UNIVERSIDADE DO OESTE DE SANTA CATARINA

CAMPUS DE SÃO MIGUEL DO OESTE

AMAURI TIAGO MARX

DO PROJETO À IMPLANTAÇÃO DE REDES SEM FIO:
Um Estudo de Caso

SÃO MIGUEL DO OESTE

2008

AMAURI TIAGO MARX

DO PROJETO À IMPLANTAÇÃO DE REDES SEM FIO:

Um Estudo de Caso

Trabalho de Monografia apresentado ao curso de Sistemas de Informação da Universidade do Oeste de Santa Catarina – Campus de São Miguel do Oeste como requisito parcial à obtenção do grau de Especialista em Sistemas de Informação.

Orientador: Prof. Claunir Pavan

SÃO MIGUEL DO OESTE

2008

Dedico este trabalho a minha família e namorada, os quais sempre me ampararam.

AGRADECIMENTOS

A Deus, por mais essa conquista em minha vida.

Ao grande mestre, Claunir Pavan, pela amizade, pelo empenho e dedicação conferidos a este projeto e principalmente por ter confiado em meu esforço.

À minha família, por sempre amparar minhas decisões e incentivar meu estudo.

À minha namorada, pelo apoio incondicional.

Ao meu grande amigo e colega de trabalho Fabrício Paloschi, o qual teve enorme participação na personalização dos códigos e telas do portal de autenticação.

A todas as pessoas que contribuíram para a conclusão deste trabalho.

A água que não corre forma um pântano;
a mente que não trabalha forma um tolo.

(Victor Hugo)

RESUMO

A funcionalidade das redes sem fio, aliado ao baixo custo para implantação e gestão, é cada vez mais empregada nas organizações. Esta monografia descreve o projeto e a implantação de uma rede sem fio considerando o campus de São Miguel do Oeste da Universidade do Oeste de Santa Catarina. Baseado na metodologia de estudo de caso exploratório descritivo, inicialmente, descreve-se um histórico acerca das comunicações sem fio, bem como conceitos e princípios das redes sem fio conforme padrões internacionais. Posteriormente, apresenta-se, em detalhes, o estudo de caso da implantação da rede sem fio no campus. A distribuição dos pontos de acesso de forma que haja intersecção entre o raio de alcance dos pontos adjacentes oferece portabilidade, já que o usuário poderá mover-se pelo campus sem perder a conexão com a rede, bem como sobrevivência em caso de falha de algum ponto de acesso. Pautados nas facilidades para o usuário final, a decisão recai pela implantação da rede sem fio com sistema de autenticação por portal (*hotspot*), uma vez que elimina a necessidade de conhecimentos para configurações ou apoio técnico institucional para a obtenção da permissão de acesso.

Palavras-chave: Redes sem fio. Hotspot. Segurança de redes sem fio.

ABSTRACT

The functionality of wireless networks, allied with the low cost for network building and management, is each time more employed in the organizations. This monograph describes the project and the implantation of a wireless network considering the campus of São Miguel do Oeste of the Universidade do Oeste de Santa Catarina. Based on a descriptive exploratory case study method, initially, is described a historical about the wireless communications, as well as concepts and principles of the wireless networks in accordance with international patterns. Later, the case study of the implantation of the wireless network in the campus is described in details. The spread of access points in a way which the rays of adjacent points have an intersection between each other offers portability, that is, the user can move around the campus without losing network connection, as well as survivability in case of some access point fail. Aiming at ease of use for the end users, the implantation of the wireless networks was made with authentication through a portal system (also known as hotspot), once it eliminates the need of knowledge about configurations or institutional technical support for the access permission.

Keywords: Wireless networks. Hotspot. Wireless networks security.

LISTA DE QUADROS

LISTA DE DESENHOS

LISTA DE FOTOGRAFIAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	*Authentication, Authorization and Accounting*
AES	*Advanced Encryption Standard*
AP	*Access Point*
BSS	*Basic Service Set*
CCMP	*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
CGI	*Common Gateway Interface*
DoS	*Denial of Service*
DS	*Distribution System*
EAP	*Extensible Authentication Protocol*
EAPoL	*EAP over LAN*
ESS	*Extended Service Sets*
FCC	*Federal Communications Comission*
IBSS	*Independent Basic Service Set*
IEEE	*Institute of Eletrical and Eletronics Engineers*
ISM	*Industrial Scientific and Medical*
LAN	*Local Area Network*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MIC	*Message Integrity Check*
PAN	*Personal Area Network*
PDA	*Personal Digital Assistants*
PoE	*Power over Ethernet*
PSK	*Pre-Shared Key*
RADIUS	*Remote Authentication Dial-In User Service*
SNMP	*Simple Network Management Protocol*
SQL	*Structured Query Language*
SSID	*Service Set Identifier*
SSL	*Secure Sockets Layer*
TKIP	*Temporal Key Integrity Protocol*
U-NII	*Unlicensed National Information Infrastructure*

UNOESC	Universidade do Oeste de Santa Catarina
VLAN	*Virtual Local Area Network*
WAN	*Wide Area Network*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless Local Area Network*
WPA	*WiFi Protected Access*
WPA-PSK	*WPA-Pre Shared Key*

SUMÁRIO

1 INTRODUÇÃO

Atualmente o crescimento de aplicações para a Internet têm sido impressionante, tornando as redes de computadores recursos críticos em qualquer sistema de informação. A diversidade e facilidade na aquisição de dispositivos conectáveis em rede, devido ao seu baixo custo, influencia significativamente na forma como os negócios são hoje conduzidos.

Em centros maiores as redes sem fio de acesso livre são comuns em locais públicos – bibliotecas, parques, cafés, livrarias, hotéis. Em instituições de ensino, principalmente universidades, esta tecnologia está cada vez mais presente. A instituição disponibiliza informações de interesse do aluno (tais como calendário acadêmico, consulta de notas, situação financeira, rematrícula, troca de mensagens entre os alunos e professores, materiais de aula), além de permitir a inscrição em eventos, consultas ao acervo da biblioteca e vários outros serviços possíveis de serem oferecidos via Internet. Os professores, que antes entregavam apostilas para os alunos fotocopiarem, agora preferem disponibilizar o material para *download* a partir de um portal acadêmico, o qual ainda lhes permite fazer uso do diário de classe digital, fórum de discussão, acesso ao perfil dos alunos, dentre outros recursos. Por fim, os alunos de hoje preferem o método de acesso *on-line* à informação, uma vez que portando um computador portátil podem carregar todo o material das disciplinas.

No sentido de atender a preferência dos acadêmicos, a universidade tem interesse em prover acesso prático e fácil aos recursos de rede do campus. Contudo, o uso de laboratórios de acesso geral nem sempre atende a demanda e/ou praticidade desejada.

No caso da Universidade do Oeste de Santa Catarina (UNOESC), campus de São Miguel do Oeste, uma das soluções possíveis para prover o acesso à rede no campus é aumentar o número de equipamentos disponíveis para acesso geral. Esta alternativa exige altos custos com instalação de canaletas externas (muitos prédios não possuem dutos e caixas de passagens adequadas), cabos metálicos ou fibras ópticas, *switches*, *patch panels*, *racks*, conectores, entre outros. Além disso, esta solução não atende totalmente a mobilidade pretendida. Outra opção consiste na instalação de uma rede local sem fio (WLAN – *Wireless Local Area Network*) com abrangência em toda a área do campus universitário. Esta solução não é afetada pelas restrições impostas pela rede cabeada, tem custo inferior e possivelmente maior escalabilidade. No entanto, a instalação de redes sem fio também demanda um estudo criterioso. O gerente da rede precisa assegurar que os serviços serão providos com qualidade,

confiabilidade e segurança. Atualmente existem diversos fornecedores de produtos para redes, cada qual com um custo diferente em termos de equipamento, software de gerência e suporte.

Neste trabalho é apresentado um estudo de caso, considerando os passos desde o projeto à implantação de uma rede sem fio, na Universidade do Oeste de Santa Catarina, campus de São Miguel do Oeste. Como cumprimento dos objetivos, este trabalho apresenta uma caracterização de redes sem fio (*wireless*); a identificação de uma arquitetura com melhor custo-eficiência a ser utilizada no campus; o processo de implantação da rede sem fio no campus; procedimentos de teste, validação e monitoração da rede sem fio do campus; a identificação e estabelecimento de mecanismos de segurança inter-redes e autenticação dos usuários da rede sem fio.

A monografia está estruturada em três partes. Na primeira parte é apresentado um histórico acerca das comunicações sem fio, bem como conceitos e princípios das redes sem fio baseados nos padrões internacionais. O estudo de caso é apresentado na segunda parte. Por fim, na terceira parte são delineadas as análises e as discussões, seguidas das principais conclusões e recomendações oriundas deste estudo.

1.1 REDES DE COMPUTADORES

De forma geral, uma rede de computadores pode ser entendida como a interconexão de diversos equipamentos, com o objetivo de compartilhar recursos entre si, como arquivos de dados, impressoras, softwares e outros equipamentos. Utiliza, basicamente, três meios de comunicação: fios ou cabos de cobre, fibras ópticas e transmissão por ondas de rádio. (SOUZA, 2005).

As redes de computadores são usualmente classificadas de acordo com seu alcance (SOARES, 1997; GRÜNEWALD, 2005):

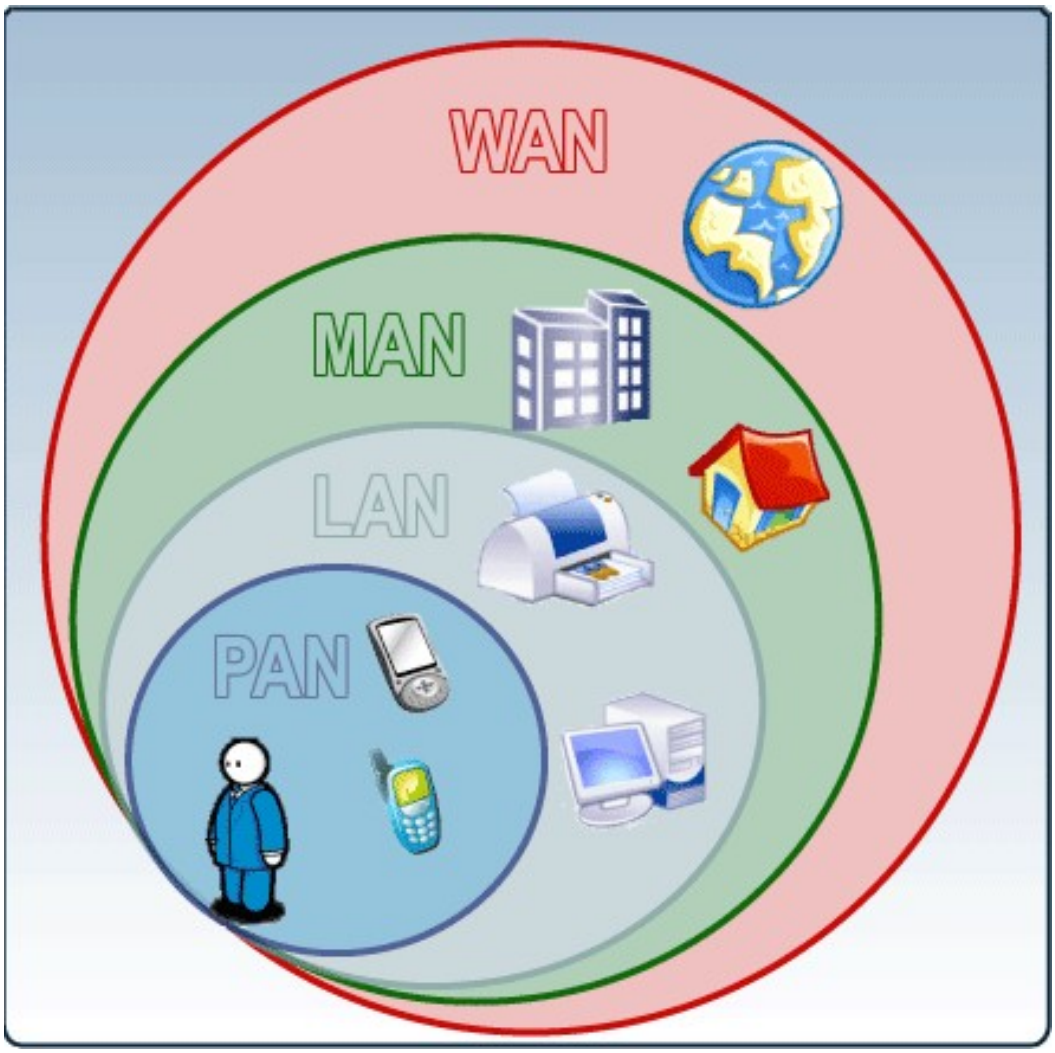
a) PAN (*Personal Area Network*) – Rede de Área Pessoal: pequeno alcance e baixo desempenho. É normalmente utilizado para a comunicação entre dispositivos pessoais, como por exemplo, a comunicação entre um PDA (*Personal Digital Assistants*) ou celular e um computador;

b) LAN (*Local Area Network*) – Rede de Área Local: rede com alcance comumente limitado à interconexão de módulos processadores (estações, servidores, impressoras, etc.) de

uma organização (escritório, escola, edifício), com a finalidade de troca e compartilhamento de informações e dispositivos periféricos;

c) MAN (*Metropolitan Area Network*) – Rede de Área Metropolitana: apresentam características semelhantes às das redes locais, porém são tipicamente empregadas para a interligação de prédios corporativos distantes (que atravessam cidades e estados);

d) WAN (*Wide Area Network*) – Rede de Longa Distância: também conhecida como rede geograficamente distribuída. Abrange uma grande área geográfica (país ou continente). Devido ao seu custo elevado, na maioria das vezes utilizam o sistema de comunicação público. Como exemplo, pode-se citar a Internet.



Desenho 1: Classificação pela abrangência das redes sem fio
Fonte: Adaptado de Rigonatti (2005).

O Desenho 1 apresenta de modo gráfico a abrangência de cada classe. A nomenclatura das redes sem fio segue o mesmo princípio. No entanto, o foco deste trabalho é totalmente voltado para redes locais sem fio (WLAN).

As redes locais sem fio foram projetadas para serem similares às redes locais, de modo que o usuário final não sofra impacto quando da sua utilização. A diferença mais expressiva é a ausência de uma ligação por fio, pois utiliza uma onda eletromagnética que se propaga no ar como meio de transmissão (RIBAS, 2002).

2 REDES SEM FIO

As redes locais sem fio são baseadas no padrão 802.11, especificado pelo *Institute of Eletrical and Eletronics Engineers* (IEEE[1]), e compostas de um conjunto de estações que se comunicam através de ondas de rádio. Os elementos de rede empregados em cada estação são determinados consoantes aos requisitos de projeto.

"Dá-se o nome de 'wireless lan' a redes locais que interligam suas estações (computadores) sem utilizar o cabeamento de cobre. A conexão entre as estações de uma rede local é efetuada por meio de radiofreqüência ou ondas infravermelhas" (SOUZA, 2005, p. 413, grifo do autor).

Neste capítulo é apresentado um breve histórico da evolução das redes sem fio, seguido pela descrição de elementos de rede e de arquiteturas possíveis. Finalmente, os modos de operação e aspectos relacionados à segurança são também apresentados.

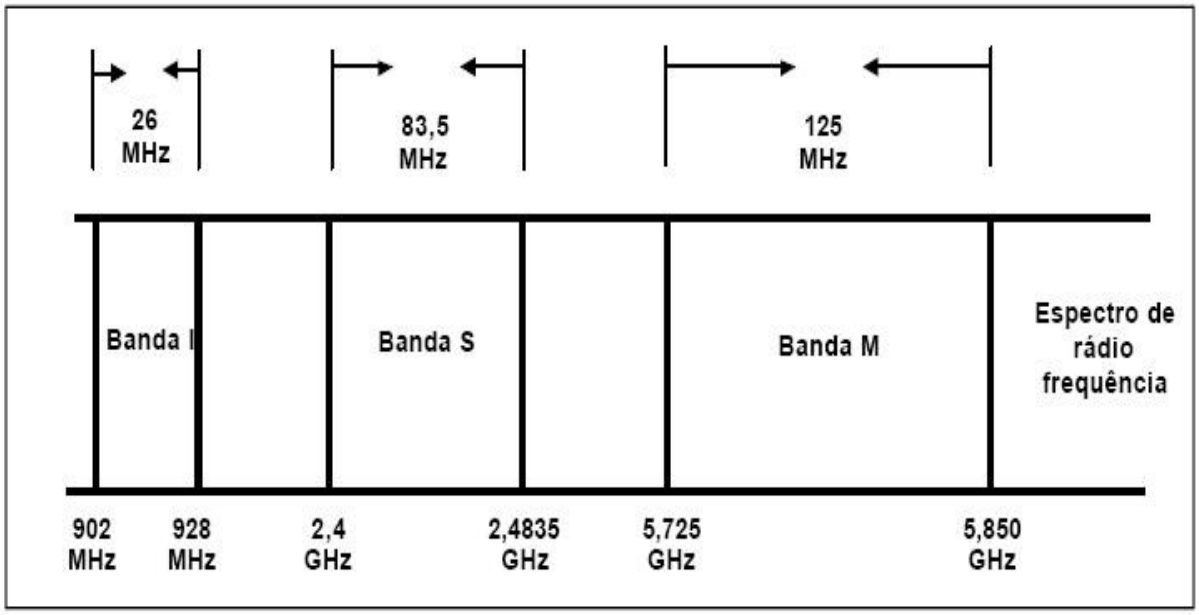
2.1 HISTÓRICO – EVOLUÇÃO DAS REDES SEM FIO

O primeiro padrão, chamado de IEEE 802.11 (sem nenhuma sigla ao final), foi publicado em 1997. Especificava taxas de transmissão de até 2 Mbps e transmissão por infravermelho ou radiofreqüência na faixa de 2.4 GHz. Este apenas serviu de base para padrões posteriores, sendo que atualmente nem se fabricam mais produtos compatíveis com tal tecnologia (SANCHES, 2005).

Dois anos mais tarde, em 1999, a IEEE efetuou algumas mudanças na camada física e lançou a especificação 802.11b, concebida com o objetivo de atender a necessidade de maior velocidade de transmissão imposta pelo mercado (ABRAS e SANCHES, 2002). Este padrão opera na freqüência de 2.4 GHz, dentro da banda ISM (*Industrial Scientific and Medical*), e pode transmitir dados à velocidade de até 11 Mbps (ONO, 2004). A banda ISM compreende as freqüências de 900 MHz, 2.4 GHz e grande parte das 5 GHz, as quais são reservadas nos EUA e em muitos outros países para utilização não-licenciada. Mas, ainda assim os dispositivos que operam nessas bandas devem ser homologados pela FCC (*Federal*

[1] É uma associação profissional técnica sem fins lucrativos com aproximadamente 380 mil membros, a qual possui como missão desenvolver padrões técnicos (SANCHES, 2005).

Communications Comission) e agências nacionais reguladoras, como a Anatel do Brasil (ENGST; FLEISHMAN, 2005). "O 802.11b foi tremendamente bem-sucedido e empresas venderam milhões de dispositivos que o suportavam" (ENGST; FLEISHMAN, 2005, p. 8).



Desenho 2: Bandas ISM
Fonte: Ribas (2002).

No mesmo ano surgiu a especificação 802.11a, a qual teve como principal característica o aumento da velocidade para um máximo de 54 Mbps, além da alteração da freqüência para a faixa de 5 GHz, menos suscetível a interferências (ROSNAM; LEARY, 2003). Deve-se ressaltar que estes dispositivos não utilizam a banda ISM e sim outra banda não licenciada, a U-NII (*Unlicensed National Information Infrastructure*).

Embora o padrão 802.11a seja semelhante ao 802.11b, não é compatível com este, uma vez que utiliza uma banda diferente no espectro de freqüências (ENGST; FLEISHMAN, 2005).

A adoção de dispositivos do padrão 802.11b praticamente dominava o mercado em meados de 2002, ora devido ao seu baixo preço frente ao padrão 802.11a, ora devido a sua adoção inicial e compatibilidades.

Entretanto, a idéia de conseguir taxas próximas a 54 Mbps animava à utilização do padrão 802.11a (ENGST; FLEISHMAN, 2005). Com esse intuito foi aprovado, em 2003, o padrão 802.11g, o qual mantinha total compatibilidade com o padrão 802.11b por operar na mesma faixa de freqüência (2.4 GHz) e ainda transmitia a taxa máxima de 54 Mbps, idêntico ao padrão 802.11a (ROSNAM; LEARY, 2003).

O Quadro 1 aponta as principais características e diferenças entre os padrões da tecnologia sem fio.

