura 17.

Figura 17. Banner de um Hotspot

Acessando o site http://www.jiwire.com presente na listagem fornecida pelo autor acima, há 241.044[8] *Hotspots* localizados em 135 países e que podem ser todos encontrados utilizando-o como ferramenta de busca. Outros dados como, quais os países com o maior número de zonas *Wi-Fi* e quais os locais mais utilizados para a aplicação deste, conforme as Tabelas 1 e 2 a seguir também podem ser encontrados.

Tabela 1. Países com o maior número de *Hotspots* no mundo

Posição	País	*Hotspots*
1	Estados	67,132
2	Reino	32,589
3	França	24,174
4	Alemanha	21,792
5	Coréia do	21,076
6	Japão	11,027
7	Rússia	8,373
8	Espanha	6,041
9	Itália	5,450
10	Taiwan	4,415

Fonte: JIWIRE, 2008

[8] Estes dados foram coletados no dia 01/03/2008, pode ser que atualmente existam mais *Hotspots* o que torna estes dados desatualizados.

Tabela 2. Locais mais utilizados para a implantação de Hotspots

Posição	Local	*Hotspots*
1	Hotéis	47,964
2	Outros	34,578
3	Restaurantes	33,004
4	Cafés	28,427
5	FON Spot	27,868
6	Lojas/Shopping	21,842
7	Pubs	8,271
8	Office Building	7,345
9	Bares	4,059
10	Lojas de	2,732

Fonte: JIWIRE, 2008

Apesar de aparecer em décimo lugar, Taiwan é o país com a cidade que possui a maior rede pública de internet banda larga sem fio do mundo. Taipei, que é a capital de Taiwan possui 2,6 milhões de pessoas e sua região metropolitana possui 90% do território coberto pelos 4100 pontos de acesso disponíveis para se conectar à rede mundial de computadores (FICHTNER, 2007).

Fichtner (2007) completa que no Brasil este processo caminha em passos lentos. O governo federal investirá 40 milhões de reais com o projeto Cidades Digitais, que irá abranger 160 cidades até o fim do ano de 2008. Ao todo no país são 5564 cidades, sendo que 3570 não estão conectadas à Internet e somente 24 delas possui acesso público sem fio.

No Brasil, o estado de São Paulo está em primeiro lugar disparado no quesito quantidade de *Hotspots* instalados com 1403, em segundo está o Rio de Janeiro com 143, em terceiro o Distrito Federal com 65 e Santa Catarina aparece em décimo lugar com 19 (JIWIRE, 2008).

5.2 ONDE ENCONTRAR E QUEM TEM ACESSO

Conforme mostra a Tabela 2, estes são os locais mais utilizados para se implantar um *Hotspot*, isto é, onde há pessoas para se conectar a eles. SOUSA (2002) explica que por não existirem fios conectando os dispositivos para acessarem à Internet por exemplo, a mobilidade é um dos ingredientes diferenciais e atrativos que estes ambientes podem oferecer para seus clientes e fazê-los com que voltem outras vezes. Na Figura 18 o autor realiza uma pesquisa na zona *wi-fi* do Criciúma Shopping.

Figura 18. Autor utilizando Wireless

O objetivo de se ter *Hotpots* em locais como aeroportos e praças, por exemplo, não é ganhar clientes, mas oferecer ao usuário uma opção que somente esta tecnologia pode oferecer. Por exemplo, sair de casa para ir até a praça consultar os e-mail's e ao mesmo tempo se distrair um pouco. Outro exemplo é a redução de gastos com infra-estrutura nas cidades onde as câmeras de segurança são utilizadas pela polícia

em locais distantes (FICHTNER, 2007).

Conectar-se nos ambientes *Wi-Fi* está ficando a cada dia mais fácil, isto porque os dispositivos para acessá-los já têm a tecnologia disponível para isso. Dentre estes equipamentos pode-se citar os notebook's, PDA's, iPhones[9], entre outros. Já para os demais que podem se ligar à rede, mas que não possuem o dispositivo instalado originalmente, há alguns adaptadores disponíveis que fazem este serviço.

5.3 *HOTSPOT* E POE

Com base no conhecimento adquirido, a utilização de equipamentos PoE tem como um dos objetivos minimizar o custo da construção do *Hotspot* bem como torná-la mais fácil. O estudo de caso que será realizado, foi escolhido pois decidiu-se que o ambiente onde será inserido o ponto de acesso não deverá ser alterado esteticamente, visto que seria necessário, pois não possui no local apropriado as tomadas de alimentação elétrica (por isso o PoE) e por não haver nenhuma outra para a rede *Ethernet* (por este motivo o *Hotspot*).

[9] Celular que acessa às redes *Wi-Fi*.

6 TRABALHOS CORRELATOS

Neste Capítulo serão apresentados alguns trabalhos correlatos, cujo foco principal é a sua utilização em muitos lugares, seja ela por necessidade, escolha ou até mesmo atrativo, como nos casos de hotéis, *cyber-cafés*, entre outros.

6.1 PROVISÃO DE QUALIDADE DE SERVIÇO EM REDES IEEE 802.11

Este trabalho foi desenvolvido por Juliana Freitag para obtenção do grau de Mestre na Universidade Estadual de Campinas e apresentado em agosto de 2004. Em seu trabalho ela reporta que o padrão IEEE 802.11 para redes locais sem fio tem sido amplamente utilizado para o acesso móvel aos serviços oferecidos pelas redes fixas, como a Internet. Uma extensão a este padrão, chamada 802.11e, vem sendo desenvolvida com o intuito de introduzir suporte a Qualidade de Serviço (QoS), de forma que as WLANs possam atender as necessidades das aplicações multimídia e de tempo real. Entretanto, as funcionalidades introduzidas não são suficientes para atender os requisitos de QoS das diferentes classes de tráfego em situações de alta carga na rede. Esta deficiência motiva o desenvolvimento de novos mecanismos para monitoramento e controle dos níveis de serviço (FREITAG, 2004).

Este trabalho propõe dois mecanismos de controle para complementar a funcionalidade de QoS: um mecanismo de controle de admissão, adaptado de estudos realizados em redes fixas, e um mecanismo que ajusta dinamicamente os parâmetros de diferenciação de serviços usados no método de acesso com contenção da extensão 802.11e. Os mecanismos propostos contribuem na provisão do serviço requisitado pelas

diferentes classes, bem como na utilização eficiente dos recursos da rede (FREITAG, 2004).

6.2 REDES SEM FIO – TECNOLOGIA, SEGURANÇA E USABILIDADE

Este trabalho foi desenvolvido por Marcus Albert Grünewald para obtenção do grau de Pós-Graduado na Faculdade de Administração e Informática Paulista apresentado no ano de 2005. Em seu trabalho ele salienta que as redes sem fio estão sendo amplamente utilizadas em vários lugares como empresas, instituições, entre outros. Suas vantagens são o custo baixo com telecomunicação, alta imunidade a ruídos, facilidade de configuração de acordo com a necessidade da empresa, sistema de segurança que garante proteção à rede contra ataques externos, além de maior mobilidade e flexibilidade para redes locais (GRÜNEWALD, 2005).

Quando o assunto é segurança, a preocupação existe tanto quanto nas redes cabeadas. Grupos de pesquisa estudam as vulnerabilidades que podem existir quando a rede é atacada por alguém de fora. Como solução existem os protocolos de seguranças, dentre os quais em seu trabalho cita o WEP e IPSec (GRÜNEWALD, 2005).

7 TRABALHO DESENVOLVIDO

O presente capítulo tem por objetivo apresentar cinco estudos de caso de instalação e aplicação de *Hotspot*, onde três são teóricos e dois práticos. Os locais escolhidos pelo autor foram o Criciúma Shopping, Shopping Della Giustina, Universidade do Extremo Sul Catarinense (UNESC), Useall Software todos localizados na cidade de Criciúma e o aeroporto Diomício Freitas em Forquilhinha.

Nos locais em que aplicou-se na prática o *Hotspot*, são encontradas duas situações distintas, onde a primeira seria basicamente para atrair mais freqüentadores para o local e a segunda é utilizada como solução de acesso à Internet.

7.1 ESTUDO DE CASO: CRICIÚMA SHOPPING

O Criciúma Shopping situa-se em Criciúma no bairro Próspera. Sua construção abrange 16.467.60m^2, sendo 14.00.00m^2 para locações. Em seu interior, no pavimento único, encontram-se 100 lojas, 2 restaurantes, 11 *fast-food*, 2 salas de cinema e 1 praça de alimentação. Fora dele há um estacionamento com espaço para mais de 600 vagas (CRICIUMA SHOPPING, 2007).

