

UNIVERSIDADE LUTERANA DO BRASIL  
CENTRO DE CIÊNCIAS NATURAIS E EXATAS



**TRABALHO DE CONCLUSÃO DE CURSO:  
SISTEMAS DE INFORMAÇÃO**

ALLAN GABRIEL HENZE

GUAÍBA, NOVENBRO DE 2007

UNIVERSIDADE LUTERANA DO BRASIL  
CENTRO DE CIÊNCIAS NATURAIS E EXATAS

**SEGURANÇA EM SISTEMA DE LOCALIZAÇÃO DE  
ESTAÇÕES SEM FIO IEEE 802.11: AUTENTICAÇÃO E  
ESTAÇÕES MALICIOSAS**

Monografia desenvolvida durante a disciplina de Trabalho de Conclusão de Curso I, apresentada ao Curso de Sistemas de Informação da Universidade Luterana do Brasil, campus Guaíba, como pré-requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador.: André Peres

GUAÍBA, NOVEMBRO DE 2007



## SUMÁRIO

Dados de Identificação .....	3
Lista de Figuras .....	5
Lista de Abreviaturas .....	6
Resumo .....	7
Abstract .....	8
1. INTRODUÇÃO .....	9
2. MOTIVAÇÃO .....	10
3. OBJETIVOS .....	11
4. REDES LOCAIS SEM FIO .....	12
4.1 <i>Wireless</i> .....	12
4.2 <i>Padrões</i> .....	13
4.3 <i>Modelo OSI</i> .....	15
4.4 <i>802.11 e as Camadas do Modelo OSI</i> .....	17
4.5 <i>Autenticação</i> .....	19
5. LOCALIZAÇÃO DE ESTAÇÕES SEM FIO .....	21
5.1 <i>Triangulação</i> .....	22
5.2 <i>Fingerprinting</i> .....	23
5.3 <i>Sistema de Localização de Estações sem Fio</i> .....	23
5.3.1 <i>Detalhes do Sistema Atual</i> .....	25
7. MODELO PROPOSTO .....	27
8. CENÁRIO .....	29
9. ROTEIRO DE TESTES .....	31
10. CONCLUSÕES .....	32
11. REFERÊNCIAS BIBLIOGRÁFICAS .....	33

## LISTA DE FIGURAS

<b>Figura 1</b>	Exemplo de Aplicabilidade de WLAN
<b>Figura 2</b>	Padrões 802.11a, 802.11b e 802.11g
<b>Figura 3</b>	Modelo OSI
<b>Figura 4</b>	Padrões 802.11 e as camadas OSI
<b>Figura 5</b>	Padrões 802.11, as camadas OSI e Autenticação
<b>Figura 6</b>	Triangulação
<b>Figura 7</b>	<i>Fingerprinting</i>
<b>Figura 8</b>	Pontos mapeados no LABIN por <i>Fingerprinting</i>
<b>Figura 9</b>	Localização dos <i>Access Points</i>
<b>Figura 10</b>	Abrangência dos <i>Access Points</i>
<b>Figura 11</b>	Planta baixa LABIN

## LISTA DE ABREVIATURAS

<b>AES</b>	Advanced Encryption Standard
<b>AMPOA</b>	Amplitude of Arrival
<b>AOA</b>	Angle of Arrival
<b>AP</b>	Access Point
<b>ASCII</b>	American Standard Code for Information Interchange
<b>CCMP</b>	Counter Mode CBC-MAC Protocol
<b>DSSS</b>	Direct-Sequence Spread-Spectrum
<b>EAP</b>	Extensible Authentication Protocol
<b>FAST</b>	Flexible Authentication via Secure Tunneling
<b>FHSS</b>	Frequency-Hopping Spread-Spectrum
<b>GSM</b>	Global System for Mobile Communications
<b>HR/FHSS</b>	High-Rate Frequency-Hopping Spread-Spectrum
<b>IAPP</b>	Inter Access Point Protocol
<b>IEEE</b>	Institute of Electrical and Electronic Engineers
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Standards Organization
<b>LAN</b>	Local Area Network
<b>LEAP</b>	Lightweight Extensible Authentication Protocol
<b>LLC</b>	Logical Link Control
<b>MAC</b>	Media Access Control
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing
<b>OSI</b>	Open Systems Interconnection
<b>PEAP</b>	Protected Extensible Authentication Protocol
<b>QoS</b>	Quality of Service
<b>SIM</b>	Subscriber Identity Module
<b>TKIP</b>	Temporal Key Integrity Protocol
<b>TLS</b>	Transport Layer Security
<b>TOA</b>	Time of Arrival
<b>WDS</b>	Wireless Distribution System
<b>WEP</b>	Wired Equivalency Privacy
<b>WLAN</b>	Wireless Local Area Network
<b>WPA</b>	Wi-Fi Protected Access

## RESUMO

A ULBRA - Universidade Luterana do Brasil – *campus* Guaíba possui um sistema de localização de estações sem fio padrão IEEE 802.11. Atualmente, tal sistema utiliza uma técnica conhecida como *fingerprinting* para determinar a posição em que as estações sem fio se encontram em suas dependências. O mesmo, entretanto, utiliza apenas informações provenientes das estações, caracterizando, assim, uma falha de segurança. Tendo em vista a necessidade de aprimorar a segurança, este TCC se propõe a aplicar uma nova camada de autenticação (baseada na localização das estações) e demonstrar como é possível tornar o ambiente mais seguro, confiável e gerenciável.