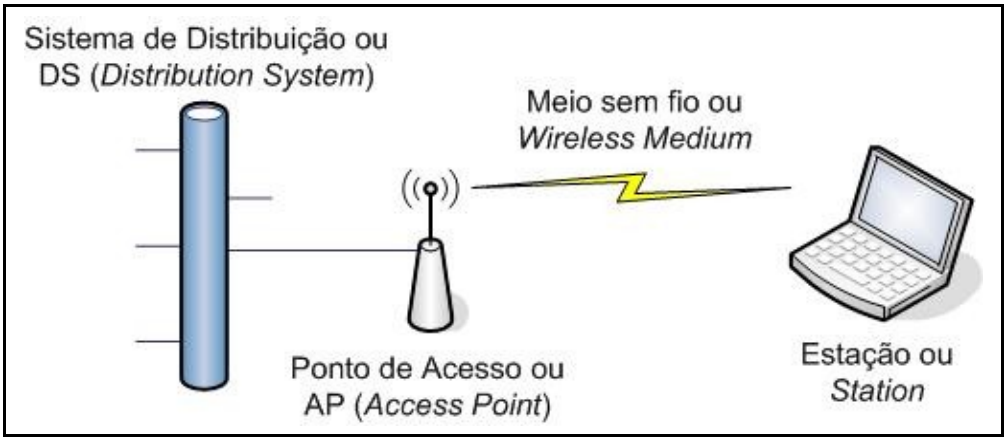
Padrão	Freqüência	Velocidade máxima[2]	Compatível com o 802.11b	Ano da padronização	Tendência à adoção
802.11b	2,4 GHz	11 Mbps	Sim	1999	Diminuindo em computadores, avançando na eletrônica mais barata.
802.11a	5 GHz	54 Mbps	Não	1999	Empresas adotando lentamente, sem consumidores.
802.11g	2,4 GHz	54 Mbps	Sim	2003	Avançando em todos os segmentos.

Quadro 1: Visão geral sobre os padrões da tecnologia sem fio
Fonte: Adaptado de Engst, Fleishman (2005).

Percebe-se que o padrão 802.11g, embora trabalhe na freqüência de 2.4 GHz e seja mais suscetível a interferências (devido ao fato de diversos aparelhos eletrônicos também trabalharem em 2.4 GHz), é uma tendência de adoção em diversos segmentos de mercado. Todavia, pode ocorrer também a adoção de dispositivos que suportem as três especificações (802.11a, 802.11b, 802.11g), de modo a oferecer total transparência aos usuários.

2.2 ARQUITETURA E ELEMENTOS DE REDE

De acordo com Gast (2002) e conforme pode ser visto no Desenho 3, as redes sem fio são compostas de quatro componentes principais:



Desenho 3: Componentes das redes sem fio
Fonte: Adaptado de Gast (2002).

[2] A velocidade máxima refere-se àquela descrita pela especificação. Entretanto, diversos fatores podem prejudicar o desempenho, tais como: interferências, protocolos de segurança, grandes distâncias entre transmissor e receptor, limitações de hardware, quantidade de usuários, dentre outros.

a) Sistema de Distribuição ou DS (*Distribution System*): é a parte lógica empregada para a comunicação entre os pontos de acesso com o propósito de formar uma grande área de abrangência. Comumente, a rede *Ethernet* é utilizada como *backbone* para o DS.

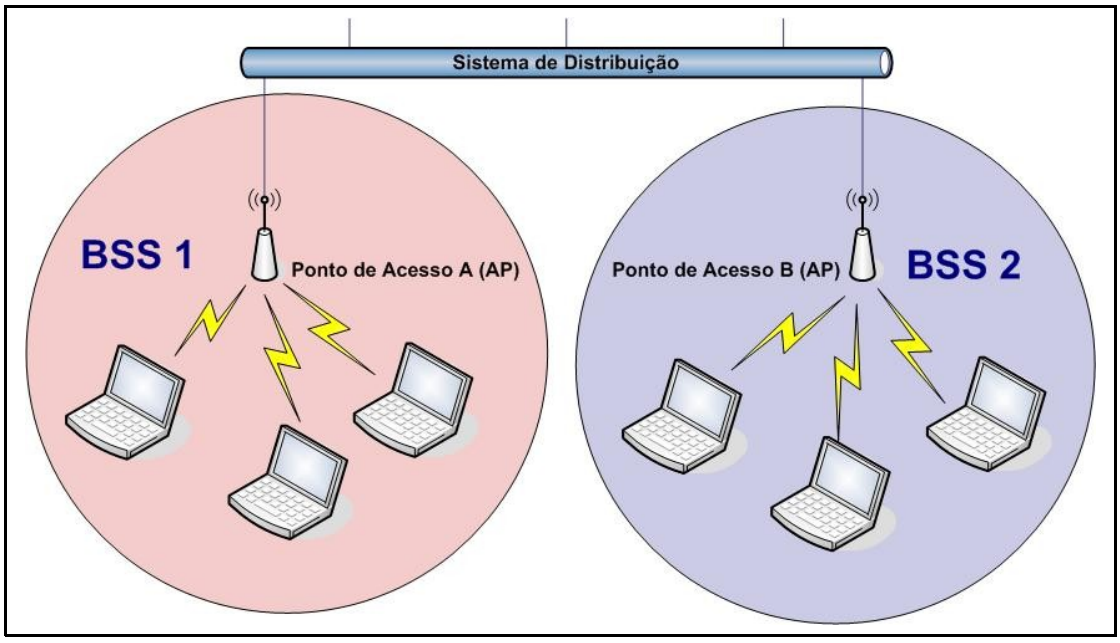
b) Ponto de Acesso ou AP (*Access Point*): possuem como função principal atuar como pontes (*bridges*) para o meio cabeado, mas também devem manter um *link* lógico entre os clientes.

c) Meio sem fio ou *Wireless Medium*: o meio sem fio é utilizado para transferir os fragmentos de dados entre as estações. Inicialmente, foram padronizadas as camadas físicas de infravermelho e radiofreqüência, porém, esta última tornou-se mais popular.

d) Estação ou *Station*: são dispositivos computacionais com interfaces de rede sem fio, como por exemplo, computadores portáteis (*notebooks*), computadores de mão (*handhelds*) ou estações de trabalho.

2.3 TOPOLOGIA / MODOS DE OPERAÇÃO

Uma WLAN é constituída de células ou conjuntos básicos de serviço, chamados de BSS (*Basic Service Set*) (Desenho 4), os quais podem ser entendidos simplesmente como grupos de estações que se comunicam entre si. Cada célula é controlada por uma estação base/ ponto de acesso (RIBAS, 2002; GAST, 2002 e KUROSE; KEITH, 2007).



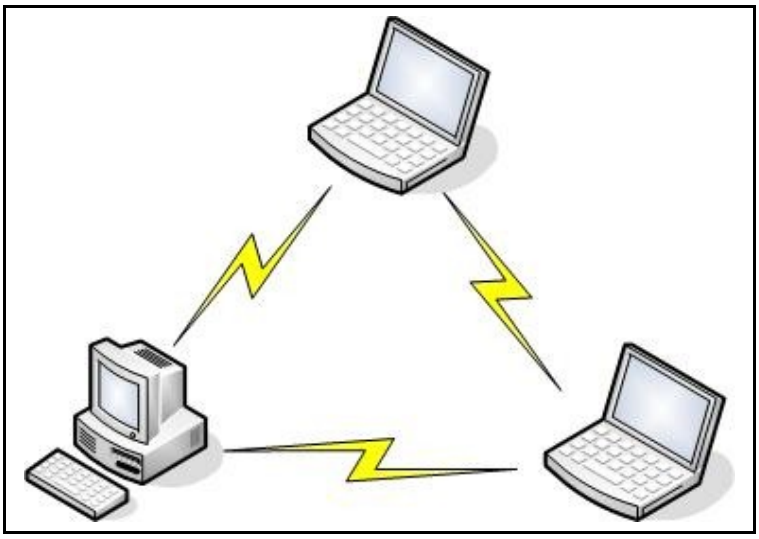
Desenho 4: Células BSS
Fonte: Adaptado de Kurose; Keith (2007) e Ribas (2002).

Rosnam e Leary (2003) elucidam que as redes são flexíveis e permitem a elaboração de três tipos de topologias ou modos de operação: IBSS (*Independent Basic Service Set*), também conhecida como rede sem fio *Ad Hoc* ou ponto a ponto; BSSs (*Basic Service Sets*), chamada de rede sem fio Infra-estruturada ou ponto de acesso; e ESS (*Extended Service Sets*), denominada como rede sem fio Infra-estruturada Estendida.

Em qualquer modo de operação da rede, um SSID (*Service Set Identifier*), também conhecido como "nome da rede sem fio", será utilizado pelas estações para identificar e/ou conectar nas redes sem fio disponíveis (GAST, 2002).

2.3.1 Rede Sem Fio IBSS (*Ad Hoc*)

Em redes IBSS ou *Ad Hoc* (Desenho 5), as estações podem se comunicar entre si diretamente sem a necessidade de um ponto de acesso, desde que estejam dentro de uma mesma área de alcance (GAST, 2002).



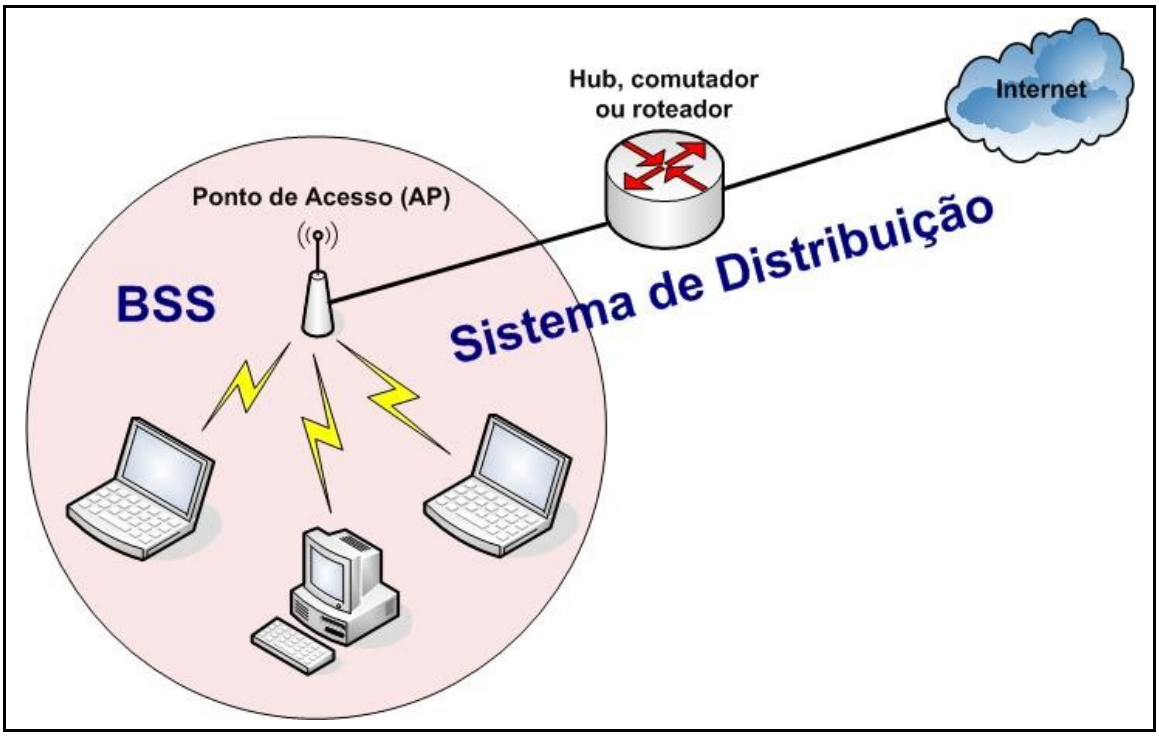
Desenho 5: Topologia *Ad Hoc*
Fonte: Adaptado de Sanches (2005).

É tipicamente utilizada para propósitos específicos e esporádicos, como por exemplo, compartilhamento de arquivos entre estações. Nesse caso, forma-se a rede conforme a necessidade, com a utilização de equipamentos próximos uns dos outros e em locais carentes de infra-estrutura. Esta rede pode ser formada por equipamentos portáteis, a fim de trocar dados na ausência de pontos de acesso (como por exemplo, em salas de conferências, trens ou mesmo em um carro) (KUROSE; KEITH, 2007).

Podem ser apontadas algumas desvantagens nas redes ponto a ponto, como o pequeno alcance e a impossibilidade de escalabilidade da rede, visto que a comunicação entre as estações ocorre de forma direta e a potência das placas de rede sem fio é muito inferior as de um ponto de acesso (REIS, 2004).

2.3.2 Rede Sem Fio BSS (Infra-estruturada)

Pode-se dizer que uma rede atua no modo BSS ou Infra-estrutura (Desenho 6) quando as estações são interconectadas entre si ou entre outras redes fazendo uso de um ponto de acesso (AP) (SANCHES, 2005).



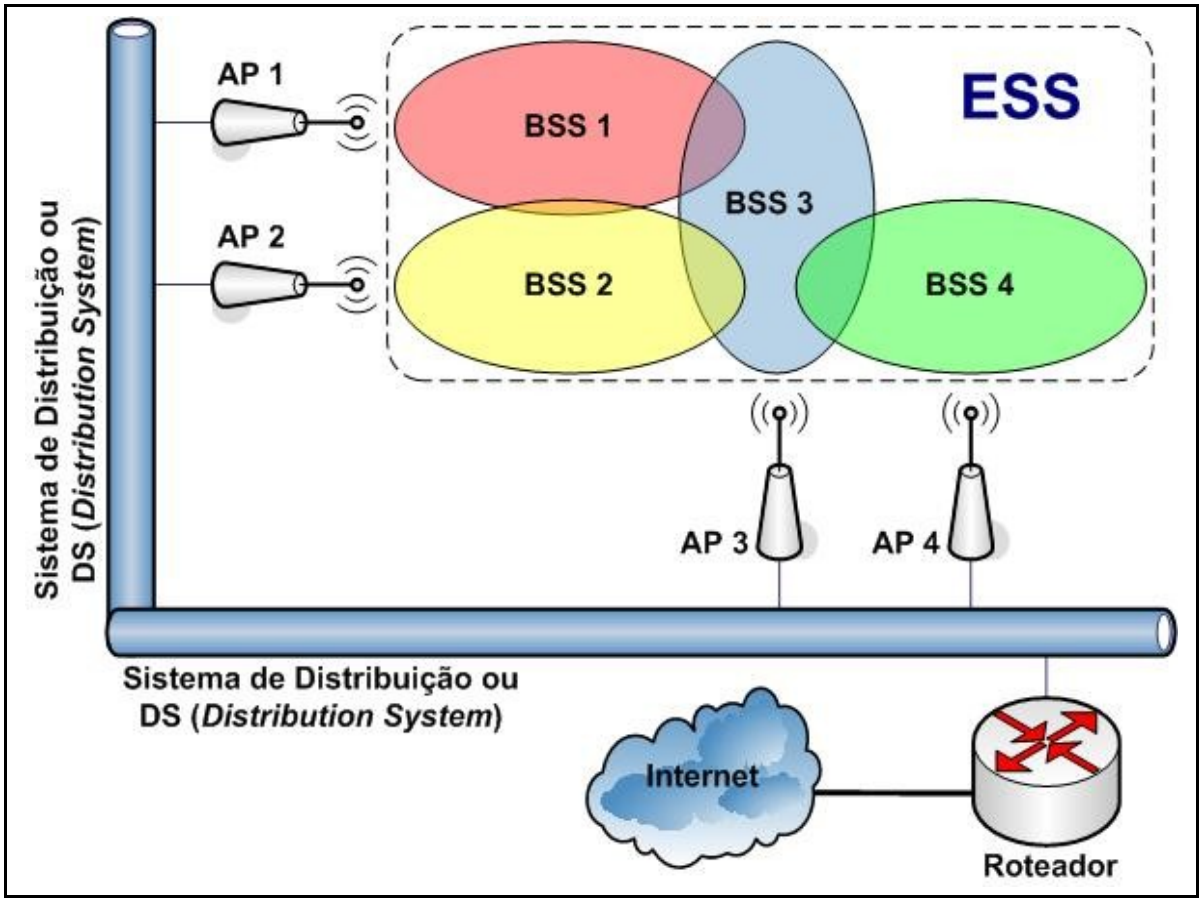
Desenho 6: Topologia Infra-estruturada
Fonte: Adaptado de Rosnam; Leary (2003).

Todo tráfego entre as estações precisa obrigatoriamente passar pelo AP, incluindo a comunicação entre as estações que estiverem na mesma área de serviço (GAST, 2002).

A designação de rede sem fio de infra-estrutura BSS provém do fato de ser necessária a utilização de um AP equipado com uma porta de conexão à rede cabeada (como por exemplo, um *link ethernet*) (ROSNAM; LEARY, 2003).

2.3.3 Rede Sem Fio ESS (Infra-estruturada Estendida)

O modo de rede sem fio ESS ou Infra-estruturada Estendida pode ser entendido como uma extensão da rede Infra-estrutura, utilizada principalmente para prover cobertura de rede para grandes áreas. O IEEE 802.11 (e suas variantes) permite a criação de redes sem fio para grandes áreas através da interconexão de diversos BSSs em um ESS (conjunto de serviços estendidos). No Desenho 7 o ESS é composto pela união dos quatros BSSs (GAST, 2002).



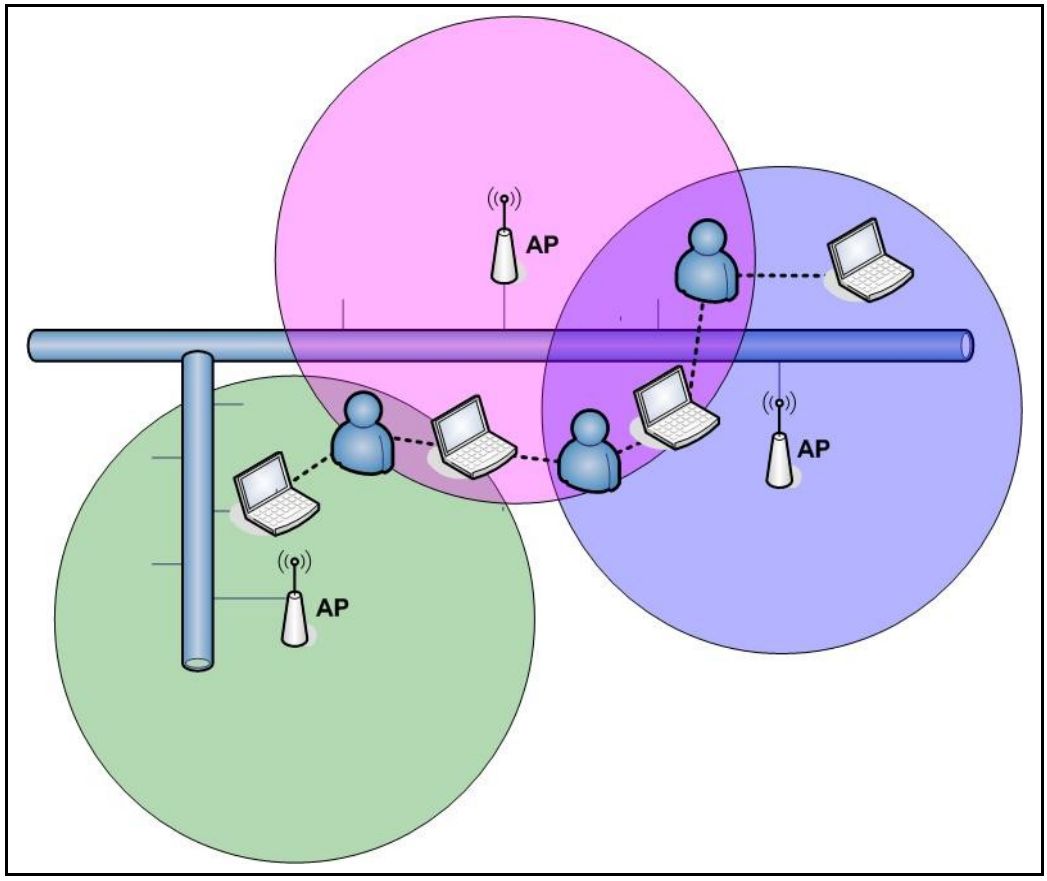
Desenho 7: Topologia Infra-estruturada Estendida (ESS)
Fonte: Adaptado de Gast (2002).

"Múltiplas infra-estruturas BSSs podem ser conectadas por meio de suas interfaces de link. [...] A coleção de BSSs interconectados por meio do DS é chamado de ESS" (ROSNAM; LEARY, 2003, p. 41, tradução nossa). O conjunto de especificações IEEE não define a tecnologia que deve ser utilizada para prover o *backbone* das redes sem fio, entretanto, a *ethernet* é na maioria das vezes utilizada.