Segundo CRICIUMA SHOPPING (2007) o mesmo é um centro de compras, diversão, lazer e entretenimento diferente de todos os outros da região. Tem capacidade para atrair mais de 200.00 pessoas por mês.

Com o grande número de pessoas circulando mensalmente, o shopping optou por disponibilizar para seus consumidores o acesso à internet por meio da rede sem fio. A implantação do *Hotspot*, que está localizado na praça de alimentação e pode

ser visualizado na parte destacada em vermelho da Figura 19, se deu em dezembro de 2007, em uma parceria realizada com uma empresa de informática de Criciúma, mas só foi divulgado para o público e imprensa em janeiro de 2008, após testes realizados pela equipe de operações do local.

Rose Fontoura, gerente de marketing do shopping, explica que é premissa básica atender às necessidades de seus clientes, e ela já existe principalmente entre os profissionais liberais e estudantes que buscam um espaço onde possam acessar a internet gratuitamente, realizar reuniões e tudo isso em um ambiente climatizado, com estacionamento seguro, alimentação e opções de compras. Segundo ela, esta inovação apenas atendeu a mais uma necessidade deste cliente e consumidor.

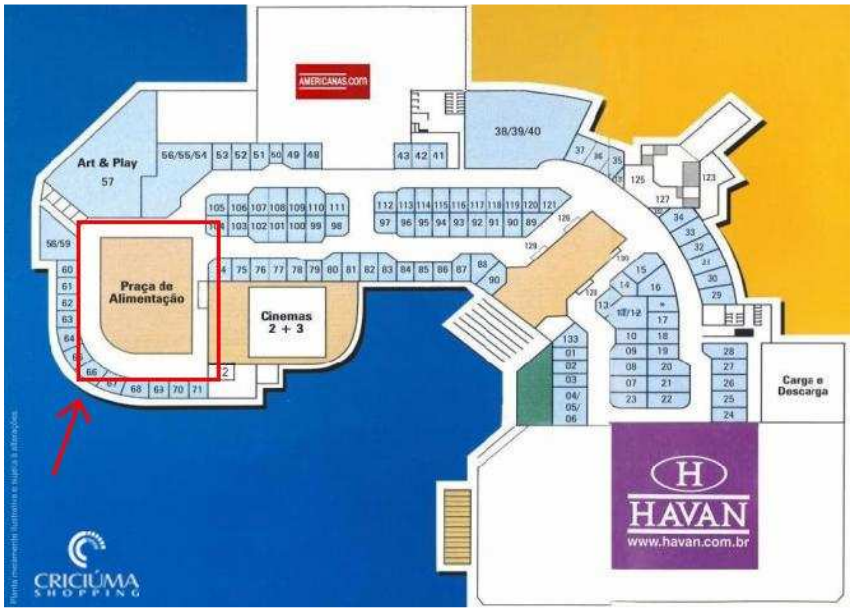

Figura 19: Mapa Criciúma Shopping
Fonte: Adaptado de CRICIUMA SHOPPING (2007)

Fontoura complementa que não foi realizada nenhuma pesquisa para conhecer os usuários ou quantos iriam utilizar o serviço, pois a demanda do mercado já previa esta necessidade. A Figura 20 mostra a localização do ponto de acesso e pode-se ter uma visão geral da praça de alimentação. Ela finaliza dizendo que a proposta é

aumentar cada vez mais o fluxo de pessoas no shopping. Com isso o consumo é conseqüência.

Figura 20. (a) Ponto de Acesso (b) Visão Geral da Praça de Alimentação
Fonte: Adaptado de CRICIUMA SHOPPING, 2007

7.2 ESTUDO DE CASO: UNIVERSIDADE DO EXTREMO SUL CATARINENSE

Com a sede localizada na cidade de Criciúma no bairro Universitário a UNESC presta serviço a toda região sul do estado de Santa Catarina e inclusive à faixa litorânea norte do Rio Grade do Sul (UNESC, 2008).

Segundo Adjano Scarmagnani, analista de suporte da universidade, em abril de 2008 foi disponibilizado para os acadêmicos, funcionários e professores, o acesso à internet por meio da rede sem fio. O objetivo foi oferecer o acesso à rede UNESC nos locais onde não há pontos de rede para os seus computadores móveis como notebooks, *handhelds*, entre outros.

A Figura 21 mostra dois dos três pontos de acesso, sendo que dois estão localizados no bloco administrativo e um outro está dentro da biblioteca. Para conectar-se à rede UNESC, é necessário utilizar algumas configurações pré-definidas que estão disponíveis em um manual oferecido pela universidade na internet[10].

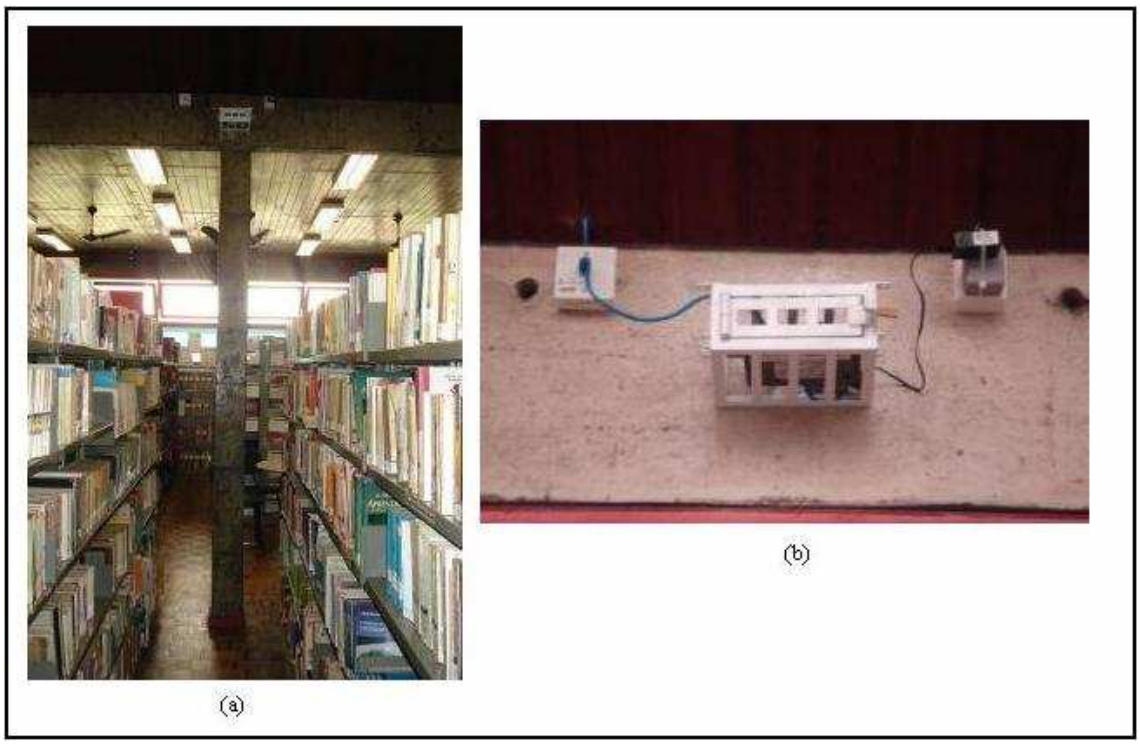

Figura 21. (a) Ponto de Acesso Biblioteca (b) Ponto de Acesso Bloco Administrativo

Scarmagnani explica que o objetivo é abranger futuramente todo o campus. Atualmente o número de usuários ao *Hotspot* gira em torno de 15 por dia.

7.3 ESTUDO DE CASO: AEROPORTO DIOMÍCIO FREITAS

Localizado na cidade de Forquilhinha, à aproximadamente 6Km do centro da cidade de Criciúma, o aeroporto Diomício Freitas conta com um terminal de passageiros com 529,54m^2, sala de embarque com 84m, área de desembarque 27,5 m^2, área de fila para check-in 30 m^2, saguão público com 178 m^2 e oito hangares para

[10] No endereço http://www.unesc.net/dirinfo/docs/MANUAL_WIRELESS_UNESC.pdf.

aeronaves (INFRAERO, 2006).