2.3.4 Múltiplos pontos de acesso (Associação e *Roaming*)

Em espaços abertos ou ambientes menores com poucos usuários (como por exemplo, redes domésticas) não será necessário mais de um AP. No entanto, quando se deseja ampliar a área de cobertura ou esta apresenta obstruções, ou ainda o volume de usuários ou tráfego aumenta, faz-se necessária a adição de mais pontos de acesso. Desta forma, deve-se garantir que os usuários que circulam na área coberta (células) da rede sem fio não percam a mobilidade.

Inicialmente, quando um cliente está em uma célula com mais de um AP, associa-se a determinado AP baseado na força do sinal ou tráfego de rede. Uma vez aceito por esse AP, o cliente continuamente faz buscas a fim de determinar se outro AP oferece um serviço melhor. Caso encontre, o cliente reassocia-se com este novo AP. Este conceito, onde o cliente se movimenta entre duas ou mais células sem perder a conexão é conhecido como *roaming* e pode ser visto no Desenho 8 (3COM, 2000).



Desenho 8: *Roaming* entre vários APs
Fonte: Adaptado de Wlana (1999).

Deve-se levar em consideração que a especificação IEEE para redes sem fio não determina como deve ser o comportamento das estações quando trocam de célula (BSS). Nesse caso, os fabricantes de dispositivos adotaram soluções proprietárias para resolver tal problema (REIS, 2004). Desta forma, caso seja necessário garantir a função de *roaming*, é indispensável considerar a adoção de pontos de acesso do mesmo fabricante (GAST, 2002).

2.4 SEGURANÇA EM REDES SEM FIO

A tecnologia de redes sem fio já conquistou grande parte das empresas ou corporações. Porém, ainda existem restrições quanto ao seu uso para transmitir informações sigilosas ou críticas, principalmente pelo fato do meio de transmissão ser de domínio público e normalmente se estender para além da área geográfica da organização (RIBAS, 2002).

Devido a essas características, as redes sem fio possuem vulnerabilidades que instigam tentativas de ataque. Logo, torna-se necessário conhecer os detalhes dos vários tipos de ataques praticados, a fim de preparar defesas (FLECK; POTTER, 2002).

> As ferramentas disponíveis para monitoração e até controle de redes sem fio não são projetadas com intenção nociva. Na sua maioria, elas foram desenvolvidas para demonstrar que fraquezas potenciais eram na verdade brechas de segurança. Os administradores de rede precisam desses tipos de ferramentas para entender como melhor proteger os dados que fluem por suas redes. Também são extremamente úteis para procurar por redes sem fio abertas quando você estiver em trânsito, para solucionar certos tipos de problemas de rede em sua própria rede e para planejar uma nova rede sem fio (ENGST; FLEISHMAN, 2005, p. 279).

Duarte (2003) e Andrade (2004) elucidam que os ataques às redes sem fio objetivam não somente prejudicar a sua disponibilidade, mas também obter acesso à rede cabeada, comprometendo os recursos nela disponíveis. Complementam ainda que, além dos riscos inerentes a uma rede cabeada, a rede sem fio está sujeita a outros tipos de ataques. Alguns deles são comentados a seguir:

a) Associação maliciosa: um usuário malicioso simula um ponto de acesso, de modo a induzir o cliente a conectar na rede falsa;

b) *MAC Spoofing*: alguns pontos de acesso podem ser configurados para limitar o acesso à rede sem fio apenas para determinados endereços físicos de rede (MAC). Nesse tipo de ataque, o usuário mal intencionado captura um endereço MAC válido de um cliente e o configura em seu equipamento, podendo usufruir de todos os recursos da rede sem fio;

c) Negação de Serviço: também conhecido como DoS (*Denial of Service*), tem a finalidade de tornar inacessíveis determinados recursos ou serviços. Existem basicamente duas formas de executar esse tipo de ataque: uma delas é causar interferências na rede sem fio utilizando equipamentos que operem na mesma freqüência dos pontos de acesso; a outra é simular um ponto de acesso com o mesmo SSID e MAC de um ponto de acesso válido na rede, com a finalidade de inundá-la com pedidos de associação e dissociação de clientes (estações);

d) Ataques de vigilância: apesar de não ser considerado uma técnica de ataque por alguns autores, consiste em técnicas de observação dos pontos de acesso físicos da rede sem fio, de forma a serem objetos de estudos futuros para invasões. Este tipo de ataque inclui até mesmo a pichação de símbolos em muros, técnica conhecida como *warchalinkg*, para a identificação de detalhes da rede sem fio.

2.4.1 Mecanismos de autenticação e segurança

Considerando o fato de que as redes sem fio utilizam ondas de rádio para a difusão de seu sinal, o que torna extremamente difícil gerenciar seus limites, nota-se o quão inseguras são em comparação com as redes cabeadas. Mas, um conjunto de políticas aliado a implantação de mecanismos de segurança pode auxiliar muito na prevenção de incidentes nessa área. O foco deste trabalho não é voltado à segurança das redes sem fio, portanto, serão descritos nessa seção apenas alguns fatores básicos que devem ser analisados na definição da segurança da rede sem fio.

Segundo Linhares, Gonçalves (2006), por via de regra, a concepção de mecanismos de segurança se baseia em três requisitos básicos:

a) Autenticação: identificação de pessoas e dispositivos. Deve garantir o acesso à rede e aos serviços somente a pessoas e dispositivos autorizados;

b) Confidencialidade: criptografia dos dados. Deve permitir que somente pessoas previamente autorizadas consigam descriptografar e entender as mensagens;

c) Integridade: deve assegurar que os dados recebidos pelo receptor sejam os mesmos que foram transmitidos pelo emissor.

2.4.1.1 Autenticação de Sistema Aberto (*Open-System*)

Esse tipo de autenticação possibilita rapidamente o acesso das estações à rede sem fio, pois o ponto de acesso aceita o pedido de associação de qualquer estação sem verificar sua identidade (endereço MAC), tornando-se, conforme o nome sugere, uma autenticação nula (GAST, 2002; ROSNAM; LEARY, 2003; EDNEY; ARBAUGH, 2003).

Desenho 9: Autenticação de sistema aberto
Fonte: Adaptado de Gast (2002).

O Desenho 9 ilustra o pedido de autenticação da estação (cliente) ao ponto de acesso, que responde autorizando a solicitação.

2.4.1.2 Autenticação por Chave Compartilhada (*Shared-Key*)

Esse tipo de autenticação utiliza-se do sistema desafio-resposta (*challenge-response*), onde a estação deve responder corretamente a um desafio enviado pelo ponto de acesso, sob pena de não autenticar-se. Nesse caso, todas as estações que quiserem ter acesso à rede devem possuir a chave secreta compartilhada. Essa solução pode tornar-se muito trabalhosa, pois será necessário configurar a chave compartilhada manualmente em todas as estações inicialmente e posteriormente, em caso de troca da chave ou quebra de sigilo (como por exemplo, se alguma pessoa sair da empresa) (GAST, 2002; ROSNAM; LEARY, 2003; DUARTE, 2003; ANDRADE, 2004).

Desenho 10: Autenticação por chave compartilhada
Fonte: Adaptado de Gast (2002).

Ao contrário da autenticação de sistema aberto, a autenticação por chave compartilhada exige o uso de criptografia, tanto pelo cliente (estação), quanto pelo ponto de acesso (AP). O Desenho 10 demonstra passo-a-passo o processo de autenticação por chave compartilhada (Rosnam; Leary, 2003):

a) O cliente envia um pedido de autenticação por chave compartilhada para o AP;

b) O AP responde com o desafio-resposta em texto plano (sem criptografia);

c) O cliente criptografa o desafio e responde ao AP;

d) Se o AP conseguir descriptografar a mensagem utilizando sua chave compartilhada e o resultado for o mesmo que o desafio enviado inicialmente à estação, transmitirá uma mensagem de sucesso para a estação;

e) O cliente finalmente poderá acessar a rede.

2.4.1.3 Autenticação por *SSID*

O SSID, como já mencionado, é conhecido como o "nome da rede". Cada fabricante de dispositivos sem fio possui um valor padrão para essa opção, e aconselha-se alterá-lo para dificultar sua identificação. Esse método consiste em desativar o recurso de envio periódico (*broadcast*) do SSID na rede sem fio, obrigando a estação a conhecer previamente a rede sem fio ao qual quer conectar-se. Habitualmente, esse método é utilizado conjuntamente com outros métodos de autenticação existentes (GRÜNEWALD, 2005).

"Não se engane com a falsa sensação de segurança. Embora uma rede 'fechada' ofereça proteção contra a maioria dos observadores casuais, muitos programas de monitoramento de redes sem fio [...] podem facilmente ver os nomes de redes fechadas"

(ENGST; FLEISHMAN, 2005, p. 273, grifo nosso). Como se pode imaginar, esse método oferece uma proteção muito fraca isoladamente e deve ser evitado (ANDRADE, 2004).

2.4.1.4 Autenticação pelo endereço MAC

Outro mecanismo disponível nos pontos de acesso pelos fabricantes (mas não definido no padrão de redes sem fio) para prover segurança é o controle de acesso baseado nos endereços físicos dos clientes (endereço MAC). Cada dispositivo de rede possui um único endereço capaz de identificá-lo de forma inequívoca, o qual é utilizado para que os pontos de acesso possam validar ou proibir o acesso à rede. Consequentemente, só é aplicável em redes pequenas, pois exige uma gestão cuidadosa e exaustiva de todos os pontos de acessos (REIS, 2004; ROSNAM; LEARY, 2003).

Esse método oferece uma proteção fraca, visto que os endereços MAC podem ser falsificados através do ataque de MAC *spoofing* (mencionado anteriormente) e, assim como o SSID, é geralmente utilizado em conjunto com outros métodos (ENGST; FLEISHMAN, 2005; ANDRADE, 2004).

2.4.1.5 Autenticação por IEEE 802.1x e EAP

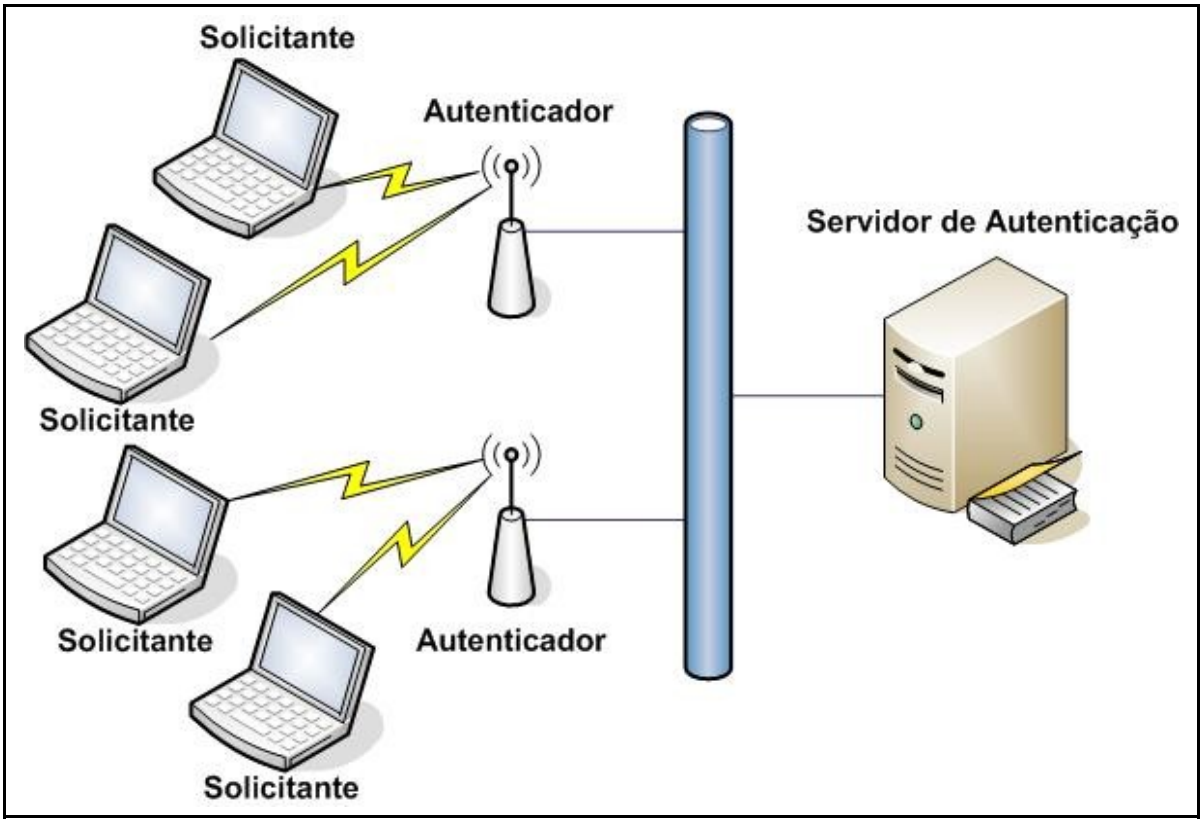
O padrão 802.1x foi desenvolvido inicialmente para redes com fio, com a finalidade de controlar o acesso de conexões à LAN baseado por portas físicas (SANCHES, 2005). Posteriormente, ele foi adaptado para uso em redes sem fio, sendo baseado no mapeamento de portas lógicas, como é o caso na associação entre dispositivos sem fio e ponto de acesso (GAST, 2002; MIYANO NETO, 2004; SANCHES, 2005). A idéia é que, para todo usuário que se conecte numa porta, seja requerido uma verificação da identidade do usuário antes da utilização da rede (EDNEY e ARBAUGH, 2003).

Os autores Edney e Arbaugh (2003), Gast (2002), Miyano Neto (2004) e Rosnam (2003) definem, conforme pode ser visto no Desenho 11, que o protocolo 802.1x é composto de três elementos:

a) Solicitante ou Suplicante: refere-se ao cliente ou dispositivo que deseja se autenticar;

b) Servidor de autenticação: sistema de autenticação responsável pelo processamento das autenticações necessárias. Normalmente, as empresas utilizam o servidor RADIUS (*Remote Authentication Dial-In User Service*), o qual corresponde a um servidor AAA (*Authentication, Authorization and Accounting*) e geralmente também é utilizado para autenticar usuários remotos;

c) Autenticador: dispositivo que permite a comunicação entre o suplicante e o servidor de autenticação. Usualmente é um ponto de acesso (AP).



Desenho 11: Elementos envolvidos na autenticação 802.1x
Fonte: Adaptado de Fleck, Potter (2002).

Para a comunicação entre o solicitante e o autenticador, é utilizado o protocolo EAP (*Extensible Authentication Protocol*), que é responsável pela criação de um canal lógico seguro entre o solicitante e o servidor de autenticação, por onde serão trafegadas as credenciais de acesso. O protocolo EAP define como as mensagens de autenticação devem ser transferidas, porém não especifica como deve ser feito o transporte sobre os protocolos de comunicação existentes, como por exemplo: o TCP/IP. Para isso, o IEEE 802.1x criou o protocolo EAPoL (*EAP over* LAN), que é um protocolo EAP encapsulado para redes locais, responsável pelo transporte das mensagens EAP. Fisicamente, os clientes se comunicarão com

os pontos de acesso através do protocolo EAPoL e os pontos de acesso, por sua vez, comunicar-se-ão com o servidor de autenticação através do protocolo 802.1x (EDNEY; ARBAUGH, 2003; LINHARES, GONÇALVES, 2006).

> O método de autenticação é definido no EAP – *Extensible Authentication Protocol*. Este protocolo fornece um *framework* para que o sistema de autenticação escolha o método apropriado de autenticação. Este método pode ser: senhas, certificados digitais ou qualquer outro tipo de *token*. Utilizando o EAP, o autenticador (APs) não precisa ser especifico quanto ao método de autenticação, basta operar como *proxy* das informações entre o suplicante e o servidor de autenticação (MIYANO NETO, 2004, p. 16, grifo nosso).

O EAP permite vários métodos de autenticação. Uma lista detalhada e comentada dos métodos de autenticação EAP pode ser encontrada em Rosnam (2003), Andrade (2004), Miyano Neto (2004), Aguiar (2005) e em WI-FI ALLIANCE (2005).

2.4.1.6 Autenticação por portal (*hotspot*)

A autenticação por portal, geralmente chamada de *hotspot*, é baseada na autenticação via interface HTTP/HTTPS, configuração de regras de *firewall* dinâmicas e outros recursos centralizados, dispostos em um dispositivo de controle – o qual deve possuir acesso à rede externa – conectado na rede local cabeada. Nesse tipo de autenticação, todo tráfego vindo dos pontos de acesso será interceptado e, somente após a autenticação do cliente, liberado (CARRION, 2005).

Desta forma, o acesso será totalmente bloqueado a qualquer usuário até que esse forneça credenciais válidas, verificadas em um banco de dados qualquer, para autenticação. Verificadas as credenciais, dinamicamente o *firewall* irá liberar o acesso para o cliente até que outra regra modifique essa ação (tempo de inatividade, desligamento da estação) (FLECK; POTTER, 2002).

Frequentemente, os ambientes de *hotspot* não oferecem segurança alguma, com exceção de usar conexão segura (HTTPS) para proteger as credenciais de ingresso, pois normalmente são utilizados em locais de acesso público, como por exemplo, hotéis, aeroportos, centros de convenções, universidades, praças públicas. Outro fato que encoraja a adoção desse mecanismo é a facilidade de acesso, pois não requer nenhum software ou configuração por parte do usuário.

A autenticação por portal pode ocorrer de várias maneiras, entre elas: (a) *closed* portal, o qual pode ser utilizado para restringir o acesso a um determinado grupo de usuários com credenciais de usuário e senha, ou então exigir o pagamento para utilização por tempo determinado; (b) *open* portal, que simplesmente requer a aceitação de um termo de uso para liberação do acesso (FLECK; POTTER, 2002).

2.4.1.7 Criptografia WEP (*Wired Equivalent Privacy*)

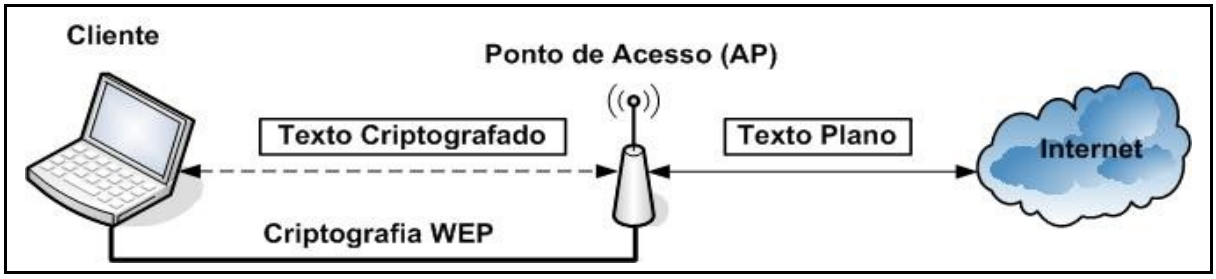
A criptografia WEP (*Wired Equivalent Privacy*) foi introduzida em 1999 no padrão IEEE 802.11 com a intenção de proporcionar segurança dos dados equivalente à de uma rede cabeada, conforme o próprio nome sugere, de acordo com os requisitos básicos já descritos para um mecanismo de segurança. É utilizada tanto para impedir o acesso à rede por usuários não autorizados quanto para prevenir a captura do tráfego da rede sem fio (MIYANO NETO, 2004).

> A WEP foi projetada para agir meramente como uma porta trancada, impedindo que os invasores penetrem no tráfego da rede sem fio; outras medidas destinam-se a sustentar essa linha inicial de defesa. A WEP basicamente criptografa todos os dados que fluem por uma rede sem fio, impedindo que os invasores espionem o tráfego da rede (ENGST; FLEISHMAN, 2005, p. 274).

O protocolo WEP é baseado em um processo criptográfico RC4, o qual criptografa os dados à medida que eles são transmitidos de forma a aumentar o seu desempenho (ANDRADE, 2004), e composto de dois elementos: um vetor de inicialização de 24 *bits* e uma chave secreta compartilhada de 40 ou 104 *bits*, resultando em uma chave de 64 ou 128 *bits* (GRÜNEWALD, 2005).

O protocolo WEP permite que o ponto de acesso autentique seus usuários seguindo o mesmo princípio já explicado anteriormente no item autenticação por chave compartilhada (ABRAS e SANCHES, 2002). De forma geral, quando a WEP é ativada, todos os dispositivos que quiserem se comunicar devem possuir a mesma chave secreta, a qual será utilizada para cifrar os dados antes de serem transmitidos. Caso algum dispositivo receba um pacote não criptografado com a chave secreta correta, o descartará sumariamente (MIYANO NETO, 2004). Maiores informações acerca do processo de transmissão de pacotes com o protocolo WEP ativado, bem como descrições detalhadas sobre o algoritmo RC4 podem ser encontradas em Miyano Neto (2004), Edney e Arbaugh (2003), Rosnam (2003) ou Gast (2002).

Conforme pode ser visto no Desenho 12, "[...] a criptografia WEP só é aplicada ao tráfego do canal de comunicação sem fio e, portanto, o tráfego roteado para fora da rede sem fio não possui criptografia WEP" (LINHARES; GONÇALVES, 2006, p. 3).



Desenho 12: Criptografia WEP
Fonte: Adaptado de Linhares, Gonçalves (2006).

Infelizmente, o protocolo WEP possui diversas fragilidades, entre elas: (a) a chave secreta deve ser conhecida por um grande número de pessoas, o que a torna vulnerável; (b) o algoritmo RC4 não implementa chaves de 64 ou 128 *bits* reais; (c) o segredo compartilhado é realmente a própria senha de criptografia; (d) existem diversas ferramentas disponíveis que são capazes de quebrar as chaves de codificação caso seja possível monitorar o tráfego da rede durante algumas horas (SANCHES, 2005; ENGST; FLEISHMAN, 2005; GAST, 2002; MIYANO NETO, 2004).

2.4.1.8 Criptografia WPA (*WiFi Protected Access*)

O grande número de limitações/vulnerabilidades identificados no protocolo WEP gerou demanda para o desenvolvimento de um novo padrão de segurança. O IEEE iniciou pesquisas para o desenvolvimento do padrão IEEE 802.11i e, enquanto este não era aprovado, a Wi-Fi Alliance[3] apresentou em 2003 um padrão intermediário entre o WEP e o IEEE 802.11i, o padrão WPA (*Wi-Fi Protected Access*), como forma de responder às críticas impostas pelo meio corporativo ao WEP (LINHARES; GONÇALVES, 2006).

Esse padrão, também chamado de WEP2 ou TKIP, além de ser compatível com o hardware que roda o WEP (não necessitando mudanças na infra-estrutura de hardware), ainda

[3] Associação internacional, sem fins lucrativos, criada em 1999 com o objetivo de difundir e promover o crescimento das redes locais sem fio (WLANs). Desde o ano 2000, a Wi-Fi Alliance já certificou mais de 4.200 dispositivos sem fio, como forma de assegurar a interoperabilidade baseado na especificação IEEE 802.11 (WI-FI ALLIANCE, 2007).

oferece melhor tratamento de segurança que o WEP, no que tange aos mecanismos de autenticação, confidencialidade e controle de integridade dos dados (AGUIAR, 2005).

> "Atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP)" (RUFINO, 2005, p.37).

O protocolo WPA utiliza uma tecnologia de criptografia de 128 bits chamada de TKIP (*Temporal Key Integrity Protocol* – Protocolo de Geração de Chaves Temporais), o qual gera chaves criptográficas diferentes para cada estação da rede com base em seus endereços físicos (MAC), tornando-o extremamente robusto.

> O TKIP [...] aumenta o tamanho do vetor de inicialização para 48 bits e assegura que a escolha desse número não é previsível. Essa alteração aumenta enormemente a complexidade de quebrar o sistema de criptografia – por várias ordens de magnitude. Os engenheiros estimam que uma chave não se repetirá por mais de cem anos em um único dispositivo. Ainda mais impressionante, cada pacote terá sua própria chave única criada a partir da mistura do vetor com uma chave-mestre (ENGST; FLEISHMAN, 2005, p. 278).

Além disso, inclui um mecanismo chamado MIC (*Message Integrity Check*) que verifica se as mensagens não foram alteradas no caminho, prevenindo com isso que um usuário malicioso capture, altere e reenvie os pacotes de dados (WI-FI ALLIANCE, 2005).

Sanches (2005) apresenta uma comparação entre os protocolos WEP e WAP, ver no Quadro 2, destacando as principais características de ambos com relação à criptografia e autenticação.

	WEP	**WPA**
Criptografia	Quebrada por cientistas e *hackers.*	Dificulta as falhas do WEP.
	Chave estática, utilizada por todos na mesma rede.	Chave de sessão dinâmica – por usuário, por sessão, por chave de pacote.
	Distribuição da chave manualmente – Necessidade de digitar a chave em todos os dispositivos.	Distribuição das chaves automaticamente.
	Chave de 40 bits.	Chave de 128 bits.
Autenticação	Quebrada, uso da Chave WEP para autenticação.	Autenticação de usuário mais forte, Utilizando 802.1x e EAP.

Quadro 2: Comparação entre WEP e WPA
Fonte: Adaptado de Sanches (2005, p. 239).

Existem dois tipos de autenticação no WPA: **WPA Pessoal**, que não faz uso de um servidor de autenticação e utiliza chave pré-compartilhada (WPA-PSK – WPA-*Pre Shared Key*); e **WPA Corporativo**, onde o AP não é responsável pela autenticação. Neste caso, é

utilizada uma infra-estrutura composta por um servidor de autenticação 802.1x em conjunto com algum tipo de protocolo de autenticação EAP (*Extensible Authentication Protocol*) (LINHARES; GONÇALVES, 2006).

2.4.1.9 Criptografia WPA2 ou 802.11i

O padrão IEEE 802.11i foi ratificado pelo IEEE em 2004 e ficou conhecido também como WPA2. O WPA2 implementa todos os elementos de segurança definidos pela especificação 802.11i e apresenta, em comparação com o WPA, avanços em relação aos algoritmos de criptografia e integridade (LINHARES; GONÇALVES, 2006; WI-FI ALLIANCE, 2005).

Assim como o WPA, o WPA2 suporta a autenticação por PSK (*Pre-Shared Key*) e IEEE 802.1x com EAP. A principal diferença é a introdução de um novo protocolo de segurança, chamado de CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), o qual introduz um método de criptografia muito mais robusto, conhecido como AES (*Advanced Encryption Standard*). Ressalta-se que o TKIP ainda pode ser utilizado de forma opcional no WPA2 (WI-FI ALLIANCE, 2005; AGUIAR, 2005, MIYANO NETO, 2004). Maiores informações sobre o CCMP (AES) podem ser encontradas em Edney; Arbaugh (2003) e em Wi-Fi Alliance (2005).

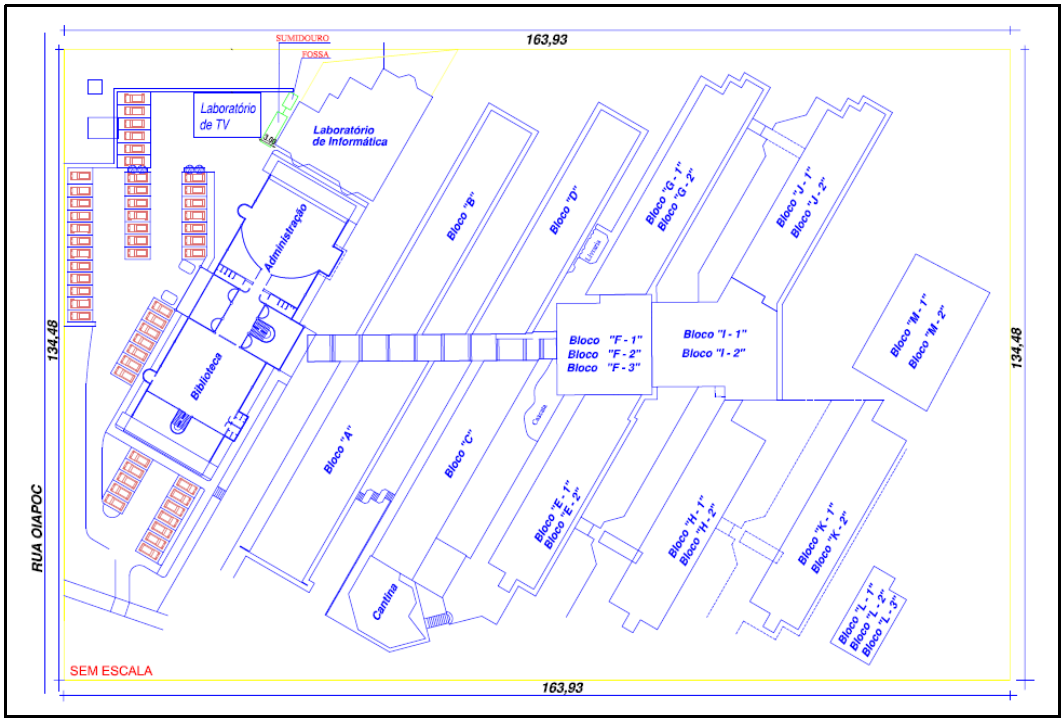
Diferentemente do WPA, este novo método de criptografia exige a substituição dos hardwares existentes, pois exige um maior poder computacional durante o processo de codificação/decodificação, impossibilitando dessa forma apenas uma atualização do *firmware* existente (LINHARES; GONÇALVES, 2006, AGUIAR, 2005).

3 ESTUDO DE CASO DA IMPLANTAÇÃO DA REDE SEM FIO NA UNOESC – CAMPUS DE SÃO MIGUEL DO OESTE

Esta pesquisa consiste de um estudo de caso exploratório descritivo abordando os conceitos e requisitos técnicos necessários para a implantação de uma rede sem fio no campus de São Miguel do Oeste da UNOESC. O escopo do trabalho limitou-se especificamente à implantação da rede sem fio para acesso à Internet.

3.1 AMBIENTE DE IMPLANTAÇÃO

A Universidade do Oeste de Santa Catarina – Campus de São Miguel do Oeste possui em torno de 4985 acadêmicos, distribuídos entre 30 cursos de graduação e 21 cursos de pós-graduação em nível de especialização. Existem ainda cerca de 360 funcionários, distribuídos entre técnicos administrativos e professores[4].



Desenho 13: Planta baixa do campus da UNOESC em São Miguel do Oeste – SC
Fonte: o autor.

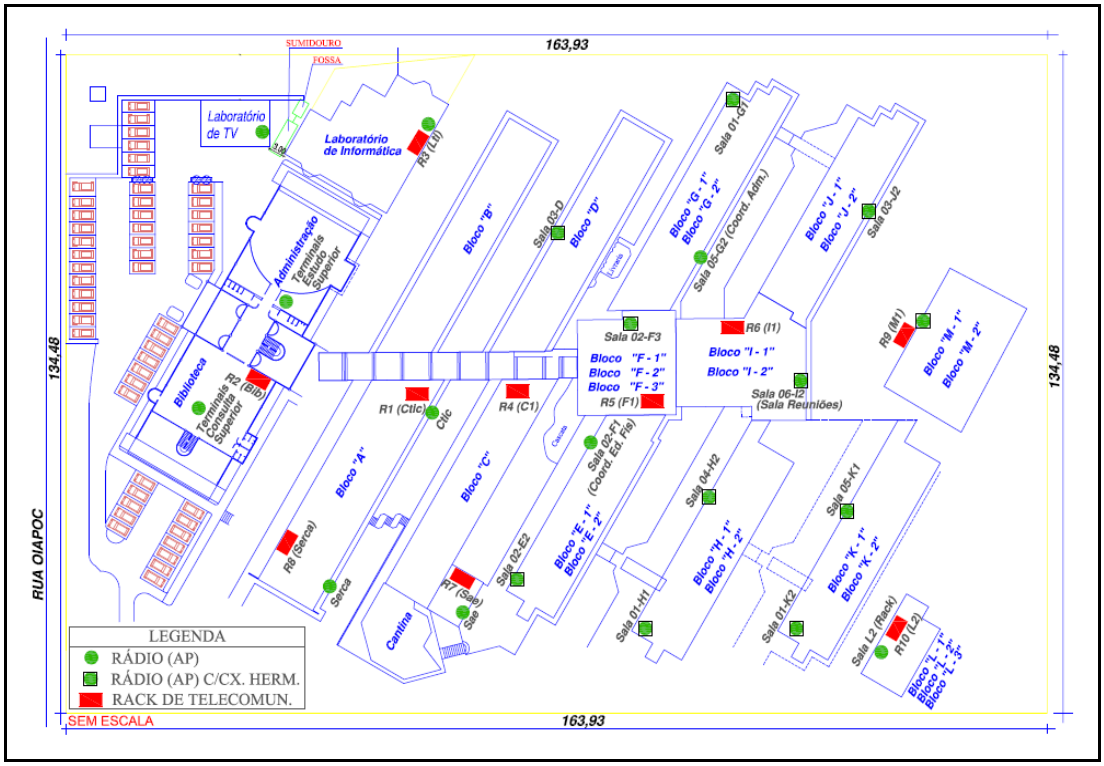
[4] Estas informações, assim como as informações sobre quantidade de alunos e cursos, foram fornecidas pela universidade e são referentes ao primeiro semestre de 2008.

A estrutura física do Campus (ver Desenho 13 ou Apêndice A, para maiores detalhes) contém atualmente 16 blocos, onde estão situados os setores administrativos (biblioteca, laboratórios, coordenações), salas de aula, cantina, centros de conveniências e auditório, distribuídos entre aproximadamente 22.045 m² de área que compõem o campus.

O aumento de serviços oferecidos *on-line*, pela instituição, gera uma demanda crescente na utilização da infra-estrutura tecnológica existente. A possibilidade dos alunos realizarem consultas de informações, pesquisa e renovações de materiais bibliográficos, matrículas e outros, através da Internet já são é realidade.

3.2 DEFINIÇÃO DA ARQUITETURA / TOPOLOGIA DA REDE

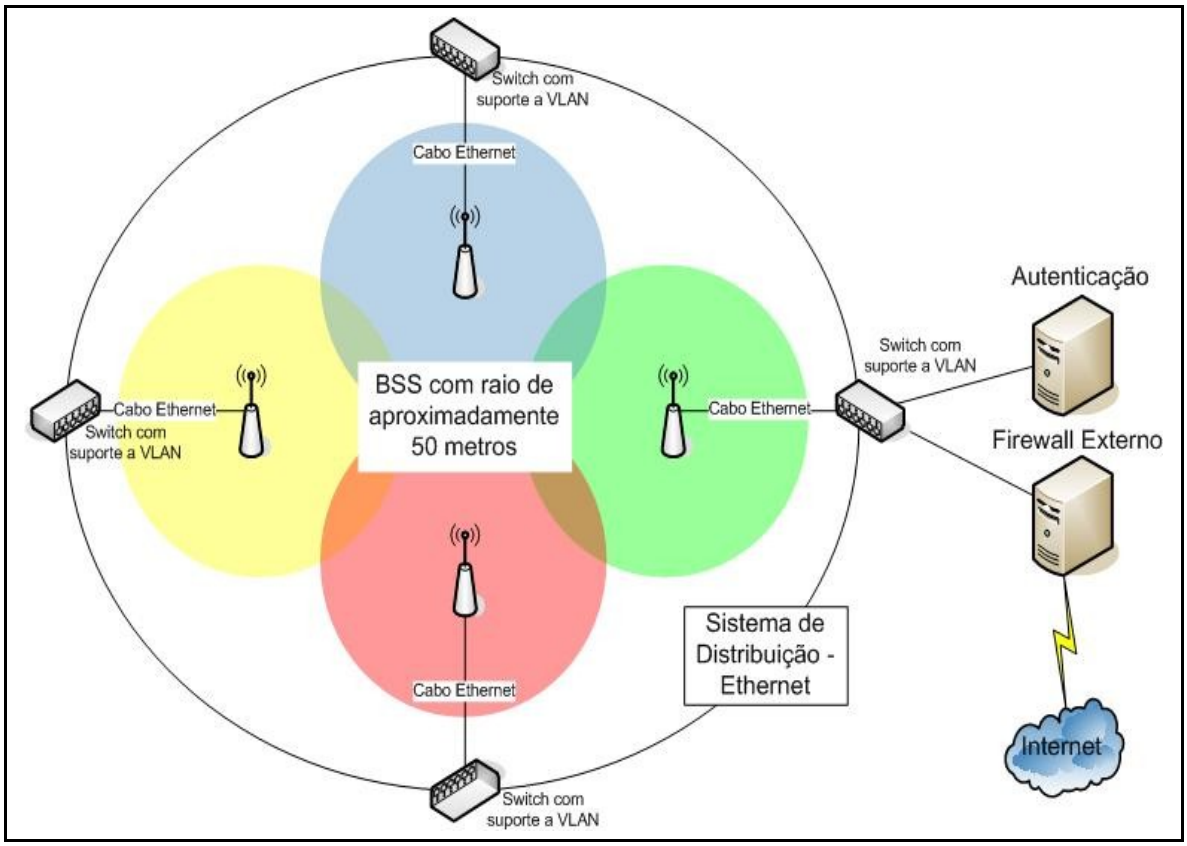
Devido ao tamanho da área geográfica a ser coberta pela rede sem fio, não seria possível cobri-la com somente um ponto de acesso. Assim sendo, optou-se pela topologia de rede sem fio infra-estruturada estendida (ESS), fazendo uso de múltiplos pontos de acesso distribuídos em locais estratégicos do campus (ver Desenho 14 ou Apêndice B, para maiores detalhes).



Desenho 14: Planta baixa da UNOESC com APs e *racks* de telecomunicações
Fonte: o autor.

Os locais/pontos estratégicos foram definidos de tal maneira que a BSS criada por um AP tenha uma intersecção com APs adjacentes (fator crítico para permitir o *roaming* entre as células). Ainda, foram priorizados os pontos próximos à infra-estrutura cabeada disponível.

Para aumentar a segurança entre as redes administrativas e a rede sem fio, de modo que uma não possa se comunicar com a outra, utilizou-se redes locais virtuais[5] (VLAN). Além disso, empregou-se um sistema de *hotspot* (melhor explicado posteriormente) para realizar a autenticação dos usuários e *firewall* para efetuar a filtragem de pacotes permitidos / proibidos.



Desenho 15: Arquitetura da rede sem fio da UNOESC
Fonte: o autor.

O Desenho 15 ilustra de forma sintética a arquitetura da rede sem fio implantada no campus de São Miguel do Oeste da UNOESC. A utilização de VLANs permite maior flexibilidade no gerenciamento das redes, pois possibilita a utilização de redes diferentes em um mesmo *switch* de forma dinâmica e segura. Desta forma, pode-se utilizar a infra-estrutura existente para transportar os dados entre os pontos de acesso espalhados pelo campus, não sendo necessário um equipamento exclusivo.

[5] Redes locais virtuais são utilizadas, dentre outras funções, para a segurança lógica e segmentação de redes locais (TANEMBAUM, 2003).

3.3 COMPONENTES UTILIZADOS

Antes de escolher os componentes que seriam utilizados para compor a rede sem fio, fez-se necessário definir o padrão e freqüência de operação. Para isso, algumas questões foram consideradas: (a) a rede sem fio tem como função somente o acesso à Internet; (b) o padrão 802.11b, de 2.4 GHz, já pode ser considerado obsoleto, visto que o padrão 802.11g, também de 2.4 GHz, oferece compatibilidade com o padrão legado e oferece maior velocidade; (c) equipamentos com suporte ao padrão 802.11a, de 5 GHZ, ainda têm custo muito superior ao 802.11g; (d) a maioria dos equipamentos portáteis disponíveis suporta o padrão 802.11g. Desta forma, o padrão 802.11g foi o escolhido pela instituição.

3.3.1 Ponto de Acesso

O ponto de acesso escolhido foi o D-Link 3200AP (Fotografia 1 ou Anexo C, para ver o conteúdo da embalagem), fabricado pela empresa D-Link, por diversos motivos: (a) atende aos requisitos da norma IEEE 802.11g; (b) homologado pela Anatel[6] (ver Anexo A) e certificado pelo Instituto Brasileiro de Certificação[7] (ver Anexo B); (c) padronização e interoperabilidade com equipamentos existentes; (d) menor custo em relação a produtos com características semelhantes; (e) suporte técnico disponível no Brasil.

Fotografia 1: Ponto de Acesso D-Link 3200AP
Fonte: o autor.

[6] Maiores informações podem ser encontradas no endereço http://www.anatel.gov.br.
[7] Para maiores informações, consulte o endereço http://www.ibrace.org.br.

Conforme especificações do fabricante, este modelo oferece suporte aos principais mecanismos de segurança: bloqueio de *broadcast* do SSID, filtragem por endereços MAC, WEP, WPA, AES e 802.11i, 802.1x, suporte a múltiplos SSID com VLAN, além de oferecer administração via software próprio (*AP Manager*), *Simple Network Management Protocol* (SNMP), *telnet*, *ssh* ou através de um *browser*. Além disso, possui suporte para *Power over Ethernet* (PoE), que é uma tecnologia que permite a alimentação (corrente elétrica) dos dispositivos através dos cabos de dados existentes (SANCHES, 2005). O fabricante ainda especifica que para uso interno (*indoor*), o sinal de transmissão pode chegar a quase 100 metros do ponto de acesso e para uso externo (*outdoor*) pode chegar aos 500 metros de distância. Obviamente, também é relatado que diversos fatores podem afetar a qualidade do sinal, conforme já foi explicado anteriormente.