Conforme o item 1.3 do presente trabalho, a internet sem fio é utilizada geralmente onde há a circulação de pessoas em locais como aeroportos, hotéis entre outros, visto que elas estão acessando e dependendo cada vez mais da internet para efetuar certas atividades em seu cotidiano.

A Figura 22 mostra o salão público, que é o local onde poderia estar instalado o ponto de acesso provendo assim o acesso sem fio à rede mundial de computadores para os freqüentadores do aeroporto.

Segundo Laurentino Bonetti, operador do aeroporto, futuras ampliações serão realizadas, e entre elas está previsto o fornecimento de sinal para internet sem fio.

Figura 22. Saguão público

7.4 APLICAÇÃO DE *HOTSPOT* : E-MIX LAN HOUSE

A loja E-Mix Lan House está localizada no segundo piso do shopping Della Giustina no centro da cidade de Criciúma. Ela possui o espaço de 25m^2 e conta com 12

computadores e internet turbo de 4Mb.

Em um contato que o autor fez para saber se existia interesse quanto à implantação de um *Hotspot*, foi conversado com Allan Pantzier, um dos sócios da lan house.

Ao analisar o projeto ele explicou que a loja estará mudando de local em breve. Alguns testes referentes ao alcance e à qualidade do sinal chegaram a ser realizados, porém devido à mudança em questão o projeto foi protelado para o segundo semestre do ano de 2008.

7.5 ESTUDO DE CASO: USEALL SOFTWARE

Os itens anteriores objetivaram demonstrar possíveis locais onde estão ou seriam instalados pontos de acesso à Internet. Neste item, demonstra-se a instalação de um ponto de acesso (*hotspot*) utilizando a tecnologia PoE na empresa Useall Software.

A utilização do *Hotspot* juntamente com o PoE irá resolver um problema que ocorre na Useall, onde o salão de festas que é utilizado para palestras, reuniões com os clientes e demonstrações dos produtos não possui nenhum ponto de acesso à Internet.

7.5.1 A Empresa

Fundada em Abril do ano de 2000, sua primeira sede situava-se no distrito do Rio Maina, em uma pequena sala anexa a uma outra empresa do ramo de informática, com cinco pessoas, as quais idealizaram e iniciaram o projeto.

Com o foco em desenvolvimento de software integrado de gestão

empresarial, atualmente atua em vários ramos como o setor de Confecção, Varejo e Atacado, Prestadoras de Serviços, Manufatura e também para Distribuidoras e Geradoras de Energia Elétrica.

Em Fevereiro de 2006, mudou-se para uma nova sede, apresentada na Figura 23, desta vez própria, construída no bairro Santa Bárbara. Atualmente são quatro diretores e conta com um quadro de setenta colaboradores.

Figura 23. Fachada da Empresa Useall Software

7.5.2 Porque utilizar um *Hotspot*

Pode-se observar que de 2000 para 2008 o quadro de funcionários aumentou, desta forma um maior controle no que se refere ao acesso à internet foi instalado

Diante deste controle, uma das soluções foi disponibilizar para os

colaboradores um computador que pudesse conectar-se à rede mundial de computadores. Esta máquina localiza-se na biblioteca, no segundo pavimento da construção e não pertence à rede interna da empresa (alguns computadores pertencentes à esta rede possuem o acesso liberado, sendo que o controle dos mesmos é feito por MAC[11]), tendo assim um maior controle.

Desta maneira, os recursos disponibilizados não atendem à demanda, ocasionando em alguns momentos uma considerável aglomeração de pessoas para acessarem a rede. Considerando que vários colaboradores possuem notebooks, optou-se então por realizar a implantação de um *hotspot* neste local.

7.5.3 Implantação do *Hotspot*

Para a concretização desta solução foi necessária a aquisição de alguns equipamentos, como o ponto de acesso. Pelo fato de não haver nenhum ponto de rede, não haver tomadas elétricas próximas ao forro no salão de festas, a compra do equipamento foi estudada, pois ele deveria ter um preço acessível, que oferecesse segurança e que suportasse o padrão 802.3af ratificado pela IEEE. O resultado foi a compra do equipamento WAP200 do fabricante Linksys e o injetor modelo TPE-101I(A) do fabricante Trendnet.

7.5.3.1 Equipamentos Adquiridos

Ambos os equipamentos foram adquiridos pelo autor em 2007. A antena pode ser observada na Figura 24. As Figuras 25 e 26 mostram algumas das principais

---

[11] Código único, não pode haver dois iguais, portanto cada placa de rede possui o seu.

telas de configuração da antena.

Figura 24. Ponto de Acesso WAP200

Na Figura 25, estão os campos que deverão ser configurados pelo usuário responsável por inserir o equipamento na rede. Deve-se então fornecer os dados referentes ao nome do dispositivo e o IP. Os campos referente ao IP, máscara de sub-rede, gateway e DNS são habilitados caso a configuração seja manual, mas pode-se utilizar estas configurações automaticamente. Na Figura 26 deve-se configurar qual o padrão wireless utilizado como 802.11b, 802.11g ou ambos, a freqüência e o nome da rede a ser criada.

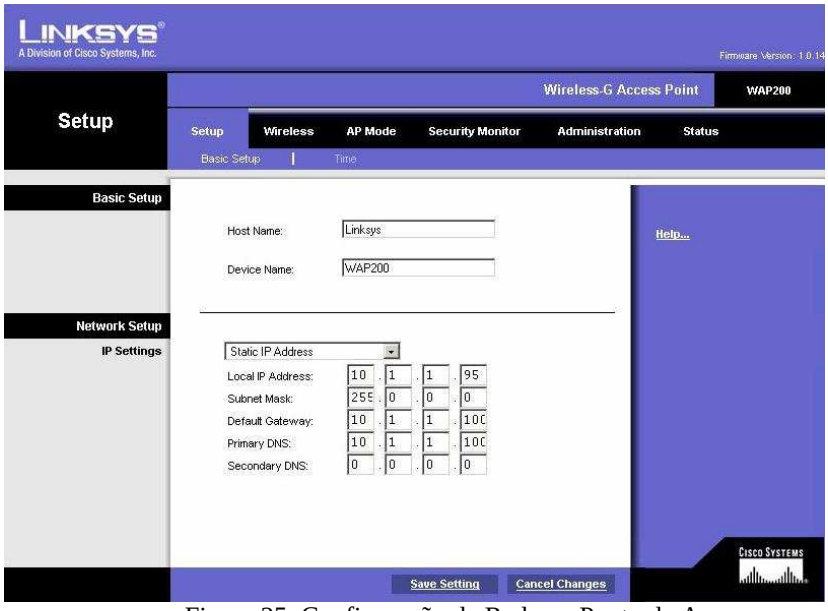

Figura 25. Configuração da Rede no Ponto de Acesso

O outro equipamento adquirido e utilizado para ligar e transferir os dados para o ponto de acesso por meio de um único cabo é o injetor TPE-101I(A), conforme a Figura 27.

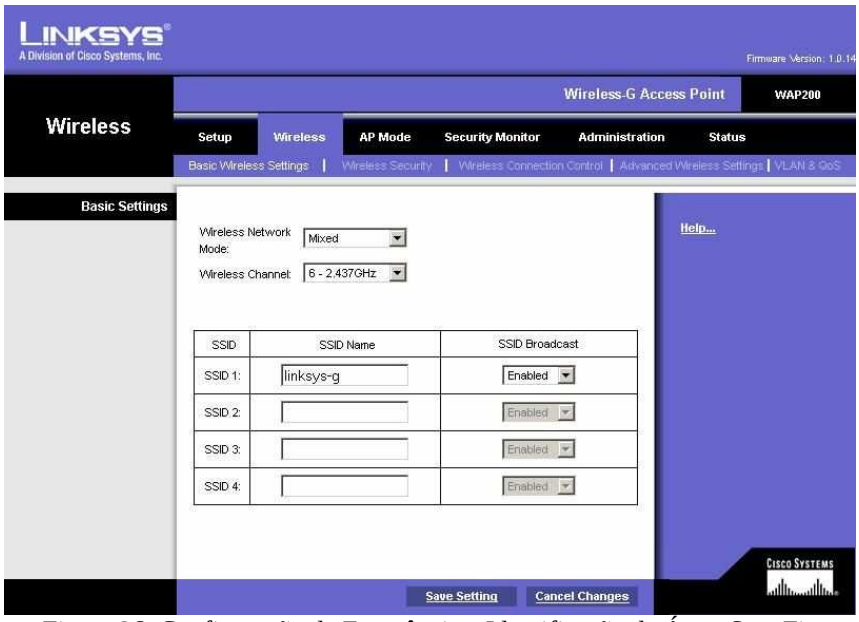

Figura 26. Configuração da Freqüência e Identificação da Área Sem Fio

Figura 27. Injetor

7.5.3.2 Local

O salão de festas da empresa situa-se no último pavimento do prédio, conforme a Figura 28. O motivo de utilizar o ponto de acesso PoE deu-se pelo fato do local de sua instalação não possuir nenhum ponto de rede Ethernet.