3.3.2 Caixa Hermética

Foi escolhido um quadro de comando de 30x20x20 cm (Fotografia 2), produzido pela empresa Cemar, para servir como caixa hermética. As caixas herméticas são construídas com chapa de aço, possuem suporte para montagem e vedação de água. Proporcionam além de segurança física, uma melhor aparência para a instalação dos pontos de acesso.

Fotografia 2: Caixa Hermética 30x20x20 cm
Fonte: o autor.

A caixa vem de fábrica com fecho de pressão, porém este pode ser substituído por fechadura com chave, de forma a garantir maior segurança contra roubos ou vandalismos aos equipamentos.

3.3.3 Sistema de Autenticação

O sistema de autenticação escolhido foi o *hotspot*, uma vez que o principal motivo da criação da rede sem fio é oferecer acesso rápido e facilitado aos utilizadores, única e exclusivamente para pesquisas acadêmicas e acesso a serviços oferecidos de forma *on-line* pela instituição.

Desta forma, os passos necessários para o estabelecimento da conexão à rede sem fio pelo utilizador podem ser resumidos conforme a seguir: (a) usuário se conecta à rede sem fio disponível; (b) digita qualquer endereço para navegação no *browser*; (c) a requisição é enviada ao *hotspot* de autenticação de forma segura (HTTPS); (d) o *hotspot* verifica em uma base de dados se as credenciais de usuário e senha conferem; (e) em caso positivo, autentica o usuário e libera o acesso à rede sob regras de *firewall* dinâmicas.

3.4 INSTALAÇÃO DOS COMPONENTES FÍSICOS

A instalação dos componentes físicos, entendidos como os pontos de acesso e as caixas herméticas, ocorreu conforme o Apêndice B, já descrito anteriormente. Os pontos de instalação foram escolhidos de acordo com testes de sinal efetuados com o auxílio de computador portátil.

Ressalta-se que, por medidas de segurança, foram instaladas caixas herméticas nos locais de maior concentração de pessoas (ver Apêndice C). Em salas administrativas, foram apenas instalados os pontos de acesso com o suporte contido na embalagem do produto (ver Apêndice D).

Para a instalação dos pontos de acesso nas caixas herméticas, foi necessário furar o metal para dar passagem às antenas (pois o metal poderia bloquear de forma significativa o sinal) e ao cabo de rede.

3.5 INSTALAÇÃO / CONFIGURAÇÃO DOS COMPONENTES LÓGICOS

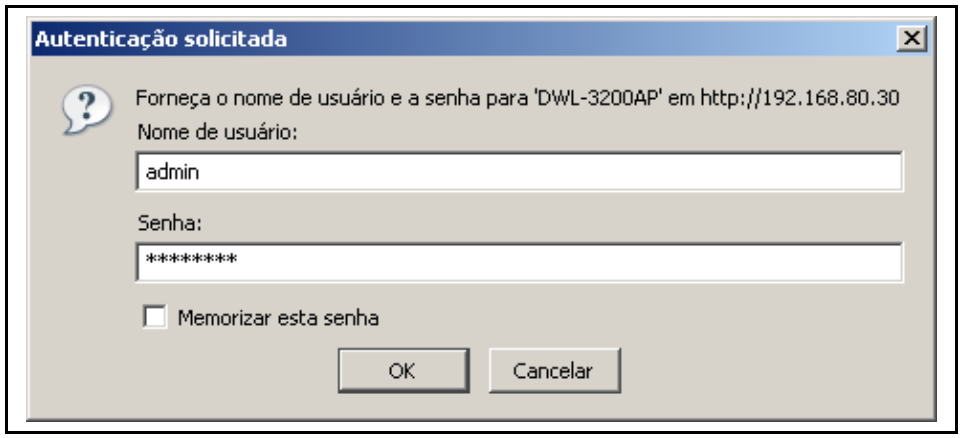
A instalação dos componentes lógicos ocorreu em duas etapas: configuração dos pontos de acesso e configuração do sistema de *hotspot*, as quais serão detalhadas a seguir.

3.5.1 Configuração dos pontos de acesso

Dentre as opções possíveis de configuração dos pontos de acesso, optou-se pela configuração através de um *browser*, pois não necessita da instalação de programas adicionais e a interface *web* é muito agradável e intuitiva.

Uma vez que a instituição optou por utilizar um sistema de *hotspot*, ao invés da autenticação por 802.1x ou então criptografia por WEP ou WPA, poucos passos foram necessários para a configuração dos pontos de acesso. A configuração ocorreu conforme as seguintes etapas:

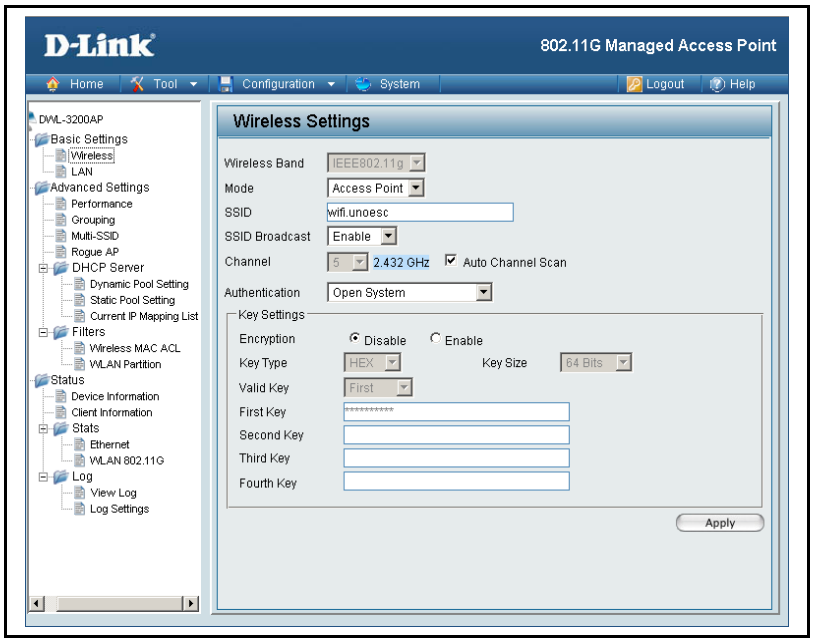
1) Através de um *browser*, apontou-se para o endereço do ponto de acesso e foram inseridas as credenciais de entrada para acessar o ponto de acesso (Desenho 16).



Desenho 16: Tela de autenticação do ponto de acesso
Fonte: o autor.

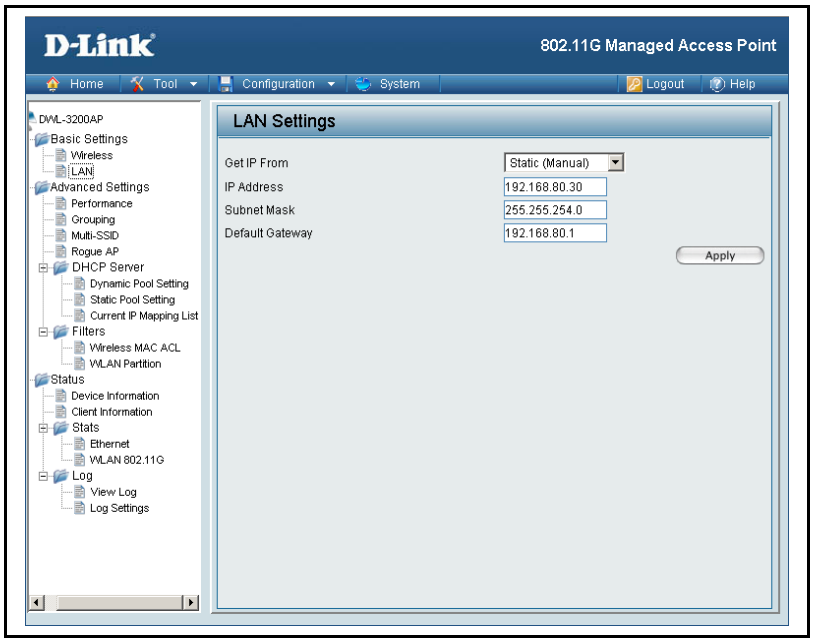
2) Umas das etapas que requerem a maior atenção é a configuração dos parâmetros da rede sem fios (Desenho 17). Nesse passo, configurou-se o ponto de acesso com o modo "Access Point"; SSID "wifi.unoesc" – conclui-se, portanto, que o nome da rede sem fios será wifi.unoesc; habilitou-se o *broadcast* do SSID – pois, pretende-se divulgar a rede a todos os usuários; foi habilitada a opção "Auto Channel Scan" – desta forma, o próprio ponto de

acesso irá procurar o melhor canal disponível, a fim de evitar interferências; o método de autenticação foi configurado para “Open System” – sem criptografia.



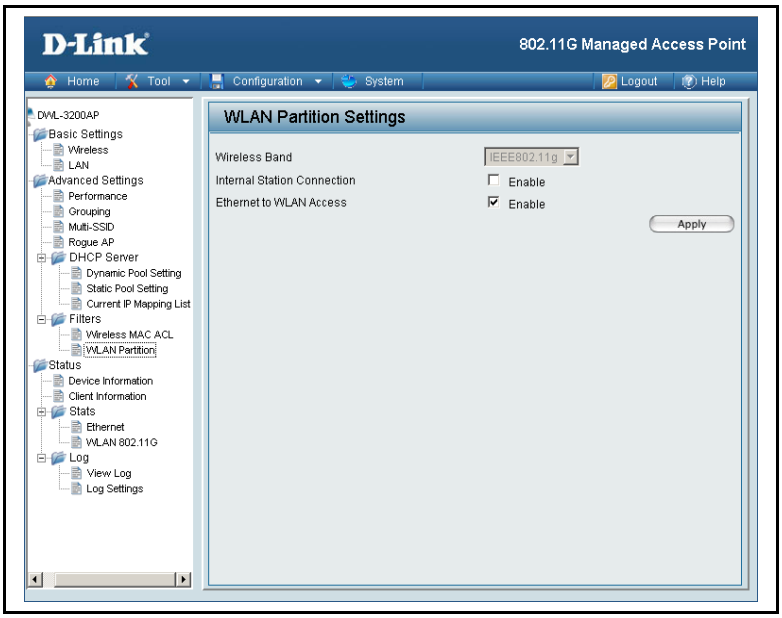
Desenho 17: Tela de configuração dos parâmetros da rede sem fio
Fonte: o autor.

3) Após isso, foram configurados os parâmetros da rede local (Desenho 18). Deve-se realçar que o “Default Gateway” aponta para o servidor de autenticação da rede sem fios. Além disso, a rede sem fios foi configurada de forma a permitir a conexão simultânea de aproximadamente 500 estações.



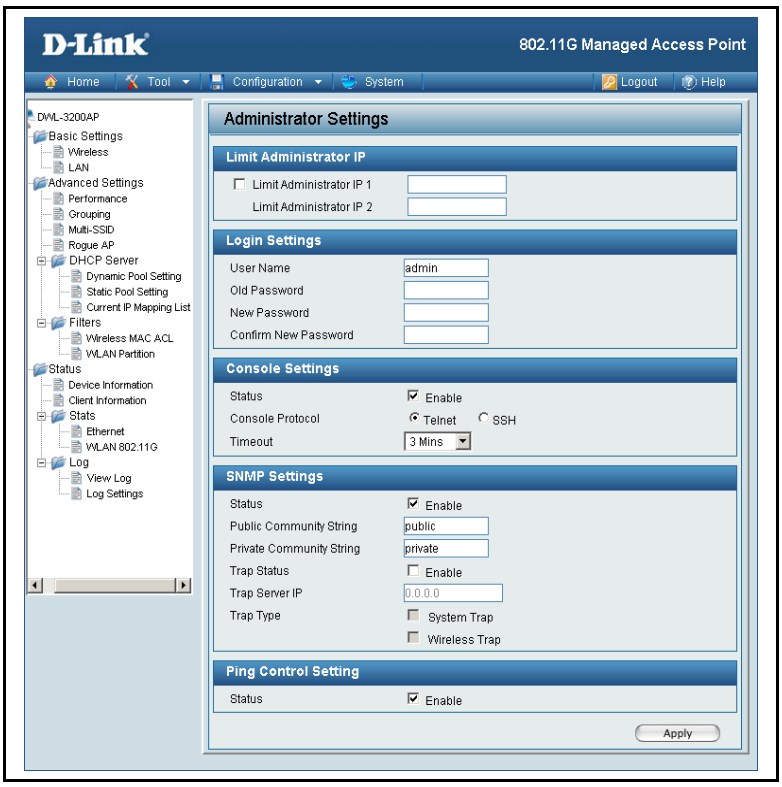
Desenho 18: Tela de configuração dos parâmetros da rede local
Fonte: o autor.

4) O tráfego entre clientes do ponto de acesso foi bloqueado através da desabilitação da opção “Internal Station Connection” (Desenho 19).



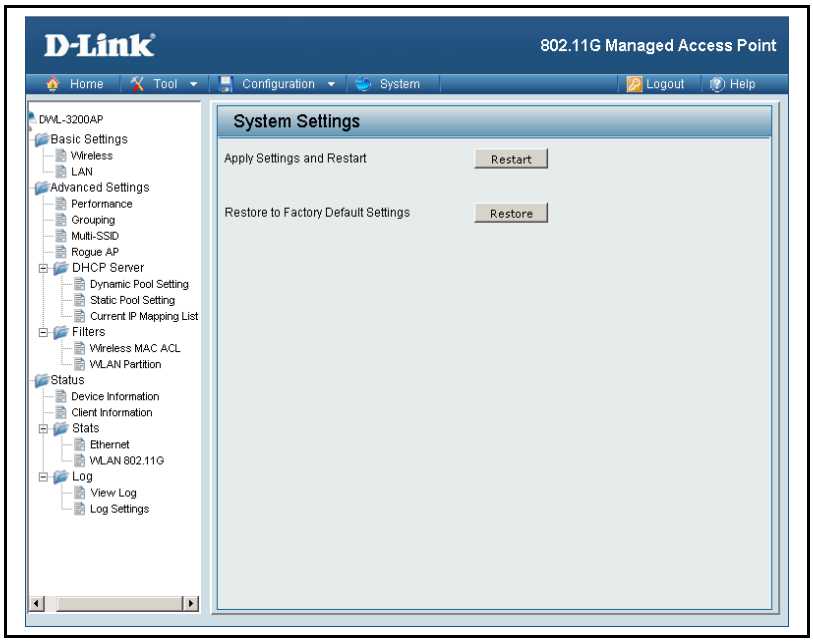
Desenho 19: Tela de bloqueio de tráfego entre clientes
Fonte: o autor.

5) Na configuração dos parâmetros de administração do ponto de acesso, foram habilitadas as configurações de SNMP e a senha para acesso foi alterada para um valor diferente daquele configurado de fábrica (Desenho 20).



Desenho 20: Tela de configurações de administração do ponto de acesso
Fonte: o autor.

6) Por último, as configurações foram salvas de forma definitiva e o ponto de acesso reiniciado, para que as alterações entrassem em vigor (Desenho 21).



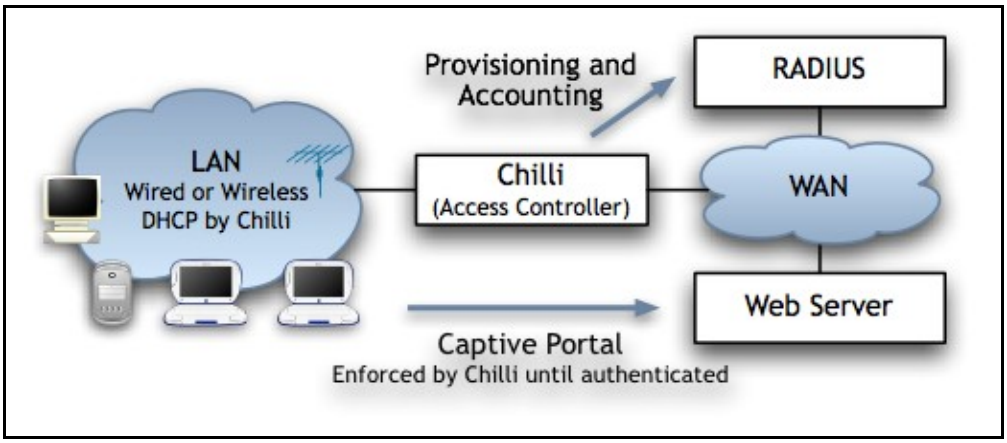
Desenho 21: Tela de gravação das configurações
Fonte: o autor.

Adverte-se, no entanto, que esses parâmetros foram configurados levando em consideração a estrutura de rede, tanto cabeada quanto sem fio, da UNOESC.

3.5.2 Configuração do sistema de *hotspot*

Para realizar a função de *hotspot* foi escolhido o CoovaChilli (Desenho 22), um sistema *open source*[8] de controle de acesso baseado no projeto ChilliSpot. O projeto ChilliSpot foi criado por Jens Jakobsen com o objetivo de autenticar usuários de redes sem fio, entretanto, seu desenvolvimento foi abandonado no ano de 2006. O desenvolvedor David Bird, que colaborava para o ChilliSpot, deu seqüência ao projeto, criando o CoovaChilli, o qual se aproveitou de grande parte do projeto do ChilliSpot e ainda acrescentou diversos novos recursos/funcionalidades (CHILLISPOT, [200-?]; COOVACHILLI, 2008). Esse foi o principal motivo da escolha por esse sistema.

[8] A concepção do termo *open source* procura atender aos seguintes requisitos: redistribuição gratuita, código fonte, trabalhos derivados, integridade do código fonte do autor, não discriminar pessoas ou grupos, não discriminar campos de interesse, distribuição da licença, uma licença não deve ser específica para determinado produto, uma licença não deve contaminar outro software (OPEN SOURCE, c2005).



Desenho 22: Estrutura do CoovaChilli
Fonte: CoovaChilli (2008).

Devido ao fato do CoovaChilli rodar no sistema operacional Linux, escolheu-se a distribuição Slackware, uma vez que grande parte dos servidores da instituição a utiliza como sistema operacional, além do fato de ser a distribuição Linux mais antiga em atividade, comprovando, portanto, sua estabilidade, robustez e eficiência.

Para as tarefas de autenticação, autorização e contabilização dos usuários foi utilizado o FreeRADIUS[9], que é um dos softwares *open source* mais conhecidos e utilizados para a implementação do RADIUS. O RADIUS, conforme já explicado, é utilizado para disponibilizar acesso a redes com autenticação (comparação do nome de usuário e senha com a base de usuários), autorização (após a autenticação, determina se aceita ou não a solicitação) e contabilização (coleta informações de acessos e uso dos recursos) (SANCHES, 2005).

Para armazenamento das credenciais dos usuários e configurações do FreeRADIUS foi adotado o MySQL[10], que é um sistema gerenciador de banco de dados, também *open source*, que utiliza a linguagem SQL (*Structured Query Language*).

Além disso, foi necessária a instalação de um servidor de páginas, pois o CoovaChilli o utiliza para a efetuar a autenticação dos clientes. Para isso, optou-se pelo Apache[11], principalmente devido aos seus recursos e suporte a execução de scripts CGI (*Common Gateway Interface*) e autenticação SSL (*Secure Sockets Layer*).

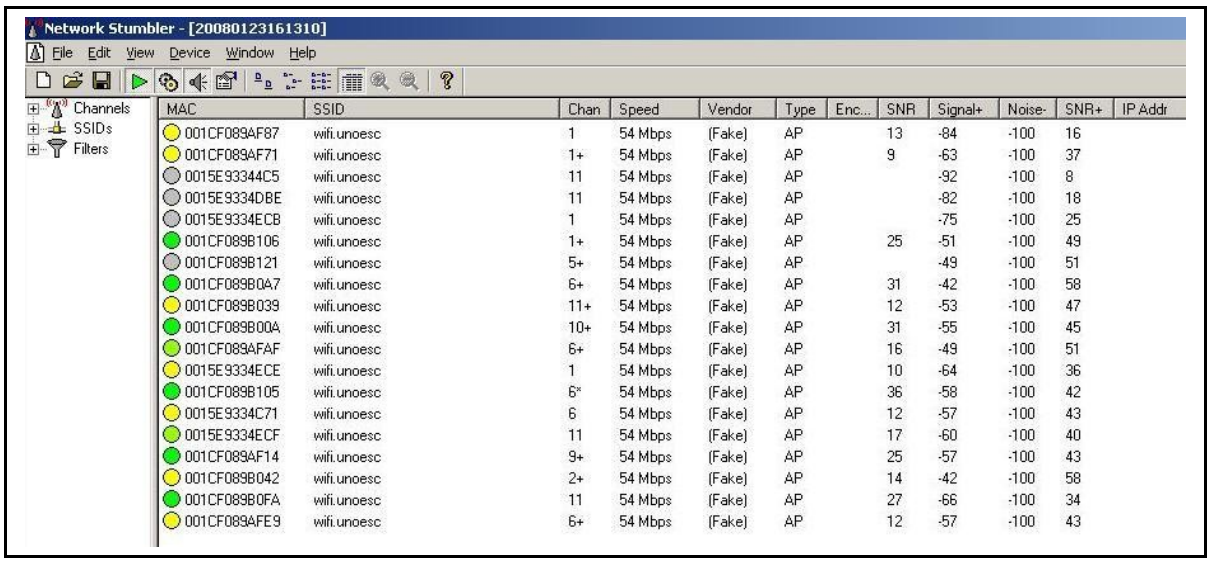
A fim de facilitar a organização deste trabalho, os passos necessários para a instalação, bem como os arquivos principais de configuração das ferramentas, foram anexados no Apêndice E.