Figura 28. Salão de Festas

Por questões estéticas decidiu-se pela não realização de obras civis para a instalação de tomadas elétricas. Na Figura 29 pode-se visualizar onde está a tomada elétrica mais próxima do ponto de acesso.

Figura 29. Ponto de Acesso no Salão de Festas

Desta forma o custo foi apenas com uma pessoa responsável por levar o cabo de rede até o dispositivo wireless. O hack no qual está inserido o injetor encontra-se no andar abaixo do salão de festas e pode ser visualizado na Figura 30. O modelo de como ficaram interconectados os equipamentos da rede encontra-se também na Figura 31. O injetor recebe um cabo de dados *Ethernet*, um outro para a alimentação de energia e une ambos para enviá-los por meio de um único cabo, que irá chegar no ponto de acesso PoE.

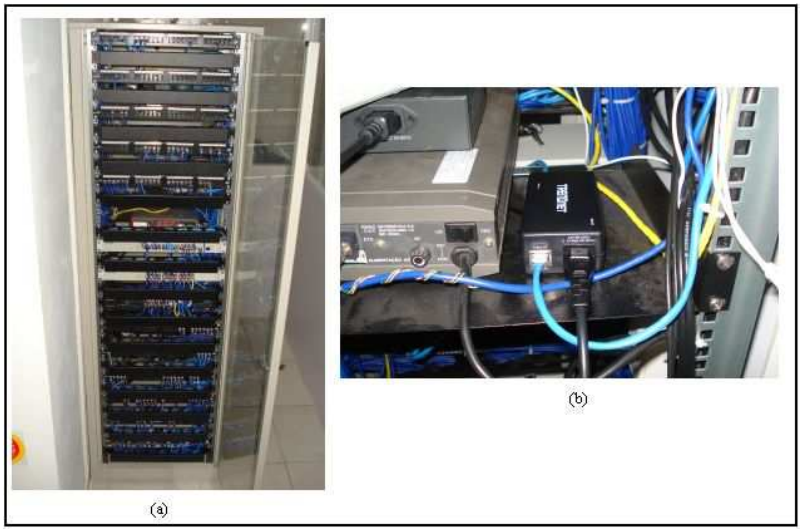

Figura 30. (a) Hack (b) Injetor

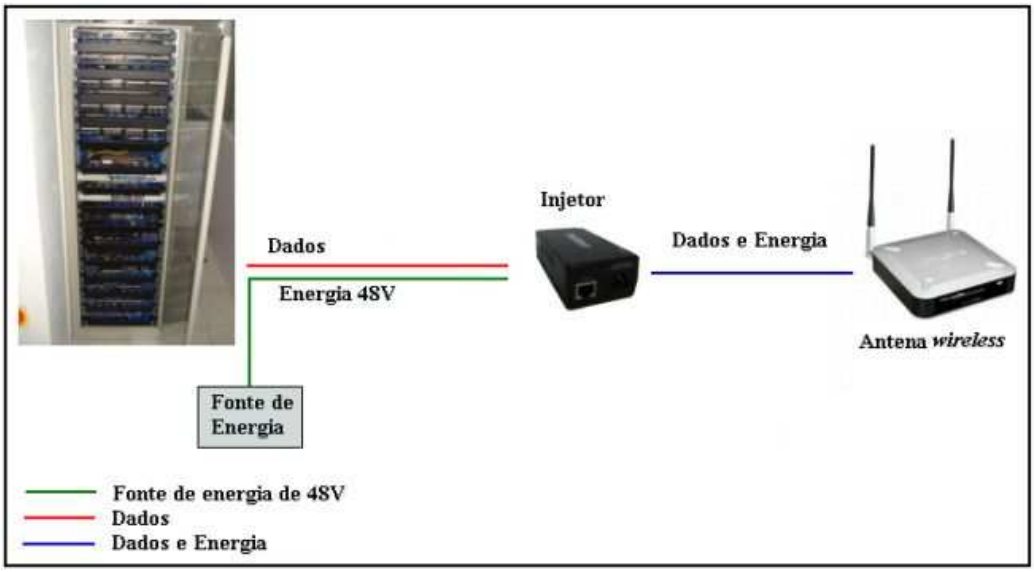

Figura 31. Solução Implantada na Useall Software

7.5.3.3 Análise de Custo

Com a solução no item anterior apresentado, procurou-se levantar em valores, qual o investimento para sua implantação. A Tabela 3, mostra o total dos gastos com produtos e serviços para a utilização do *Hotspot* na Useall Software.

Tabela 3. Demonstrativo de custo

Produto/Serviço	Custo
Injetor PoE TPE-101I(A)	R$ 224,89
Linksys Access Poit WAP200	R$ 635,01
25 metros de cabo par trançado	R$ 37,50
2 conectores RJ-45 macho	R$ 1,00
Assistência Técnica	R$ 58,00
Total	R$ 956,40

É importante ressaltar que o custo do *hotspot* em si pode ser considerado alto quando comparado a outros equipamentos que não usam a tecnologia PoE, porém este custo é minimizado quando considerada a não realização de obras civis necessárias para sua instalação.

7.5.3.4 Como Utilizar

Para se conectar ao ponto de acesso é necessário possuir um equipamento compatível com o padrão 802.11g. Sabe-se que existem duas redes na empresa, onde uma é interna e outra externa usada exclusivamente para o acesso à internet. A primeira rede está na faixa de IP 192.168.0.XXX e a segunda na faixa 10.1.1.XXX conforme mostra a Figura 32. Nem todos os IP's estão liberados para acessar todos os sites na rede referente à Internet, por isso é necessário configurá-lo de acordo com o IP livre para isso, caso contrário o usuário irá conectar-se somente nos sites sem restrições.

Independentemente da rede na qual o equipamento está inserido, o proxy do navegador de internet deve estar configurado para utilizar o IP 192.168.0.200 e porta 3128, conforme na Figura 33.

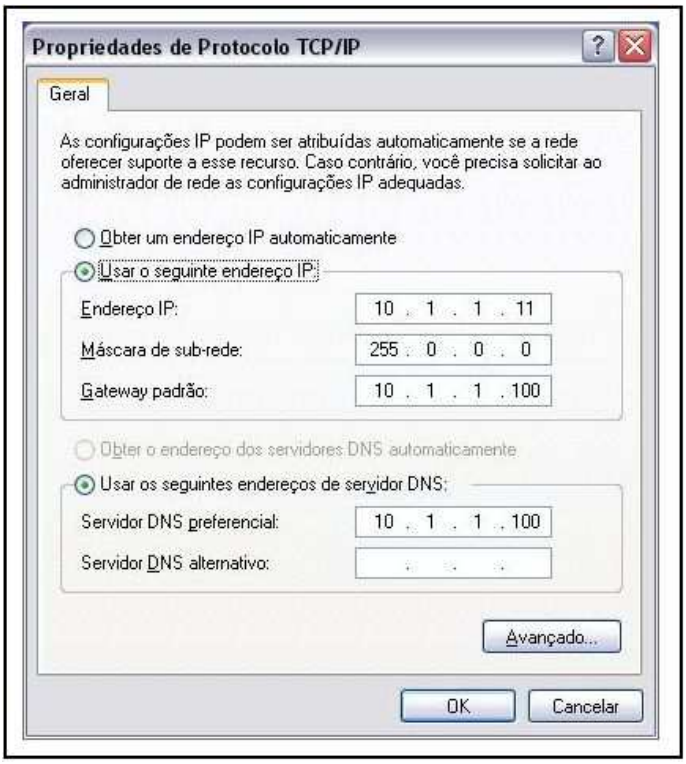

Figura 32. Configuração da Placa de Rede Sem Fio

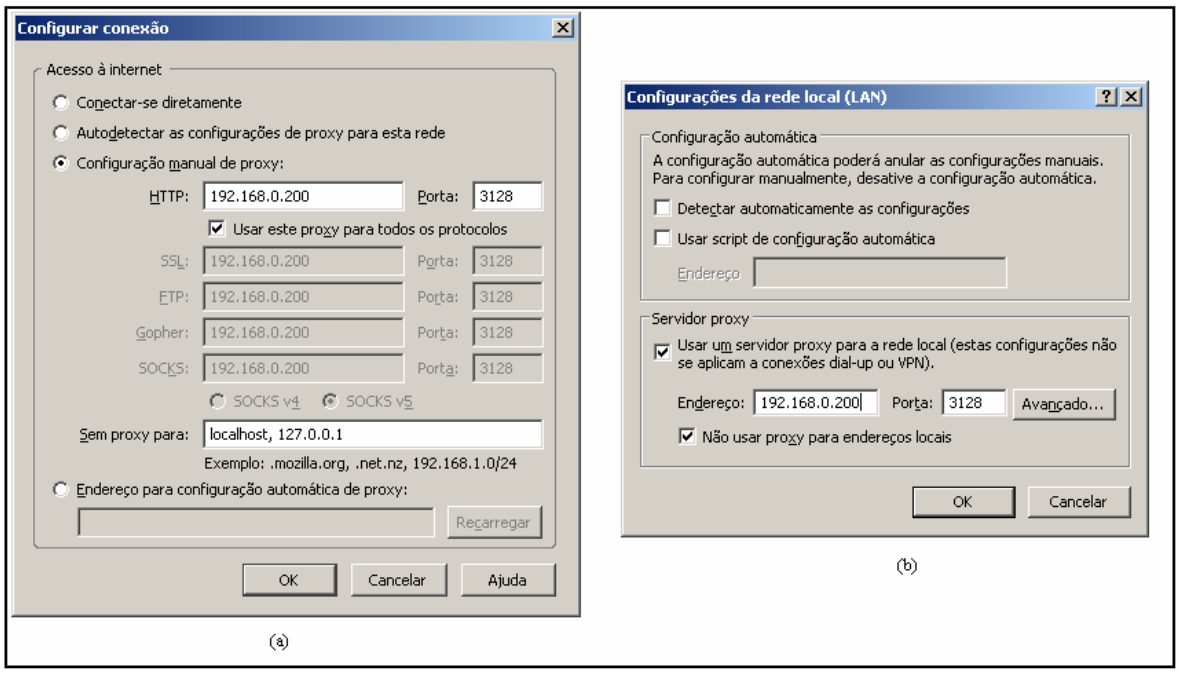

Figura 33. Configuração Proxy (a) Mozilla Firefox (b) Internet Explorer

7.5.3.5 Qualidade do sinal

Utilizando um dispositivo portátil (PDA), foi possível verificar a qualidade do sinal fornecido, por meio do indicador digital existente no equipamento. Isto pode ser visualizado na Tabela 4.

Tabela 4. Qualidade do Sinal

Distância (m)	Qualidade do Sinal
10	Excelente
25	Excelente
50	Bom
80	Razoável
110	Fraca

Cabe ressaltar que estes resultados foram obtidos considerando-se a distância em relação ao ponto central e a obstáculos como móveis, paredes de alvenaria e equipamentos de informática.

CONCLUSÃO

Este trabalho possibilitou um envolvimento com diversos conceitos e tecnologias, entre elas as redes *wireless* e o padrão 802.3af (PoE). Nota-se a cada dia um crescimento do número de pessoas conectadas à Internet, e com isso a necessidade de criar novas alternativas para acessá-la.

Diante disto, a implantação de um *hotspot* baseado na tecnologia PoE possibilitou à empresa Useall Software resolver um problema relativo ao acesso à Internet de forma rápida e de qualidade.

Alguns pontos podem ser estudados no futuro como o desenvolvimento de mecanismos de segurança para evitar invasões na rede da empresa por usuários não habilitados. Com o conhecimento adquirido, pode-se também dar continuidade e implantar este serviço nos locais onde o estudo de caso foi apenas teórico.

REFERÊNCIAS

AMARAL, Bruno Marques; MAESTRELLI, Marita. **Segurança em Redes Wireless 802.11.** Rio de Janeiro: CBPF, 2004. Disponível em: ftp://ftp2.biblioteca.cbpf.br/pub/apub/2003/nt/nt_zip/nt00303.pdf Acessado em: 07/09/2007

BARCELOS, Joao Paulo Malheiro de; GONÇALVES, Raphael Guimarães; ALVES JUNIOR, Nilton. O Padrão 802.11. Rio de Janeiro: CBPF, 2003. Disponível em: ftp://ftp2.biblioteca.cbpf.br/pub/apub/2003/nt/nt_zip/nt00303.pdf Acessado em: 07/09/2007

COMER, Douglas; STEVENS, David L. Interligação em rede com **TCP**/IP. Rio de janeiro: Ed. Campus, 1999.

CRICIUMA SHOPPING. Site Oficial do Criciúma Shopping. Disponível em: www.criciumashopping.com.br Acessado em: 18/03/2008.

CYCLADES. **Guia internet de conectividade.** 3.ed. São Paulo: Cyclades**,** 1997.

DUNCAN, Isabela Barreto. **Modelagem e Análise do Protocolo IEEE 802.11.** 2006. 127 f. Dissertação (Mestrado) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: http://www.land.ufrj.br/laboratory/repository/upfiles/mastersthesis/dissertacao_isabela.pdf Acessado em: 06/09/2007

ERCILIA, Maria. **A internet.** São Paulo: PubliFolha, 2000.

FERNANDES, Marcos Bortolotto. **WIMAX Redes Metropolitanas Sem Fio de Alta Velocidade:** Um estudo de caso para viabilidade e aplicação na Região Carbonífera. 2006. 80 f. Trabalho de Conclusão de Curso (Bacharel) – Escola Superior de Criciuma, Santa Catarina, 2006.

FICHTNER, Mirian. **A Rede Democrática.** VEJA, São Paulo, ano 40, n. 46, p. 122-123, 2007.

FREITAG, Juliana. **Provisão de Qualidade de Serviço em Redes IEEE 802.11.** 2004. 105 f. Dissertação (Mestrado) – Universidade Estadual de Campinas, São Paulo, 2004. Disponível em: http://libdigi.unicamp.br/document/?view=vtls000344348 Acessado em: 13/10/2007

GIMENES, Eder Coral. **Segurança de Redes Wireless.** 2005. 58 f. Trabalho de Conclusão de Curso (Técnologo) - Faculdade de Tecnologia de Mauá, São Paulo, 2005.

GRÉGIO, A .R .A. **Wireless Honeynets:** Um Modelo de Topologia para Captura e Análise de Ataques a Redes sem Fio. 2005. 57 f. Trabalho de Conclusão de Curso

(Bacharel) - Universidade Estadual Paulista Júlio de Mesquita Filho, São Paulo, 2005. Disponível em: http://www.acmesecurity.org/publicacoes/monografias/folder.2005-12-27.0965990514/acme-pf-2004-andre-final.pdf Acessado em: 04/10/2007

GREGO, Mauricio. **VPN em Hotspot.** INFO Exame, São Paulo, ano 20, n. 249, p. 30-31, 2006.

GRÜNEWALD, Marcus Albert. **Redes sem fio** – Tecnologia, Segurança e Usabilidade. 2005. 119 f. Pós-Graduação (Especialização) - Faculdade de Informática e Administração Paulista, São Paulo, 2005.

GUIZZO, Erico. **Internet :** o que é, o que oferece, como conectar-se. São Paulo: Ática, 2002.

HAYDEN, Matt. **Aprenda em 24 horas redes.** 2.ed. Rio de Janeiro: Campus, 1999.

IEEE. **Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.** Nova Iorque: IEEE, 2003**.**

INFRAERO. **Site do Aeroporto Diomício Freitas.** Disponível em: www.infraero.gov.br/aero_prev_home.php?ai=446 Acessado em: 22/03/2008

JIWIRE. **Site Localizador de *Hotspots*.** Disponível em: http://www.jiwire.com Acessado em: 01/03/2008.

JUNIOR, C. A. C; BRABO, G. S; AMORAS, R. A. S. **Segurança em redes wireless padrão IEEE 802.11b:** Protocolos WEP, WPA e análise de desempenho. 2004. 78 f. Trabalho de Conclusão de Curso (Bacharel) - Universidade da Amazônia, Pará, 2004. Disponível em: http://www.cci.unama.br/margalho/portaltcc/tcc2004/carlosgustavo&romulo.pdf Acessado em: 29/09/2007.