[9] Para maiores informações, consulte o endereço http://www.freeradius.org.
[10] Maiores informações podem ser encontradas no endereço http://www.mysql.org
[11] Software igualmente *open source*. Para maiores informações, acesse o endereço http://httpd.apache.org.

3.6 PROCEDIMENTOS DE TESTES, VALIDAÇÃO E MONITORAÇÃO

Para testar e validar os pontos de acesso distribuídos pelo campus, foi utilizado a ferramenta NetStumbler[12], que é um dos mais conhecidos utilitários para detecção de redes sem fio, talvez por ser uma das primeiras ferramentas disponíveis para essa função. Além disso, gera gráficos da qualidade do sinal da rede sem fio, auxiliando no entendimento e identificação de problemas. Entretanto, somente funciona nos sistemas operacionais Windows 98/Me, 2000 e XP (ENGST, FLEISHMAN, 2005; DUARTE, 2003). Para o sistema operacional Linux recomenda-se a utilização da ferramenta Kismet[13], a qual possui função semelhante.

"O NetStumbler informa o SSID, o nível de sinal da rede através das cores (verde – excelente, amarelo – bom, vermelho – ruim), o canal, indica se o WEP está ou não ativado e mais algumas informações" (ANDRADE, 2004, p. 54).



MAC	SSID	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+	IP Addr
001CF089AF87	wifi.unoesc	1	54 Mbps	(Fake)	AP		13	-84	-100	16	
001CF089AF71	wifi.unoesc	1+	54 Mbps	(Fake)	AP		9	-63	-100	37	
0015E93344C5	wifi.unoesc	11	54 Mbps	(Fake)	AP			-92	-100	8	
0015E9334DBE	wifi.unoesc	11	54 Mbps	(Fake)	AP			-82	-100	18	
0015E9334ECB	wifi.unoesc	1	54 Mbps	(Fake)	AP			-75	-100	25	
001CF089B106	wifi.unoesc	1+	54 Mbps	(Fake)	AP		25	-51	-100	49	
001CF089B121	wifi.unoesc	5+	54 Mbps	(Fake)	AP			-49	-100	51	
001CF089B0A7	wifi.unoesc	6+	54 Mbps	(Fake)	AP		31	-42	-100	58	
001CF089B039	wifi.unoesc	11+	54 Mbps	(Fake)	AP		12	-53	-100	47	
001CF089B00A	wifi.unoesc	10+	54 Mbps	(Fake)	AP		31	-55	-100	45	
001CF089AFAF	wifi.unoesc	6+	54 Mbps	(Fake)	AP		16	-49	-100	51	
0015E9334ECE	wifi.unoesc	1	54 Mbps	(Fake)	AP		10	-64	-100	36	
001CF089B105	wifi.unoesc	6*	54 Mbps	(Fake)	AP		36	-58	-100	42	
0015E9334C71	wifi.unoesc	6	54 Mbps	(Fake)	AP		12	-57	-100	43	
0015E9334ECF	wifi.unoesc	11	54 Mbps	(Fake)	AP		17	-60	-100	40	
001CF089AF14	wifi.unoesc	9+	54 Mbps	(Fake)	AP		25	-57	-100	43	
001CF089B042	wifi.unoesc	2+	54 Mbps	(Fake)	AP		14	-42	-100	58	
001CF089B0FA	wifi.unoesc	11	54 Mbps	(Fake)	AP		27	-66	-100	34	
001CF089AFE9	wifi.unoesc	6+	54 Mbps	(Fake)	AP		12	-57	-100	43	

Desenho 23: Detecção dos pontos de acesso da rede sem fios no Bloco E2
Fonte: o autor.

Com o auxílio dessa ferramenta, pode-se perceber que a distribuição dos pontos de acesso de acordo com o Apêndice B mostrou-se muito eficiente, pois em grande parte dos blocos a conexão à rede sem fio pode ocorrer em mais de um ponto de acesso. Isso significa dizer que, caso ocorram problemas com algum ponto de acesso, mesmo assim o serviço continuará a ser oferecido no mesmo local, pelos pontos de acesso adjacentes. Como exemplo dessa situação, pode-se citar o Bloco E2 (Desenho 23), onde seis pontos de acesso foram

[12] Para maiores informações, consulte o endereço http://www.stumbler.net.
[13] Para maiores informações, consulte o endereço http://www.kismetwireless.net.

detectados com qualidade do sinal excelente e, outros tantos com qualidade variando entre média, boa ou sem sinal. Somente para efeitos de comparação, outras imagens podem ser vistas no apêndice F.

A monitoração dos pontos de acesso e do servidor da rede sem fios é feita através do Cacti[14], que é uma ferramenta de rede baseada no gerenciamento de gráficos, os quais podem ser gerados através de informações baseadas, dentre outras maneiras, no protocolo SNMP. Não faz parte do escopo deste trabalho documentar a instalação e configuração da ferramenta e nem mesmo detalhar suas características e funcionalidades. Todavia, foram anexadas imagens nos apêndices G e H para proporcionar uma maior noção das potencialidades deste programa.

Desta forma, é possível efetuar uma manutenção preventiva, por meio da geração relatórios diários, semanais, mensais ou anuais da utilização da rede, processador, memória, tempo de *uptime*, dentre outros; e corretiva, através da detecção de problemas (como por exemplo, queda de um ponto de acesso) em tempo real.

3.7 CUSTOS

Como a UNOESC, campus de São Miguel do Oeste, já possuía uma infra-estrutura de rede existente, grande parte foi aproveitada para a implantação da rede sem fio. Desta forma, alguns locais já contavam com *racks, switches* e cabeamento de rede. Portanto, o Quadro 3 demonstra os custos[15] dos itens adicionais que foram necessários para a implantação da rede sem fio.

Item	Qtde	Preço Unitário (R$)	Preço Total (R$)
Ponto de Acesso D-Link Wireless DWL-3200AP AirPremier 2.4GHz 54 / 108Mbps	22	550,00	12.100,00
Ponto de Acesso Wireless AirPlus XtremeG 2.4GHz 54Mbps / 108Mbps	06	245,00	1.470,00
Caixa Hermética 30x20x20	10	79,00	790,00
Cabo Multilan-Plus 4P Azul Cat. 5e Furukawa (Cx. c/305 m)	04	289,75	1.159,00
Patch Cable 1,5M Cat. 5e Preto 568A	50	5,00	250,00

[14] Para saber mais, acesse o endereço http://www.cacti.net.
[15] Preços estimados relativos a dezembro de 2007. Os preços podem variar conforme o fornecedor.

Bracket 19" Standard Fechado 12U 470MM	01	340,00	340,00
Switch D-Link Corporate 3526 - 24x 10/100Mbps + 2x 10/100/1000Mbps Combo	02	925,00	1.850,00
Servidor Firewall e Autenticação Wireless	01	2.100,00	2.100,00
		Total Geral (R$)	20.059,00

Quadro 3: Custos envolvidos na implantação da rede sem fio
Fonte: o autor.

Destaca-se que o Quadro 3 apresenta somente as despesas com capital (equipamentos). Os custos de mão de obra para instalação e consultoria não são demonstrados, uma vez que dependem do local (região) onde o serviço é executado. Contudo, são descritos os custos mensais com gestão e operação da rede, que compreendem energia elétrica, horas técnicas de um profissional de redes e o *link* de Internet (ver Quadro 4).

Descrição	Qtde	Preço Unitário (R$)	Preço Total (R$)
Energia elétrica dos pontos de acesso (fonte de 48V, 0.4A)[16]	28	2,08	58,24
Energia elétrica do Servidor Wireless[17]	01	51,84	51,84
Horas técnicas do profissional de redes[18]	06	7,50	45,00
Link de Internet Empresarial 1 Mbit	01	1.250,00	1.250,00
		Total Geral (R$)	1.405,08

Quadro 4: Custos mensais da rede sem fio
Fonte: o autor.

Como nota de observação, os equipamentos de uso comum ou simultâneo, tanto para a infra-estrutura de rede cabeada quanto para a infra-estrutura de rede sem fio (tais como, *switches*, estabilizadores, *nobreaks*), não foram considerados.

[16] Valor estimado considerando que os pontos de acesso consumam o valor máximo de 6.42 *watts* (especificado pelo fabricante), custo do *quilowatt*/hora de R$ 0,45 e que os pontos de acesso permaneçam ligados 24 horas por dia durante todo o mês.
[17] Considerando que o servidor consome uma média de 160 watts, custo do *quilowatt*/hora de R$ 0,45 e que fique ligado 24 horas por dia durante todo o mês.
[18] Levando em consideração que o profissional receba um salário de R$ 1.650,00.

4 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

As redes sem fio vêm apresentando um amplo crescimento, relacionado principalmente com a queda dos preços dos dispositivos, crescimento de aplicações para a Internet e facilidade de implementação deste tipo de rede. Nesta monografia foram descritos os passos necessários desde o projeto até a implantação de uma rede sem fio, levando em consideração o campus de São Miguel do Oeste da Universidade do Oeste de Santa Catarina.

Foram delineados nesta pesquisa os conceitos e princípios envolvidos na utilização das redes sem fio de acordo com padrões reconhecidos por órgãos internacionais. Alguns aspectos referentes à segurança de redes sem fio também foram levantados, no entanto, optou-se por não utilizar nenhum mecanismo de criptografia na implantação da rede sem fio, uma vez que o foco desta é voltado somente a pesquisas acadêmicas e portal acadêmico, o qual já oferece segurança por HTTPS.

Estes assuntos investigados auxiliaram na compreensão das arquiteturas possíveis para a implantação (hardware, software e protocolos), definição da quantidade de pontos de acesso necessários para a completa cobertura da área do campus, bem como detalhes técnicos dos elementos de rede. Neste caso, observou-se que o padrão 802.11g, a arquitetura infra-estruturada estendida, a quantidade de 22 pontos de acesso e a separação de redes por VLAN foram as melhores opções para a rede sem fio implantada.

Optou-se pela instalação de um sistema de autenticação por portal, também conhecido como *hotspot*, sobretudo pelas facilidades oferecidas aos usuários finais, já que não exige dos utilizadores quaisquer conhecimentos de configuração ou solicitação de apoio técnico institucional para a obtenção da permissão de acesso.

A instalação dos pontos de acesso e caixas herméticas foi feita em locais estratégicos, definidos com o auxílio de um computador portátil e software de análise de qualidade do sinal, a fim de proporcionar intersecção entre o raio de alcance dos pontos de acesso e cobertura total da área do campus.

Para comprovar a eficiência do sistema, novamente com a utilização de um computador portátil, foram efetuados testes de validação do sinal em diversos locais do campus, bem como a monitoração dos dispositivos envolvidos na implantação da rede sem fio (pontos de acesso e servidor de autenticação).

Como recomendações para trabalhos futuros, uma boa alternativa seria a implantação de um sistema *web* de relatórios, contendo históricos de acessos das conexões efetuadas e

estatísticas de utilização por usuário e/ou grupos. Desta forma, será possível determinar a quantidade de usuários que utilizam a rede, assim como aqueles que mais consomem recursos.

Ainda, visto que os pontos de acesso adquiridos para a solução suportam o recurso de VLAN, sugere-se a criação de uma rede sem fio segura, fazendo uso de criptografia WPA2 com autenticação por IEEE 802.1x, possibilitando ao usuário final optar pelo método de conexão à rede sem fio.

REFERÊNCIAS

3COM. **IEEE 802.11b Wireless LANs**. 2000. Disponível em: <http://www.3com.com/other/pdfs/infra/corpinfo/en_US/50307201.pdf>. Acesso em: 14 abr. 2008.

ABRAS, Gustavo Eduardo; SANCHES, Jayme César Guarenghi. **Wireless Lan**. 2002. 67f. Monografia (Especialização em Redes e Sistemas Distribuídos) – Pontifícia Universidade Católica do Paraná, Curitiba, 2002.

AGUIAR, Paulo Américo Freire. **Segurança em Redes Wi-Fi**. 2005. 79f. Monografia (Graduação em Sistemas de Informação) – Universidade Estadual de Monte Carlos, Monte Carlos, 2005. Disponível em: <http://www.ccet.unimontes.br/arquivos/monografias/73.pdf>. Acesso em: 22 abr. 2008.

ANDRADE, Lidiane Parente. **Análise das vulnerabilidades de segurança existentes nas redes locais sem fio**: um estudo de caso do projeto wlaca. 2004. 75f. Monografia (Graduação em Ciências da Computação) – Universidade Federal do Pará, Belém, 2004. Disponível em: <http://www.lprad.ufpa.br/~margalho/wdeec/tcc.pdf>. Acesso em: 15 abr. 2008.

CARRIÓN, Demetrio de Souza Diaz. **Avaliação de protocolos de autenticação em redes sem fio**. 2005. 164f. Dissertação (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2005. Disponível em: <http://www.ravel.ufrj.br/arquivosPublicacoes/tese_demetrio.pdf>. Acesso em: 23 abr. 2008.

CHILLISPOT. Página do projeto. [200-?]. Disponível em: <http://www.chillispot.info>. Acesso em: 08 mai. 2008.

COOVACHILLI. Página do projeto. 2008. Disponível em: <http://coova.org/wiki/index.php/CoovaChilli>. Acesso em: 08 mai. 2008.

DUARTE, Luiz Otávio. **Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x**. 2003. 55f. Monografia (Graduação em Ciências da Computação) – Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, 2003. Disponível em: <http://www.acmesecurity.org/hp_ng/files/testes_monografias/acme–monografia–Wireless–2003–LOD.pdf>. Acesso em: 15 abr. 2008.

EDNEY, Jon; ARBAUGH, William A.. **Real 802.11 Security**: Wi-Fi Protected Access and 802.11i. [S.l.]: Addison Wesley, 2003. 480p.

ENGST, Adam; FLEISHMAN, Glenn. **Kit do iniciante em redes sem fio**: o guia prático sobre redes Wi-Fi para Windows e Macintosh. São Paulo: Pearson Makron Books, 2005. 460p.

FLECK, Bob; POTTER, Bruce. **802.11 Security**. 1. ed.: O'Reilly, 2002. 208p.

GAST, Matheus. **802.11 Wireless Networks**: The Definitive Guide. 1. ed.: O'Reilly, 2002. 464p.

GRÜNEWALD, Marcus Albert. **Redes sem fio** – Tecnologia, Segurança e Usabilidade. 2005. 119f. Monografia (Especialização em Gestão de Tecnologia da Informação) – Faculdade de Informática e Administração Paulista, São Paulo, 2005.

KUROSE, James F.; Ross, Keith W.. **Redes de computadores e a internet**: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2007. 634p.

LINHARES, André Guedes; GONÇALVES, Paulo André da S.. Uma análise dos mecanismos de segurança em redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w. In: I JORNADA CIENTÍFICA DA UNIBRATEC, 2006, Recife. Disponível em: <http://www.unibratec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf>. Acesso em: 22 abr. 2008.

MIYANO NETO, Roberto**. A evolução dos mecanismos de segurança para redes sem fio 802.11**. 2004. 27p. Trabalho de Graduação (Disciplina Introdução a Computação Móvel) – Curso de Graduação em Engenharia de Computação, Pontifícia Universidade Católica do Rio de Janeiro - PUC-Rio, Rio de Janeiro, 2004. Disponível em: <http://www-di.inf.puc-rio.br/~endler/courses/Mobile/Monografias/04/Miyano-Mono.pdf>. Acesso em: 21 abr. 2008.

ONO, Edson Toshiaki. **Implantação de rede wireless de alta velocidade**. 2004. 108f. Monografia (Graduação em Ciências da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2004.

OPEN SOURCE definition. c2005. Disponível em: <http://www.opensource.org/docs/definition.php>. Acesso em: 15 dez. 2005.

REIS, Hermevaldo Pereira. **Estudo de redes wireless lan em ambiente de laboratório**. 2004. 163f. Trabalho de Graduação (Disciplina de Iniciação Científica) – Curso de Engenharia de Telecomunicação, Departamento de Telecomunicações, Universidade São Marcos – Unimarco, São Paulo, 2004. Disponível em: <http://www.smarcos.br/graduacao/arquivos/trabalho_final_hermevaldo.pdf>. Acesso em: 08 jan. 2008.

RIBAS, Júlio César da Costa. **Perfil de link sem fio em ambiente aberto**: avaliação através de medições. 2002. 175f. Dissertação (Mestrado em Ciências da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2002.

RIGONATTI, Thiago. **Introdução ao mundo wireless**. 2005. Disponível em: <http://www.mobilelife.com.br/artigos/introducao-ao-mundo-wireless>. Acesso em: 07 abr. 2008.

ROSNAM, P.; LEARY, J. **Wireless LAN Fundamentals**. 1. ed.: Cisco Press, 2003. 312p.

RUFINO, Nelson Murilo de Oliveira. **Segurança em redes sem fio**. 2.ed. São Paulo: Novatec, 2005. 224p.

SANCHES, Carlos Alberto. **Projetando redes WLAN**: conceitos e práticas. Rio de Janeiro: Érica, 2005. 342p.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores**: das LANS, MANS e WANS às redes ATM. 2. ed., rev. e ampl. Rio de Janeiro: Campus, 1997. 705p.

SOUZA, Lindeberg Barros de. **Redes de computadores**: dados, voz e imagem. 8. ed. São Paulo: Érica, 2005. 485p.

TANENBAUM, Andrew S.. **Redes de computadores**. Rio de Janeiro: Campus, 2003. 923p.

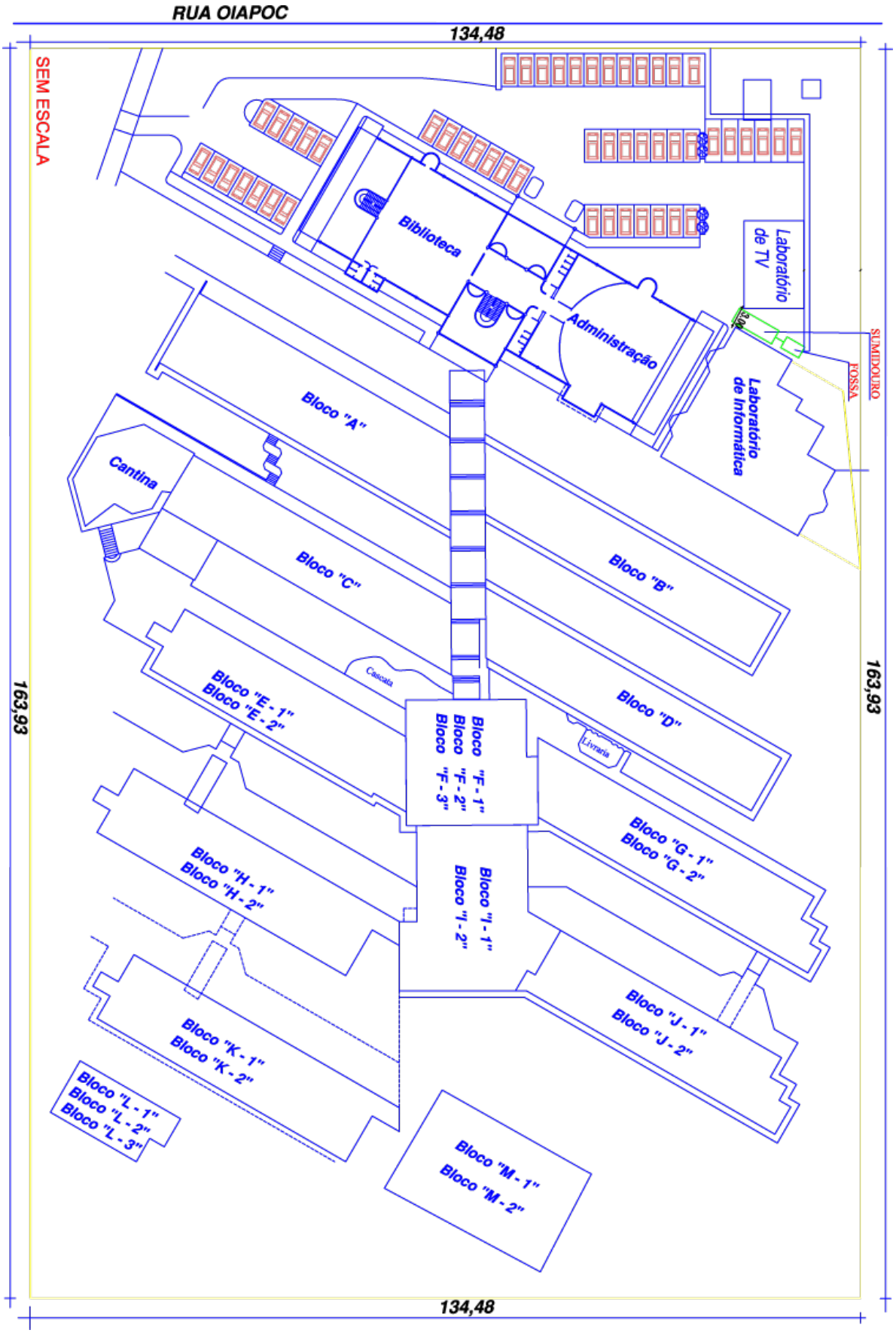
Wi-Fi Alliance. **Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise**. 2005. Disponível em: <http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf>. Acesso em: 22 abr. 2008.