KUROSE**,** James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down.** 3. ed São Paulo: Pearson Addison Wesley, 2006.

LACERDA, Pablo de Souza. **Análise de Segurança em Redes Wireless 802.11x.** 2007. 49 f. Trabalho de Conclusão de Curso (Bacharel) - Universidade Federal de Juiz de Fora, Minas Gerais, 2007. Disponível em: http://www.ice.ufjf.br/index2.php?option=com_docman&task=doc_view&gid=5&Itemid=74. Acessado em: 27/09/2007

LEAL, David. **WiFi Hotspots: Como Encontrar Redes Wifi E Comunidades De Partilha Wifi - Mini-Guia**. 2007. Disponível em: http://www.masternewmedia.org/pt/colaboracao_on-line/wifi-networks/wifi-hotspots-como-encontrar-redes-wifi-e-comunidades-de-partilha-wifi-20071021.htm Acessado em: 01/03/2008.

LIMA JÚNIOR, Almir Wirth. **Tecnologias de redes & comunicação de dados**. Rio de Janeiro: Alta books, 2002.

MATOS, Luiz. **Guia profissional e redes wireless.** São Paulo: Digerati Books, 2005.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware.** São Paulo: Novatec, 2005.

MURHAMMER, Martin W. et al. **TCP/IP**: tutorial e técnico**.** São Paulo: Makron Books, 2000.

POWER OVER ETHERNET. **IEEE 802.3af Power Over Ethernet:** A Radical New Technology. 2003. Disponível em: http://www.poweroverethernet.com/articles.php?article_id=52 Acessado em: 03/10/2007.

RUFINO, Nelson. **Segurança em Redes sem Fio.** 2 ed. São Paulo: Novatec, 2005.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de cumputadores das LANs, MANs e WANs às Redes ATM.** 6. ed. Rio de Janeiro: Campus, 1995.

SOUSA, Maxuel Barbosa de. **Wireless:** Sistema de Rede Sem Fio. Rio de Janeiro: Brasport, 2002.

SPURGEON, Charles E. **Ethernet**: o guia definitivo. Rio de Janeiro: Campus, 2000.

TANENBAUM**,** Andrew S. **Redes de computadores.** 5. ed. Rio de Janeiro: Campus, 2003.

THOMAS, Robert M. **Introdução às redes locais.** Rio de Janeiro: Makron Books, 1997.

TORRES**,** Gabriel. **Redes de computadores:** curso completo. Rio de Janeiro: Axcel Books do Brasil, 2001.

TRENDNET INJECTOR. **Power Over Ethernet (PoE) Injector.** 2005. Disponível em: http://www.trendnet.com.au/pages/productsInformation.aspx?C=39&P=TPE-101I Acessado em: 12/10/2007

TRENDNET SPLITTER. **Power Over Ethernet (PoE) Splitter.** 2005. Disponível em: http://www.trendnet.com.au/pages/productsInformation.aspx?P=TPE-102S Acessado em: 12/10/2007

UNESC. **Site oficial da Univerdidade do Extremo sul Catarinense.** Disponível em: www.unesc.net Acessado em: 27/04/2008

VIEIRA, Eduardo. **Os bastidores da internet no Brasil.** Barueri, SP: Manole, 2003.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores: configuração, manutenção e expansão.** São Paulo: Makron Books, 2000.

BIBLIOGRAFIA COMPLEMENTAR

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança:** o guia oficial RSA. Rio de Janeiro: Elsevier, 2002.

CARRIÓN, Demetrio de Souza Diaz. **Implementação De Um Ponto De Acesso Seguro Para Redes 802.11b Baseado No Sistema Operacional OPENBSD. 2003.** 58 f. Trabalho de Conclusão do Curso (Engenharia) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2003. Disponível em: http://www.lockabit.coppe.ufrj.br/downloads/academicos/implementacao_80211.pdf Acessado em: 15/10/2007

DULANEY, Emmett et al. **Desvendando o TCP/IP:** métodos de instalação, manutenção e implementação de redes TCP/IP. 4.ed Rio de Janeiro: Campus, 1997.

DORNAN, Andy. **Wireless communication:** o guia essencial de comunicação sem fio. Rio de Janeiro: Campus, 2001.

FARREL, Adrian. **A internet e seus protocolos:** uma análise comparativa. Rio de Janeiro: Elsevier, 2005.

MICROSOFT. **Decisão sobre uma Estratégia de Rede sem Fio Protegida.** 2004. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx Acessado em: 29/09/2007.

MINOLI, Daniel. **Hotspot Networks: WiFi for Public Access Locations.** McGraw-Hill, Professional. 2002.

PETERSON, Larry L; DAVIE, Bruce S. **Redes de computadores:** uma abordagem de sistemas. Rio de Janeiro: Elsevier, 2004.

TEIXEIRA JUNIOR, José Helvécio. **Redes de computadores:** serviços, administração e segurança. São Paulo: Makron Books, 1999.

APÊNDICE A – ARTIGO

Estudo de Caso Para Instalação de Hotspots Utilizando a Tecnologia Power Over Ethernet para Fornecimento de Energia nos Dispositivos Wireless

Alex Cardoso de Jesus [1], Arildo Sônego[1]

[1] Universidade do Extremo Sul Catarinense (UNESC)
Caixa Postal 3167 – CEP. 88806-000 – Criciúma, SC, Brasil

alexkardozo@gmail.com, arildo@unesc.net

Abstract. *This article presents the construction of a Hotspot using the Power Over Ethernet technology to provide energy for the wireless antenna. After the technologies research, the Hotspot was deployed in the Useall Software company to provide their employees an alternative Internet access.*

Resumo. *O presente artigo apresenta a construção de um Hotspot utilizando a tecnologia Power Over Ethernet para fornecer energia para a antena wireless. Após a pesquisa das tecnologias foi realizada a implantação do Hotspot na empresa Useall Software, para disponibilizar aos seus colaboradores uma alternativa de acesso à Internet.*

1. Introdução

As redes de computadores são utilizadas em locais distintos, como por exemplo, em ambientes comerciais, domésticos, instituições de ensino, entre outros e têm como objetivo interligar os componentes pertencentes a ela (TANENBAUM, 2003). Desta forma, muitas técnicas relacionadas à conectividade foram desenvolvidas para que de alguma forma algum processo ou serviço oferecido fosse aprimorado trazendo algum benefício. Este trabalho irá utilizar duas destas técnicas, são elas: as Redes *Wireless* e a tecnologia *Power Over Ethernet* (PoE).

A Rede *Wireless* é uma forma de tornar a interligação dos computadores algo mais flexível por meio da mobilidade, pois não são utilizados fios para conectar os computadores, mas sim um dispositivo no computador e outro chamado de ponto de acesso, que irá fornecer a permissão e acesso deles na rede (GREGO, 2006). O *Power Over Ethernet* é a técnica responsável por transmitir em um único cabo par-trançado (mais utilizado nas redes de computadores atualmente) energia elétrica e os dados ao ponto de acesso (IEEE, 2003).

O presente artigo apresenta uma solução para a Useall Software por meio das duas tecnologias supracitadas. No salão de festas da empresa foi implantado um *Hotspot* com o PoE, para disponibilizar aos seus colaboradores uma alternativa para acessar à Internet, pois até o presente momento há somente uma máquina para este fim, o que é considerado pouco quando comparado com a quantidade de usuários.

Outra vantagem é que com isso torna-se mais fácil realizar uma reunião,

treinamento, palestra ou outro evento semelhante, onde seja necessário acessar a rede interna da empresa. Para isto foi necessário, além do estudo teórico para a implantação, adquirir o Ponto de Acesso e o Injetor PoE, em seguida compreender seu funcionamento e configurá-los. Por fim apresentam-se os testes realizados, satisfação e análise de custo.

2. Estudo de Caso: Useall Software

Os itens anteriores objetivaram demonstrar possíveis locais onde estão ou seriam instalados pontos de acesso à Internet. Neste item, demonstra-se a instalação de um ponto de acesso (*hotspot*) utilizando a tecnologia PoE na empresa Useall Software.

A utilização do *Hotspot* juntamente com o PoE irá resolver um problema que ocorre na Useall, onde o salão de festas que é utilizado para palestras, reuniões com os clientes e demonstrações dos produtos não possui nenhum ponto de acesso à Internet.

2.1 A Empresa

Fundada em Abril do ano de 2000, sua primeira sede situava-se no distrito do Rio Maina, em uma pequena sala anexa a uma outra empresa do ramo de informática, com cinco pessoas, as quais idealizaram e iniciaram o projeto.

Com o foco em desenvolvimento de software integrado de gestão empresarial, atualmente atua em vários ramos como o setor de Confecção, Varejo e Atacado, Prestadoras de Serviços, Manufatura e também para Distribuidoras e Geradoras de Energia Elétrica.

Em Fevereiro de 2006, mudou-se para uma nova sede, apresentada na Figura 1, desta vez própria, construída no bairro Santa Bárbara. Atualmente são quatro diretores e conta com um quadro de setenta colaboradores.

Figura 1. Fachada da Empresa Useall Software

2.2 Porque utilizar um Hotspot

Pode-se observar que de 2000 para 2008 o quadro de funcionários aumentou, desta forma um maior controle no que se refere ao acesso à internet foi instalado

Diante deste controle, uma das soluções foi disponibilizar para os colaboradores um computador que pudesse conectar-se à rede mundial de computadores. Esta máquina localiza-se na biblioteca, no segundo pavimento da construção e não pertence à rede interna da empresa (alguns computadores pertencentes à esta rede possuem o acesso liberado, sendo que o controle dos mesmos é feito por MAC), tendo assim um maior controle.

Desta maneira, os recursos disponibilizados não atendem à demanda, ocasionando em alguns momentos uma considerável aglomeração de pessoas para acessarem a rede. Considerando que vários colaboradores possuem notebooks, optou-se então por realizar a implantação de um *hotspot* neste local.

2.3 Implantação do Hotspot

Para a concretização desta solução foi necessária a aquisição de alguns equipamentos, como o ponto de acesso. Pelo fato de não haver nenhum ponto de rede, não haver tomadas elétricas próximas ao forro no salão de festas, a compra do equipamento foi estudada, pois ele deveria ter um preço acessível, que oferecesse segurança e que suportasse o padrão 802.3af ratificado pela IEEE. O resultado foi a compra do equipamento WAP200 do fabricante Linksys e o injetor modelo TPE-101I(A) do fabricante Trendnet.

2.3.1 Equipamentos Adquiridos

Ambos os equipamentos foram adquiridos pelo autor em 2007. A antena pode ser observada na Figura 2. A Figura 3 mostra algumas das principais configurações da antena.

Figura 2. Ponto de Acesso WAP200

Na Figura 3, estão os campos que deverão ser configurados pelo usuário responsável por inserir o equipamento na rede. Deve-se então fornecer os dados referentes ao nome do dispositivo e o IP. Os campos referente ao IP, máscara de sub-rede, gateway e DNS são habilitados caso a configuração seja manual, mas pode-se utilizar estas configurações automaticamente.

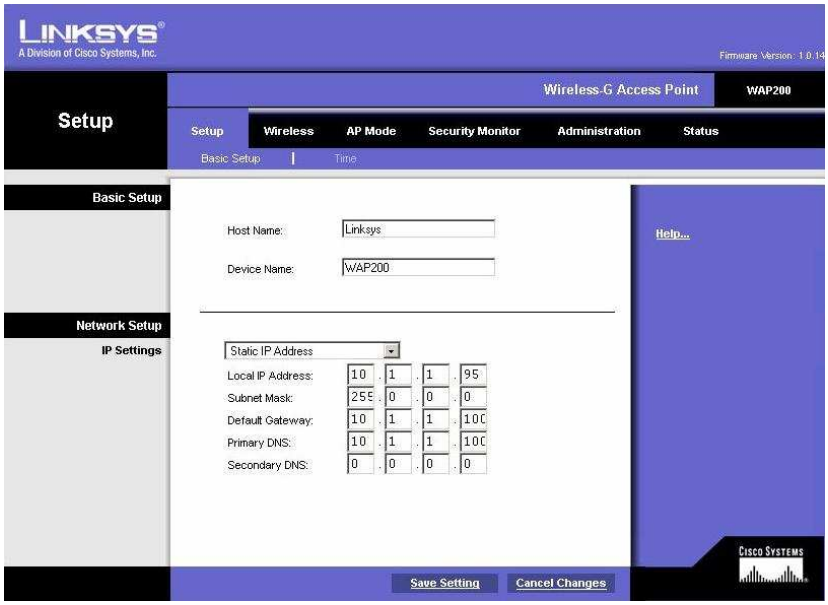

Figura 3. Configuração da Rede no Ponto de Acesso

O outro equipamento adquirido e utilizado para ligar e transferir os dados para o ponto de acesso por meio de um único cabo é o injetor TPE-101I(A), conforme a Figura 4.

Figura 4. Injetor

2.3.2 Local

O salão de festas da empresa situa-se no último pavimento do prédio, conforme a Figura 5. O motivo de utilizar o ponto de acesso PoE deu-se pelo fato do local de sua instalação não possuir nenhum ponto de rede Ethernet.

Por questões estéticas decidiu-se pela não realização de obras civis para a instalação de tomadas elétricas. Na Figura 6 pode-se visualizar onde está a tomada elétrica mais próxima do ponto de acesso.

Figura 5. Salão de Festas

Figura 6. Ponto de Acesso no Salão de Festas

Desta forma o custo foi apenas com uma pessoa responsável por levar o cabo de rede até o dispositivo wireless. O hack no qual está inserido o injetor encontra-se no andar abaixo do salão de festas e pode ser visualizado na Figura 7. O modelo de como ficaram interconectados os equipamentos da rede encontra-se também na Figura 8. O injetor recebe um cabo de dados *Ethernet*, um outro para a alimentação de energia e une ambos para enviá-los por meio de um único cabo, que irá chegar no ponto de acesso PoE.

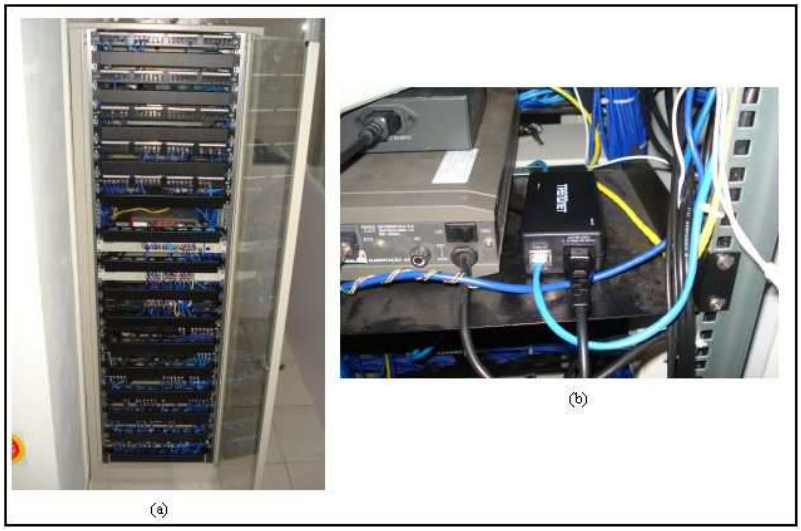

Figura 7. (a) Hack (b) Injetor

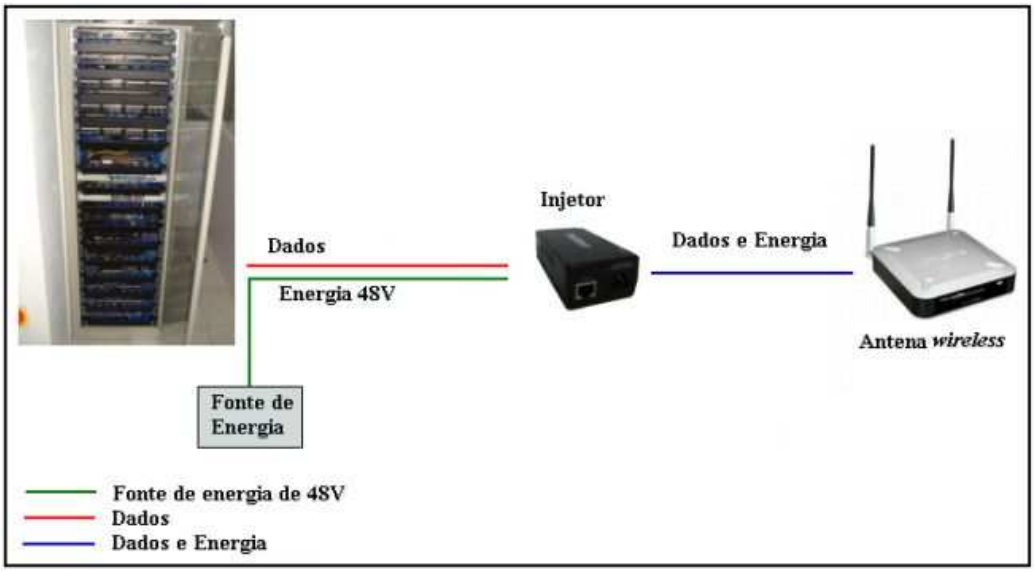

Figura 8. Solução Implantada na Useall Software

2.3.3 Análise de Custo

Com a solução no item anterior apresentado, procurou-se levantar em valores, qual o investimento para sua implantação. A Tabela 1, mostra o total dos gastos com produtos e serviços para a utilização do *Hotspot* na Useall Software.