_____. **Get to Know the Alliance**. 2007. Disponível em: <http://www.wi-fi.org/about_overview.php>. Acesso em: 22 abr. 2008.

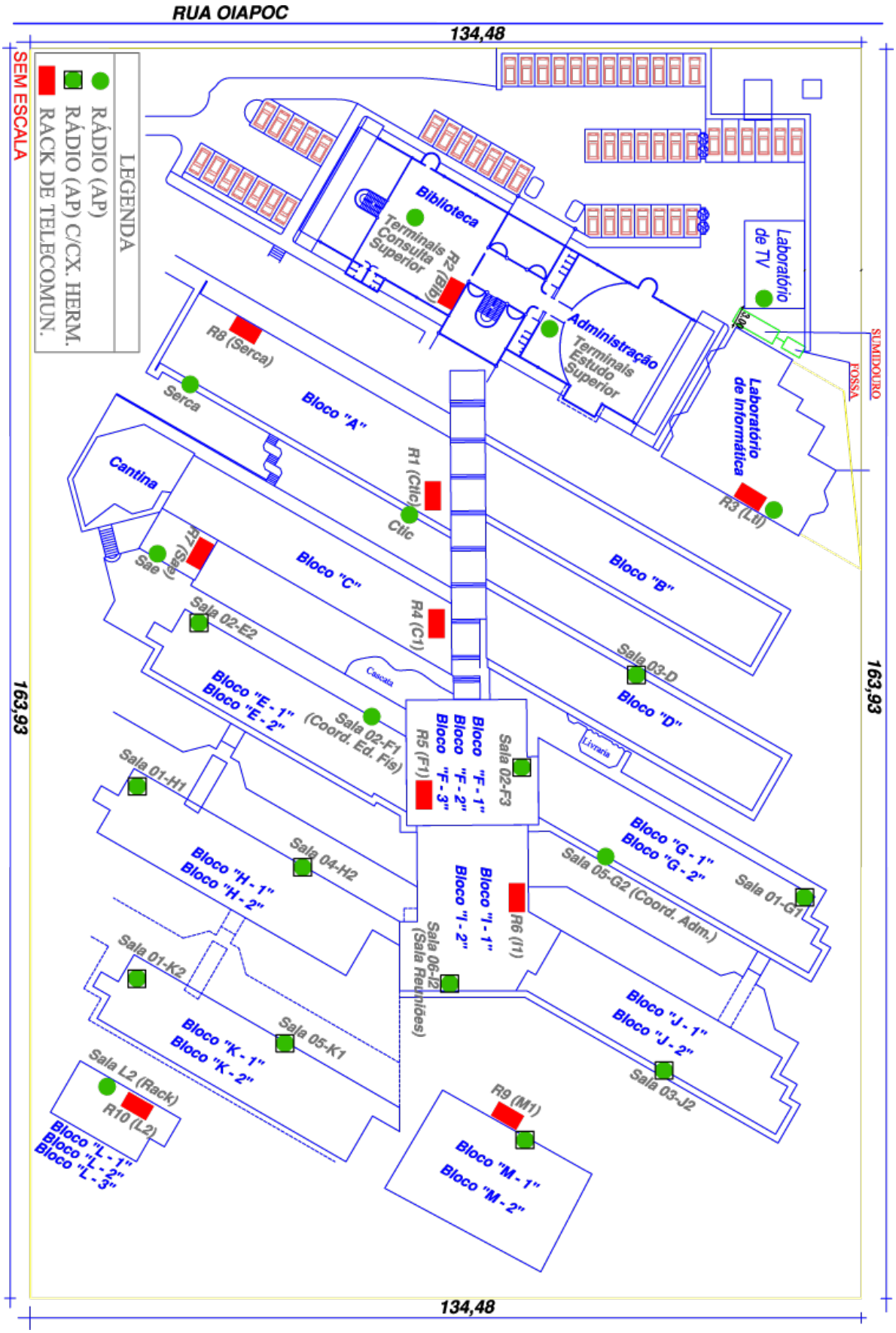
WLANA. **Introduction to Wireless LANs**. 1999. WLANA Resource Center, 1999. Disponível em: <http://sss-mag.com/pdf/wlanintro.pdf>. Acesso em: 14 abr. 2008.

APÊNDICES

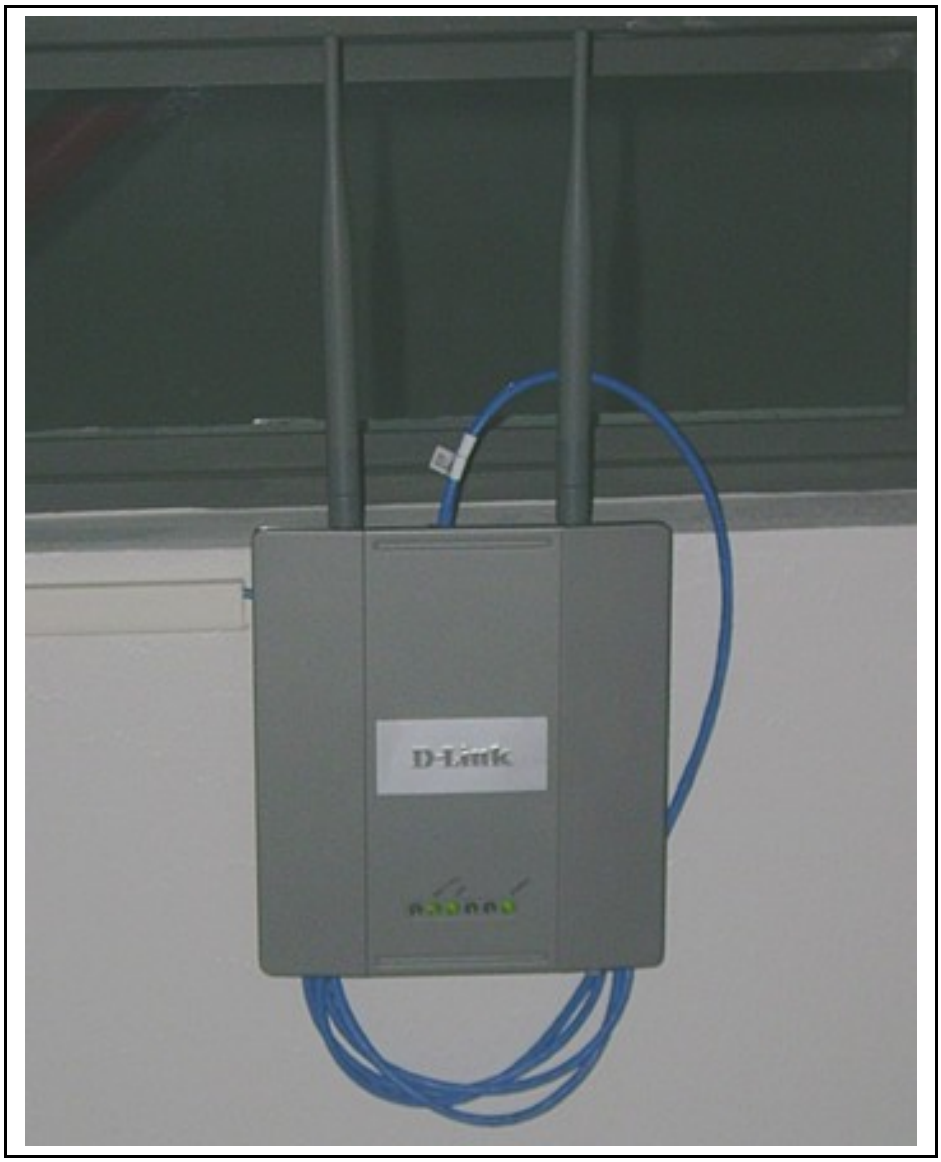
APÊNDICE A – Planta baixa da UNOESC – Campus de São Miguel do Oeste



APÊNDICE B – Planta baixa da UNOESC com APs e *racks* de telecomunicações



APÊNDICE C – Instalação dos pontos de acesso em salas administrativas



APÊNDICE D – Instalação dos pontos de acesso com caixa hermética

APÊNDICE E – Instalação e configuração do sistema de *hotspot*

O sistema operacional utilizado foi o Linux, distribuição Slackware 12. Todos os comandos abaixo foram executados através de um usuário administrador. O delimitador "\" é utilizado para demonstrar que os comandos continuam na próxima linha, sem quebra.

INSTALAÇÃO DO MYSQL:

```
# wget
http://ftp.linux.cz/pub/linux/slackware/slackware-12.0/patches/packages/m
ysql-5.0.51-i486-1_slack12.0.tgz
# installpkg mysql-5.0.51-i486-1_slack12.0.tgz
# su mysql
$ mysql_install_db
$ exit
# chmod 755 /etc/rc.d/rc.mysqld
```

Comandos para iniciar ou parar o servidor MySQL:

```
# /etc/rc.d/rc.mysqld start
# /etc/rc.d/rc.mysqld stop
```

Definição da senha de root do MySQL:

```
# mysqladmin -u root password '<SENHA_ROOT_MYSQL>'
```

INSTALAÇÃO DO FREERADIUS:

```
# wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-
server-2.0.4.tar.gz
# tar xvzf freeradius-server-2.0.4.tar.gz
# cd freeradius-server-2.0.4
# ./configure --prefix=/usr --with-logdir=/var/log \
--with-radacctdir=/var/log/radacct --with-raddbdir=/etc/raddb
# make
# make install
```

Arquivo /etc/rc.d/rc.radiusd (criado para a inicialização do FreeRADIUS):

```
#!/bin/sh
RADIUSD=/usr/sbin/radiusd
test -f $RADIUSD || exit 0
case "$1" in
  start)
        if [ ! -f /var/log/radutmp ]
        then
                :>/var/log/radutmp
        fi
        $RADIUSD
        ;;
  startdebug)
        if [ ! -f /var/log/radutmp ]
        then
                :>/var/log/radutmp
        fi
        $RADIUSD -X
        ;;
  stop)
        killall radiusd 2>/dev/null
```

```
        ;;
  restart)
        killall radiusd 2>/dev/null
        sleep 3
        $RADIUSD
        ;;
  *)
        echo "Usage: $0 {start|startdebug|stop|restart}"
        exit 1
esac
exit 0
```

Comandos para iniciar ou parar o servidor FreeRADIUS:

```
/etc/rc.d/rc.radiusd start
/etc/rc.d/rc.radiusd stop
```

Não foram feitas modificações no arquivo /etc/raddb/radius.conf.

Configuração do arquivo /etc/raddb/clients.conf:

```
client localhost {
        ipaddr          = 127.0.0.1
        secret          = testing123
        require_message_authenticator = no
}
# Servidor de hotspot
client 192.168.100.1 {
        secret          = testing123
        shortname       = coovachilli
        nastype         = other
}
```

Configuração do arquivo /etc/raddb/sql.conf:

```
sql {
        database = "mysql"
        driver = "rlm_sql_${database}"
        server = "localhost"
        login = "radius"
        password = "<SENHA_RADIUS_MYSQL>"
        radius_db = "radius"
        acct_table1 = "radacct"
        acct_table2 = "radacct"
        postauth_table = "radpostauth"
        authcheck_table = "radcheck"
        authreply_table = "radreply"
        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply"
        usergroup_table = "radusergroup"
        deletestalesessions = yes
        sqltrace = no
        sqltracefile = ${logdir}/sqltrace.sql
        num_sql_socks = 5
        connect_failure_retry_delay = 60
        nas_table = "nas"
        $INCLUDE sql/${database}/dialup.conf
}
```

Configuração do arquivo (somente para testes) /etc/raddb/users:

```
# Usuario para teste de autenticacao
```

```
steve   Cleartext-Password := "teste"
```

Configuração do arquivo /etc/raddb/sites-available/default:

```
authorize {
        preprocess
        chap
        mschap
        suffix
        eap {
                ok = return
        }
        sql
        expiration
        logintime
        pap
}
authenticate {
        Auth-Type PAP {
                pap
        }
        Auth-Type CHAP {
                chap
        }
        Auth-Type MS-CHAP {
                mschap
        }
        unix
        eap
}
preacct {
        preprocess
        acct_unique
        suffix
        files
}
accounting {
        detail
        unix
        radutmp
        sql
        attr_filter.accounting_response
}
session {
        radutmp
}
post-auth {
        exec
        Post-Auth-Type REJECT {
                attr_filter.access_reject
        }
}
pre-proxy {
}
post-proxy {
        eap
}
```

Teste de autenticação de usuário:

```
# radtest steve teste 127.0.0.1:1812 0 testing123
```

INTEGRAÇÃO DO MYSQL COM O FREERADIUS:

Criação e importação da estrutura da base radius:

```
# echo "CREATE DATABASE radius;" | mysql -u root -p<SENHA_ROOT_MYSQL>
# mysql -u root -p<SENHA_ROOT_MYSQL> -D radius \
< /etc/raddb/sql/mysql/schema.sql
```

Criação do usuário radius e devidas permissões:

```
# echo "GRANT ALL PRIVILEGES ON radius.* TO radius@localhost identified \
by '<SENHA_RADIUS_MYSQL>';" | mysql -u root -p<SENHA_ROOT_MYSQL>
# echo "FLUSH PRIVILEGES;" | mysql -u root -p<SENHA_ROOT_MYSQL>
```

Exemplo de cadastro de usuário:

```
INSERT INTO radcheck (username,attribute,op,value) VALUES \
('amauri','Cleartext-Password',':=','senhateste');
INSERT INTO radcheck (username,attribute,op,value) VALUES \
('a10767','Cleartext-Password',':=','senhateste2');
INSERT INTO radcheck (username,attribute,op,value) VALUES \
('fabricio','Cleartext-Password',':=','senhateste3');
```

Exemplo de cadastros e parâmetros de grupos de usuários:

→ Criação do grupo wifi_bloq. Os usuários pertencentes a esse grupo terão seu acesso negado:

```
INSERT INTO radgroupcheck (groupname,attribute,op,value) VALUES \
('wifi_bloq','Auth-Type',':=','Reject');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_bloq','Reply-Message',':=','Esta conta foi desativada. Para \
maiores informações, consulte a CTIC ou o LTI.');
```

→ Criação do grupo wifi_acad. Os usuários pertencentes a esse grupo não poderão efetuar conexões simultâneas, possuirão limitação de banda em 10 KB/s para upload e 20 KB/s para download e terão a sessão finalizada em caso de ociosidade por mais de 1 hora:

```
INSERT INTO radgroupcheck (groupname,attribute,op,value) VALUES \
('wifi_acad','Simultaneous-Use',':=','1');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_acad','Idle-Timeout',':=','3600');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_acad','WISPr-Bandwidth-Max-Up',':=','80000');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_acad','WISPr-Bandwidth-Max-Down',':=','160000');
```

→ Criação do grupo wifi_prof. Os usuários pertencentes a esse grupo não poderão efetuar conexões simultâneas, possuirão limitação de banda em 15 KB/s para upload e 30 KB/s para download e terão a sessão finalizada em caso de ociosidade por mais de 2 horas:

```
INSERT INTO radgroupcheck (groupname,attribute,op,value) VALUES \
('wifi_prof','Simultaneous-Use',':=','1');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_prof','Idle-Timeout',':=','7200');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_prof','WISPr-Bandwidth-Max-Up',':=','120000');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_prof','WISPr-Bandwidth-Max-Down',':=','240000');
```

→ Criação do grupo wifi_tecn. Os usuários pertencentes a esse grupo não poderão efetuar conexões simultâneas, possuirão limitação de banda em 15 KB/s para upload e 25 KB/s para download e terão a sessão finalizada em caso de ociosidade por mais de 2 horas:

```
INSERT INTO radgroupcheck (groupname,attribute,op,value) VALUES \
('wifi_tecn','Simultaneous-Use',':=','1');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_tecn','Idle-Timeout',':=','7200');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_tecn','WISPr-Bandwidth-Max-Up',':=','120000');
INSERT INTO radgroupreply (groupname,attribute,op,value) VALUES \
('wifi_tecn','WISPr-Bandwidth-Max-Down',':=','200000');
```

Exemplo da associação de usuários com os grupos:

```
INSERT INTO radusergroup (username,groupname,priority) VALUES \
('amauri','wifi_tecn','1');
INSERT INTO radusergroup (username,groupname,priority) VALUES \
('amauri','wifi_acad','2');
INSERT INTO radusergroup (username,groupname,priority) VALUES \
('fabricio','wifi_prof','1');
```

Exemplo de bloqueio de usuário:

```
INSERT INTO radusergroup (username,groupname,priority) VALUES \
('a10767','wifi_bloq','1');
```

INSTALAÇÃO DO APACHE:

```
# wget
http://ftp.linux.cz/pub/linux/slackware/slackware-12.0/patches/packages/h
ttpd-2.2.8-i486-1_slack12.0.tgz
# installpkg httpd-2.2.8-i486-1_slack12.0.tgz
# chmod 755 /etc/rc.d/rc.httpd
```

Geração dos certificados para a conexão segura (https):

```
# mkdir /etc/apache/ssl
# cd /etc/apache/ssl
# openssl genrsa -out wifi.unoesc.key 1024
# openssl req -new -key wifi.unoesc.key -out wifi.unoesc.csr
# openssl x509 -days 3650 -req -in wifi.unoesc.csr -signkey \
wifi.unoesc.key -out wifi.unoesc.crt
# chmod 700 wifi.unoesc.key
```

Configuração do arquivo /etc/httpd/httpd.conf. Foram acrescentadas as seguintes diretivas para a integração com o CoovaChilli:

```
Alias /auth/ "/usr/local/coovachilli/auth/"
<Directory "/usr/local/coovachilli/auth/">
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>
<Directory "/usr/local/coovachilli/auth/bin/">
        AllowOverride None
        Options ExecCGI
        AddHandler cgi-script .cgi
        Order allow,deny
        Allow from all
</Directory>
Include /etc/httpd/extra/httpd-ssl.conf
```

Configuração do arquivo /etc/httpd/extra/httpd-ssl.conf

```
Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl
SSLPassPhraseDialog  builtin
SSLSessionCache        shmcb:/var/run/httpd/ssl_scache(512000)
SSLSessionCacheTimeout  300
SSLMutex  file:/var/run/httpd/ssl_mutex
<VirtualHost _default_:443>
      DocumentRoot "/srv/httpd/htdocs"
      ServerName wifi.unoescsmo.edu.br:443
      ServerAdmin amauri@unoescsmo.edu.br
      ErrorLog /var/log/httpd/error_log
      TransferLog /var/log/httpd/access_log
      SSLEngine on
      SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:\
      +MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
      SSLCertificateFile /etc/httpd/ssl/wifi.unoesc.crt
      SSLCertificateKeyFile /etc/httpd/ssl/wifi.unoesc.key
      <FilesMatch "\.(cgi|shtml|phtml|php)$">
           SSLOptions +StdEnvVars
      </FilesMatch>
      <Directory "/srv/httpd/cgi-bin">
           SSLOptions +StdEnvVars
      </Directory>
      BrowserMatch ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0
      CustomLog /var/log/httpd/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

Comandos para iniciar ou parar o servidor Apache:

```
/etc/rc.d/rc.httpd start
/etc/rc.d/rc.httpd stop
```

INSTALAÇÃO DO COOVACHILLI:

```
# mkdir coova-svn
# cd coova-svn
# svn checkout http://dev.coova.org/svn/coova-chilli/
# cd coova-chilli
# sh bootstrap
# ./configure --prefix=/usr/local/coovachilli
# make
# make install
# mkdir -p /usr/local/coovachilli/{etc,auth/bin}
# cp doc/firewall.iptables /usr/local/coovachilli/etc/
# cp doc/hotspotlogin.cgi /usr/local/coovachilli/auth/bin/
# cp /usr/local/coovachilli/etc/chilli/defaults \ /usr/local/coovachilli/
etc/chilli/config
# ln -s /usr/local/coovachilli/etc/init.d/chilli /etc/rc.d/rc.coovachilli
```

Configuração do arquivo /usr/local/coovachilli/etc/chilli/config:

```
HS_WANIF=eth0
HS_LANIF=eth1
HS_NETWORK=192.168.182.0
HS_NETMASK=255.255.254.0
HS_UAMLISTEN=192.168.182.1
```

```
HS_UAMPORT=3990
HS_NASID=nas_coovachilli
HS_UAMSECRET=senha_muito_secreta
HS_RADIUS=192.168.100.1
HS_RADIUS2=192.168.100.1
HS_RADSECRET=testing123
HS_UAMALLOW=192.168.100.1
HS_UAMSERVER=192.168.182.1
HS_UAMFORMAT=https://\$HS_UAMSERVER/auth/bin/hotspotlogin.cgi
HS_UAMHOMEPAGE=http://\$HS_UAMLISTEN:\$HS_UAMPORT/www/coova.html
HS_MODE=hotspot
HS_TYPE=chillispot
HS_WWWDIR=/usr/local/coovachilli/etc/chilli/www
HS_WWWBIN=/usr/local/coovachilli/etc/chilli/wwwsh
HS_PROVIDER=wifi.unoesc
HS_PROVIDER_LINK=http://www.unoescsmo.edu.br/
HS_LOC_NAME="CTIC-UNOESCSMO"
HS_LOC_NETWORK="wifi.unoesc"
```

Configuração do arquivo /usr/local/coovachilli/auth/bin/hotspotlogin.cgi. Além da personalização da tela de autenticação (vista mais adiante), foram alterados os seguintes parâmetros:

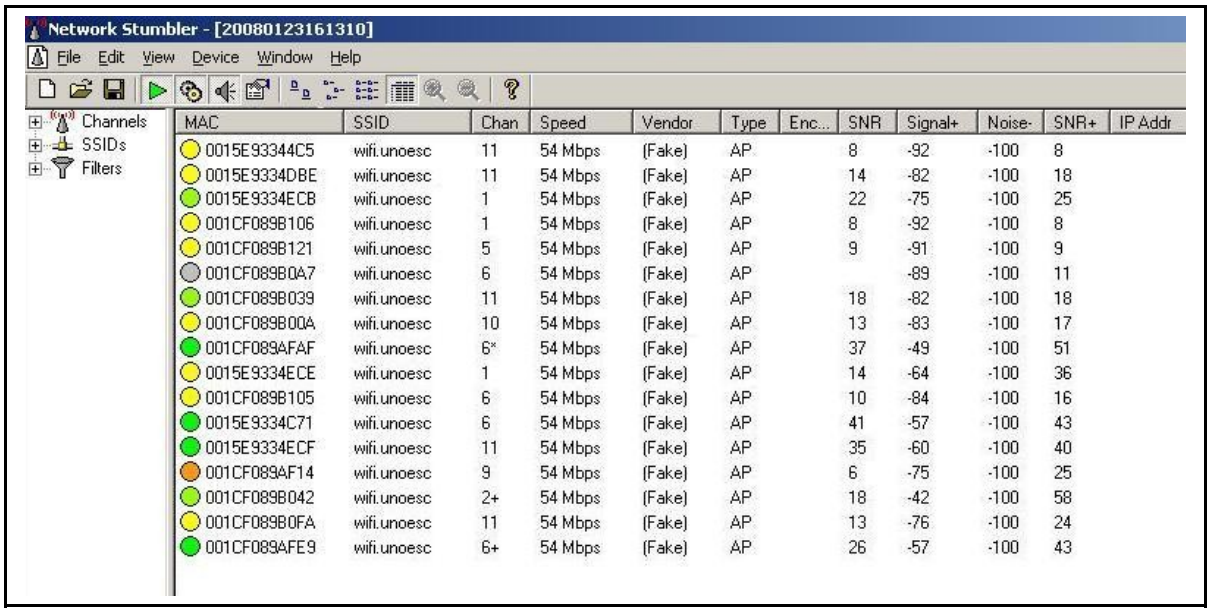
```
$uamsecret = "senha_muito_secreta";
$userpassword=1;
```

Comandos para inicilizar ou parar o CoovaChilli:

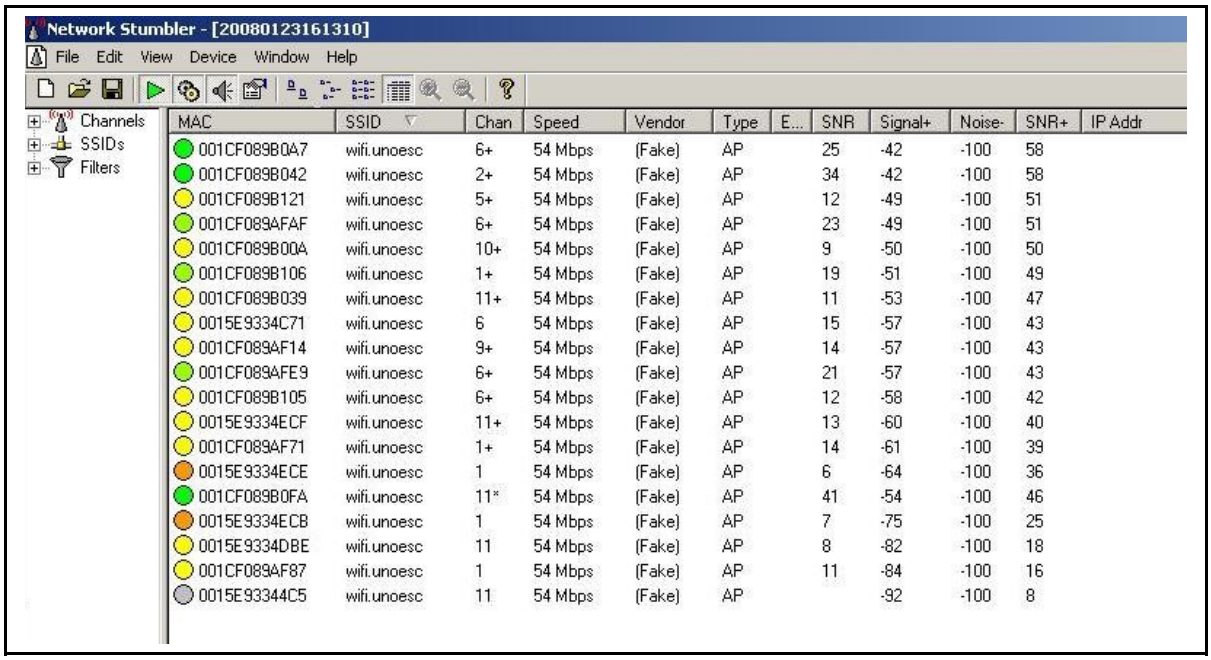
```
/etc/rc.d/rc.coovachilli start
/etc/rc.d/rc.coovachilli stop
```

Foram feitas personalizações no arquivo /usr/local/coovachilli/auth/bin/hotspotlogin.cgi para que, dentre outras características, a tela de autenticação dos usuários da rede sem fio ficasse conforme a seguir:

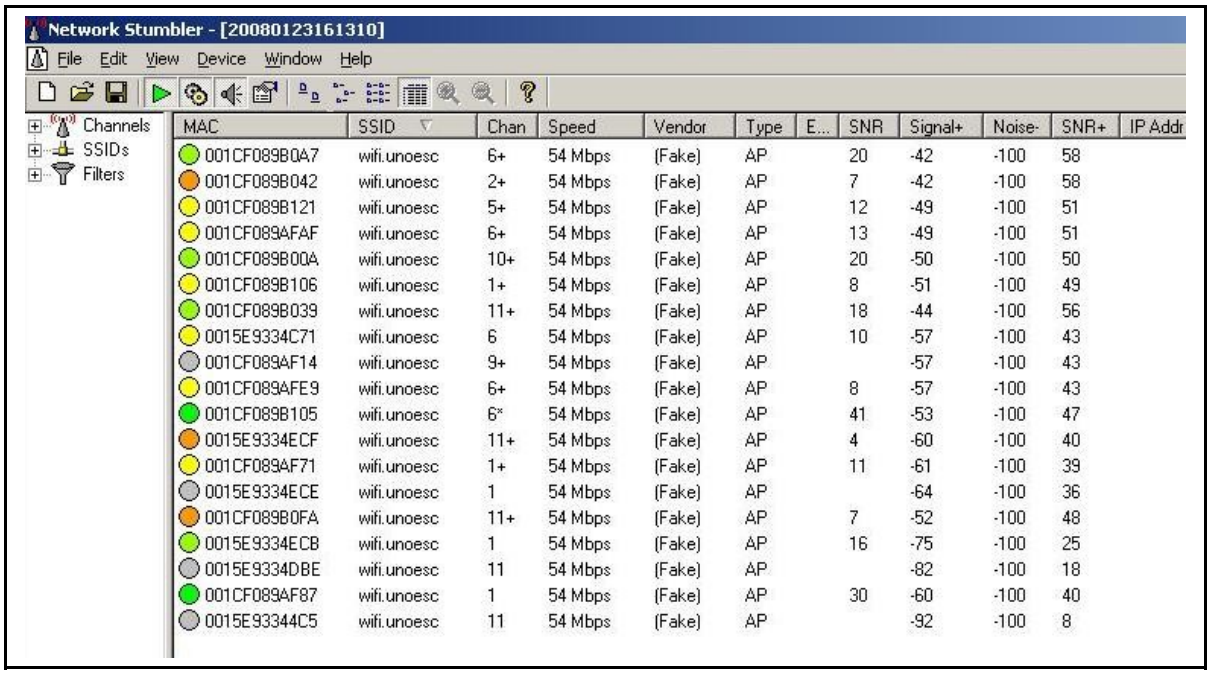
APÊNDICE F – Detecção dos pontos de acesso da rede sem fios



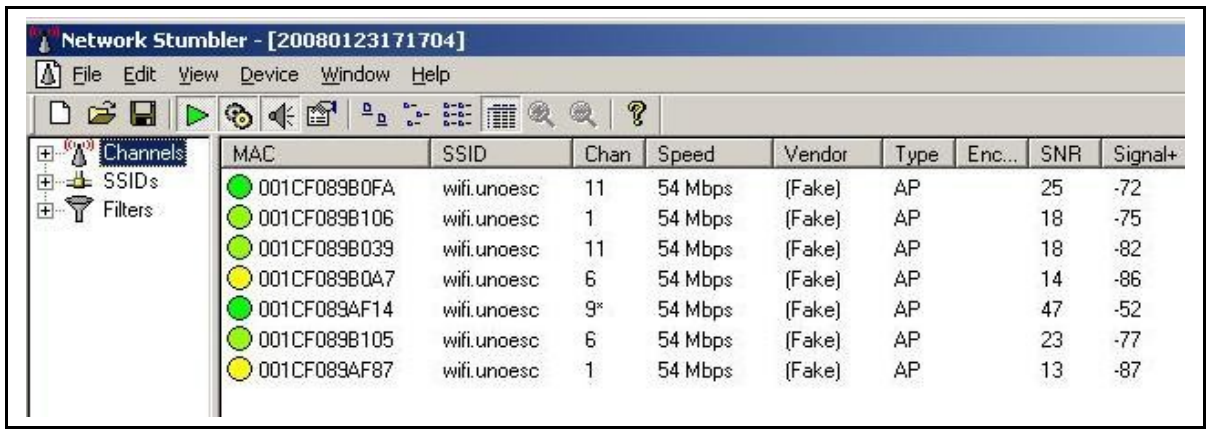
Detecção dos pontos de acesso no Bloco B



Detecção dos pontos de acesso no Bloco F3



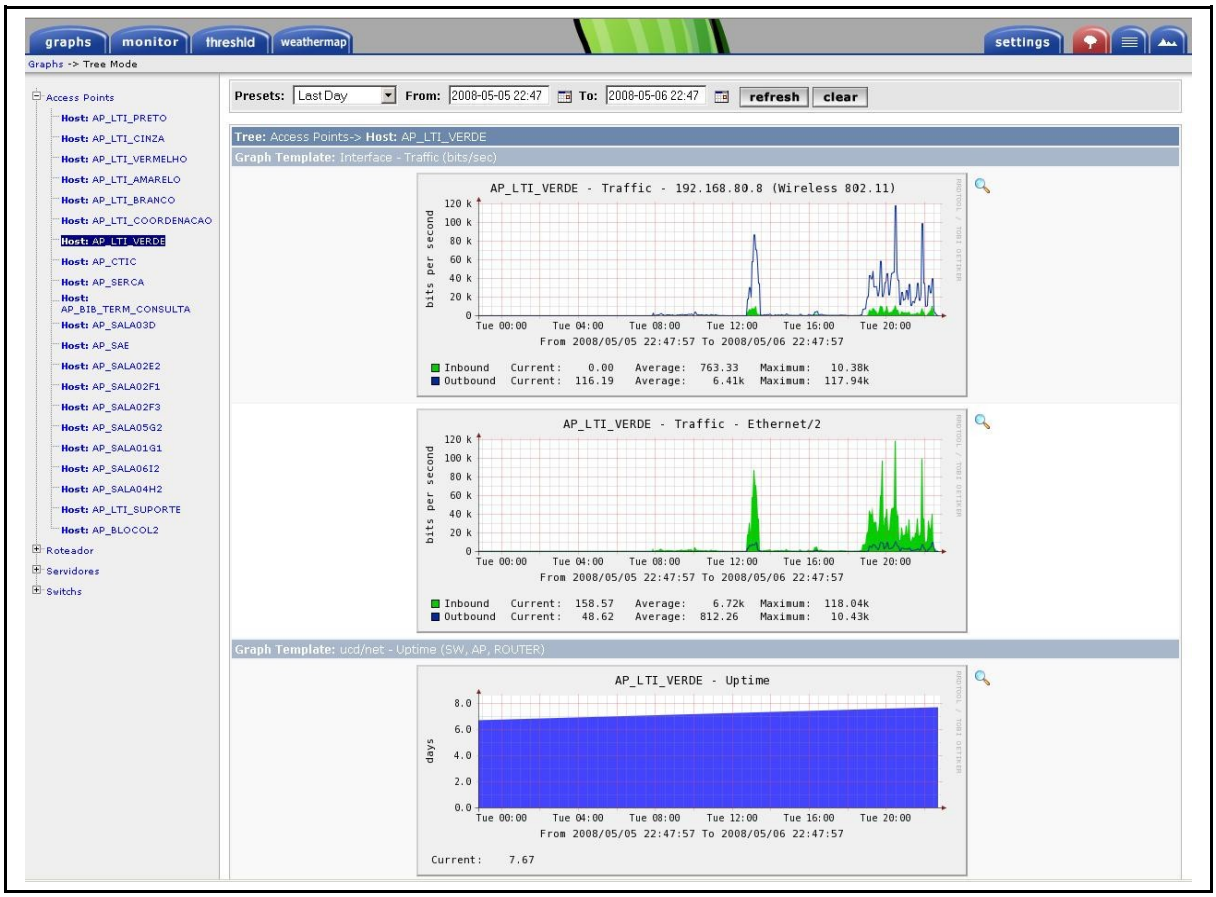
Detecção dos pontos de acesso no Bloco H2



Detecção dos pontos de acesso na cantina universitária

APÊNDICE G – Monitoração em tempo real dos equipamentos da rede sem fios através do Cacti

APÊNDICE H – Monitoração da utilização da rede e *uptime* dos pontos de acesso através do Cacti



ANEXOS

ANEXO A – Homologação do ponto de acesso D-Link 3200AP pela Anatel

REPÚBLICA FEDERATIVA DO BRASIL
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

ANATEL

Certificado de Homologação
(Intransferível)

Nº **1754-06-1931**

Validade: **Indeterminada**

Emissão: **16/11/2006**

Solicitante:
D-LINK BRASIL LTDA.
AV. DAS NAÇÕES UNIDAS 11857 14º ANDAR BROOKLIN NOVO
04578-000 - SAO PAULO - SP

Fabricante:
D-LINK CORPORATION
Nº 8, LI-HSING 7 ROAD, SCIENCE-BASED INDUSTRIAL PARK
HSINCHU - TAIWAN - R.O.C.

Este documento homologa, nos termos do Regulamento para Certificação e Homologação de Produtos para Telecomunicações, aprovado pela Resolução Anate nº 242, de 30 de novembro de 2000, o Certificado de Conformidade nº 01067/06 , emitido pelo **OCD - IBRACE - Instituto Brasileiro de Certificação**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação do serviço ou aplicação a que se destina.

Tipo:
Transceptor de Radiação Restrita - Categoria **II**

Modelo(s):
DWL-3200AP

Serviço/Aplicação:
Redes Locais

Características técnicas básicas:

Faixa de Freqüências Tx (MHz)	Potência Máxima de Saída (W)	Designação de Emissões	Tecnologias	Tipo de Modulação
2400,0 a 2483,5	0,346	12M1X9D	SEQÜÊNCIA DIRETA	DBPSK, DQPSK, CCK
2400,0 a 2483,5	0,238	16M7X9D	OFDM	16QAM, 64QAM

Possui antena incorporada com ganho de 5 dBi. Na instalação do produto devem ser observados os valores de potência E.I.R.P. conforme as seções IX e X do Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita. A antena usada com o transmissor não deve ser operada em conjunto com nenhuma outra antena ou transmissor. Equipamentos operando entre 2400 MHz e 2483,5 MHz e com potência e.i.r.p. superior a 400 mW, em localidades com população superior a 500.000 habitantes, deverão ser licenciados pela Anatel, nos termos da regulamentação específica pertinente a esta faixa de radiofreqüências.

Observações:

Constitui obrigação do fornecedor do produto no Brasil providenciar a identificação do produto homologado, nos termos do art. 39 do Regulamento anexo à Resolução Anatel nº 242, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SGCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Francisco Carlos Giacomini Soares
Gerente Geral de Certificação e
Engenharia do Espectro

ANEXO B – Certificado de conformidade técnica do ponto de acesso D-Link 3200AP pelo Instituto Brasileiro de Certificação

ibrace

INSTITUTO BRASILEIRO DE CERTIFICAÇÃO

Matriz: Av. José de Souza Campos, 763 14º andar - Cambuí - Campinas / SP CEP 13025-320
CNPJ 04.469.737/0001-09 Tel.: 55- 19- 3296-0012
Filial: SRTV/SUL, Quadra 701, Centro Empresarial Brasília, Bloco A Sala 701 Brasília / DF Cep: 70340-907
Tel.: 55-61- 3226-8220

CERTIFICADO DE CONFORMIDADE TÉCNICA DE PRODUTO PARA TELECOMUNICAÇÕES

Número do Certificado: 01067/06 **Data de Certificação:** 01/09/2006 **Validade:** 01/09/2008

Solicitante: D-Link Brasil Ltda **CNPJ:** 04.677.565/0001-69

Endereço: Av. das Nações Unidas, 11857- 14º. Andar – São Paulo - SP

Fabricante: D-Link Corporation **CNPJ:** N/A **Unidade Fabril:** A mesma

Endereço: No.8, Li-Hsing 7 Road, Science-Based Industrial Park, Hsinchu, Taiwan, R.O.C.

Modelo: DWL-3200AP

Tipo de Produto: Transceptor de Radiação Restrita - Modulação Digital **Categoria:** II

Tipo de Serviço: Não Aplicável

Norma(s) Técnica(s) Aplicáveis:
- Resolução Nº365.

Características Técnicas Básicas:
- Faixa de freqüência (Tx): 2400 MHz a 2483,5 MHz (802.11b e 802.11g);
- Potência Máxima de Transmissão: 0,346 W (802.11b) e 0,238 W (802.11g);
- Taxa de Transmissão: 1, 2, 5,5 e 11 Mbit/s (802.11b) e 6, 9, 12, 18, 24, 36, 48 e 54 Mbit/s (802.11g);
- Tipo de modulação: DBPSK, DQPSK e CCK (802.11b) e BPSK, QPSK, 16 QAM, 64 QAM (802.11g);
- Designação de Emissões: 12M1X9D (802.11b) e 16M7X9D (802.11g);
- Ganho da Antena: 5 dBi.

O IBRACE, no uso das atribuições que lhe confere o Ato de Designação nº 19.436, de 28/09/2001, da ANATEL, concede esta certificação ao produto acima informado, baseado em ensaio de tipo e avaliações periódicas quando aplicáveis, sendo que, para sua comercialização, deverá ser obtida a homologação junto à ANATEL e estar devidamente identificado conforme regulamentação pertinente.

Cesar Crisanti Filho
Presidente

Local: Campinas, São Paulo Data de Emissão: 17/10/2006

ANEXO C – Conteúdo da embalagem do ponto de acesso D-Link 3200AP