Tabela 1. Demonstrativo de custo

Produto/Serviço	Custo
Injetor PoE TPE-101I(A)	R$ 224,89
Linksys Access Poit WAP200	R$ 635,01
25 metros de cabo par trançado	R$ 37,50
2 conectores RJ-45 macho	R$ 1,00
Assistência Técnica	R$ 58,00
Total	R$ 956,40

É importante ressaltar que o custo do *hotspot* em si pode ser considerado alto quando comparado a outros equipamentos que não usam a tecnologia PoE, porém este custo é minimizado quando considerada a não realização de obras civis necessárias para a sua instalação.

2.3.4 Como Utilizar

Para se conectar ao ponto de acesso é necessário possuir um equipamento compatível com o padrão 802.11g. Sabe-se que existem duas redes na empresa, onde uma é interna e outra externa usada exclusivamente para o acesso à internet. A primeira rede está na faixa de IP 192.168.0.XXX e a segunda na faixa 10.1.1.XXX conforme mostra a Figura 9. Nem todos os IP's estão liberados para acessar todos os sites na rede referente à Internet, por isso é necessário configurá-lo de acordo com o IP livre para isso, caso contrário o usuário irá conectar-se somente nos sites sem restrições.

Independentemente da rede na qual o equipamento está inserido, o proxy do navegador de internet deve estar configurado para utilizar o IP 192.168.0.200 e porta 3128, conforme na Figura 10.

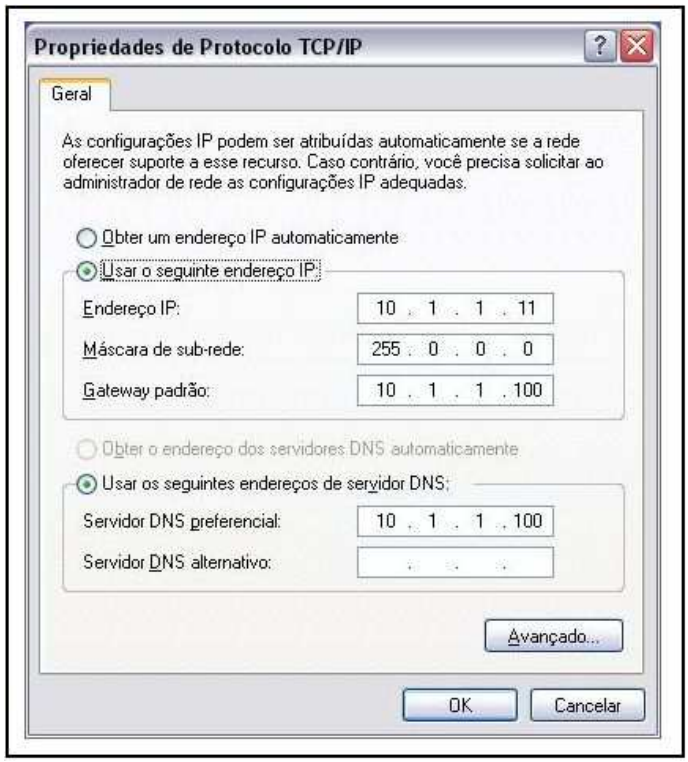

Figura 9. Configuração da Placa de Rede Sem Fio

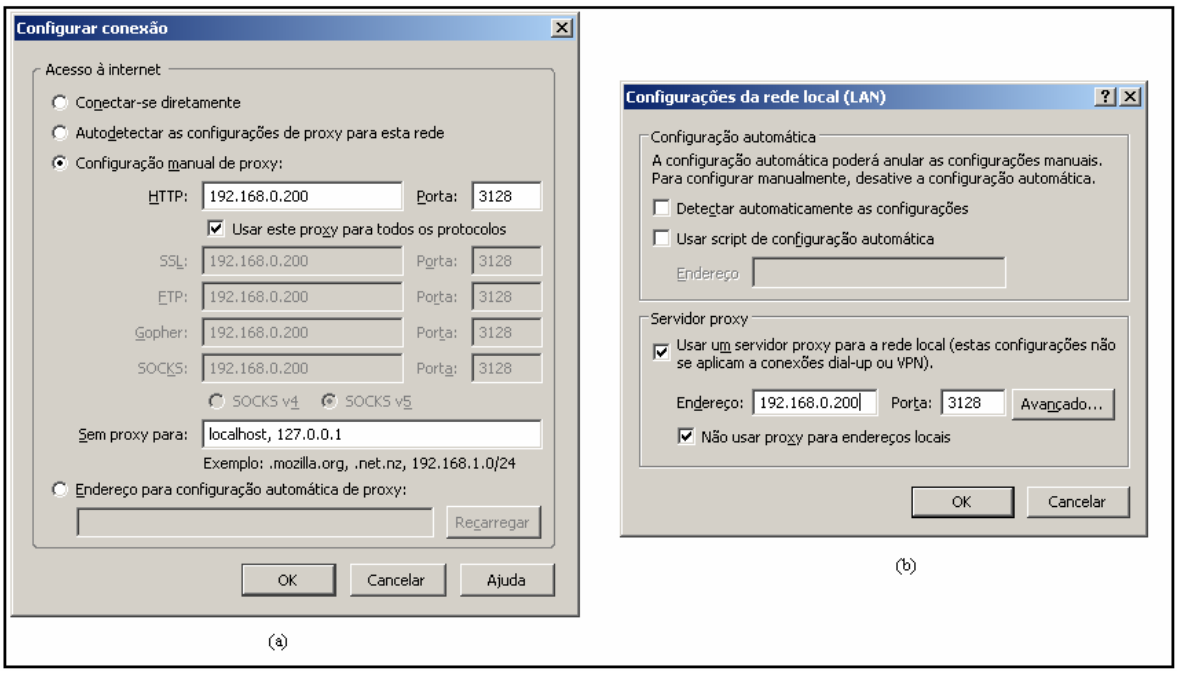

Figura 10. Configuração Proxy (a) Mozilla Firefox (b) Internet Explorer

2.3.5 Qualidade do sinal

Utilizando um dispositivo portátil (PDA), foi possível verificar a qualidade do sinal fornecido, por meio do indicador digital existente no equipamento. Isto pode ser visualizado na Tabela 2.

Tabela 2. Qualidade do Sinal

Distância (m)	Qualidade do Sinal
10	Excelente
25	Excelente
50	Bom
80	Razoável
110	Fraca

Cabe ressaltar que estes resultados foram obtidos considerando-se a distância em relação ao ponto central e a obstáculos como móveis, paredes de alvenaria e equipamentos de informática.

3. Conclusão

Este trabalho possibilitou um envolvimento com diversos conceitos e tecnologias, entre elas as redes *wireless* e o padrão 802.3af (PoE). Nota-se a cada dia um crescimento do número de pessoas conectadas à Internet, e com isso a necessidade de criar novas alternativas para acessá-la.

Diante disto, a implantação de um *hotspot* baseado na tecnologia PoE possibilitou à empresa Useall Software resolver um problema relativo ao acesso à Internet de forma rápida e de qualidade.

Alguns pontos podem ser estudados no futuro como o desenvolvimento de mecanismos de segurança para evitar invasões na rede da empresa por usuários não habilitados. Com o conhecimento adquirido, pode-se também dar continuidade e implantar este serviço nos locais onde o estudo de caso foi apenas teórico.

4. Referência

GREGO, Mauricio. **VPN em Hotspot.** INFO Exame, São Paulo, ano 20, n. 249, p. 30-31, 2006.

IEEE. **Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.** Nova Iorque: IEEE, 2003**.**

TANENBAUM**,** Andrew S. **Redes de computadores.** 5. ed. Rio de Janeiro: Campus, 2003.