**Palavras-chaves:** Wireless, WLAN, 802.11, *Fingerprinting*, Autenticação baseada na localização.

## **ABSTRACT**

ULBRA - Universidade Luterana do Brasil - campus of Guaíba has a wireless stations location system IEEE 802.11 standard. Today, this system uses a technique known as fingerprinting to determine the position within the university area in which the wireless stations are. However, this pattern uses only the information that comes from the stations, what characterizes a security failure. So, being necessary an improvement in the security, this TCC proposes to apply a new authentication layer (stations location based) and demonstrate how it is possible to have a safer, more secure and manageable environment.

**Key-words:** Wireless, WLAN, 802.11, Fingerprinting, Location-based authentication.

## 1. INTRODUÇÃO

Atualmente é vertiginosa a velocidade com que novas tecnologias vêm se disseminando. A cada ano surgem no mercado novas soluções que podem trazer benefícios estratégicos, caso utilizados corretamente, tais como *Access Point* (pontos de acesso wireless), Máquinas Virtuais, Telefonia IP, Frameworks, *Appliances* de rede, entre outros.

Desta forma, a Universidade Luterana do Brasil - ULBRA - *campus* Guaíba, presentemente, dispõe de um sistema de localização de estações sem fio que apresenta, de forma gráfica, a localidade em que determinada estação se encontra dentro da área de abrangência da rede *wireless*, porém, tal informação pode ser errônea. A sua precisão está diretamente interligada com a confiabilidade e integridade das informações passadas pelas estações móveis, visto que as estas podem distorcê-las, de forma mal intencionada, antes de enviá-las ao servidor.

Este TCC aborda, de forma objetiva, embasamentos teóricos referentes à redes *wireless*, padrões da família IEEE 802.11, o relacionamento entre os padrões utilizados e as camadas do modelo OSI, os métodos e técnicas utilizados para se localizar uma estação sem fio dentro de um determinado perímetro de abrangência e o desenvolvimento de uma nova etapa no processo de autenticação, baseando-se na localização das estações.

## 2. MOTIVAÇÃO

Nos dias de hoje, a ULBRA *campus* Guaíba, possui uma cobertura de rede wireless relativamente ampla. Com o passar do tempo, naturalmente, a preocupação com segurança de rede vem crescendo de forma intensa. Desta forma, o primeiro passo, visando o propósito de gerência de rede, foi dado no momento em que um sistema capaz de localizar estações sem fio dentro de suas dependências foi desenvolvido.

Assim sendo, o próximo passo seria a possibilidade de limitar o acesso apenas a estações que estejam fisicamente dentro da universidade e que os responsáveis pela administração da rede tivessem ciência e concordassem com que uma determinada estação tivesse acesso ao serviço *wireless* oferecido.

Face ao exposto, este TCC visa ampliar conhecimentos na área de segurança de rede e ambiente *wireless* e implementar a melhoria de segurança necessária para que tais funcionalidades sejam concretizadas.

### **3. OBJETIVOS**

Além do desenvolvimento acadêmico, que considero o principal objetivo deste TCC – por oferecer oportunidades de colocar em prática algumas teorias já abordadas em sala de aula – visto implementar um novo método de autenticação em redes *wireless*, baseado na localização.

Adquirir novos conhecimentos também pode ser considerado um dos objetivos centrais deste trabalho, visto que muitas das tecnologias inerentes ao processo possuem uma complexidade relativamente elevada e não foram abordadas no meio acadêmico até então.

## 4. REDES LOCAIS SEM FIO

### 4.1 WIRELESS

Atualmente, o conceito mais básico de *wireless* está extremamente difundido: comunicação sem fio. Com uma visão um pouco mais técnica, podemos dizer que wireless é, na realidade, toda e qualquer comunicação entre dois ou mais pontos distintos utilizando ondas eletromagnéticas onde não são utilizados fios como meio físico.

Segundo (PAHLAVAN, 2002), WLAN (*wireless local area network*) ou rede local sem fio é exatamente o que o nome se refere. Trata-se de aplicar a tecnologia *Wireless* como meio de comunicação em uma rede local de computadores, substituindo o cabeamento convencional. Desta forma, todas as funcionalidades das LAN também estão presentes na WLAN, incluindo compartilhamento de arquivos, compartilhamento de periféricos, acesso à internet entre outros recursos, como exemplificado na figura 1, disponível em (3COM, 2003).

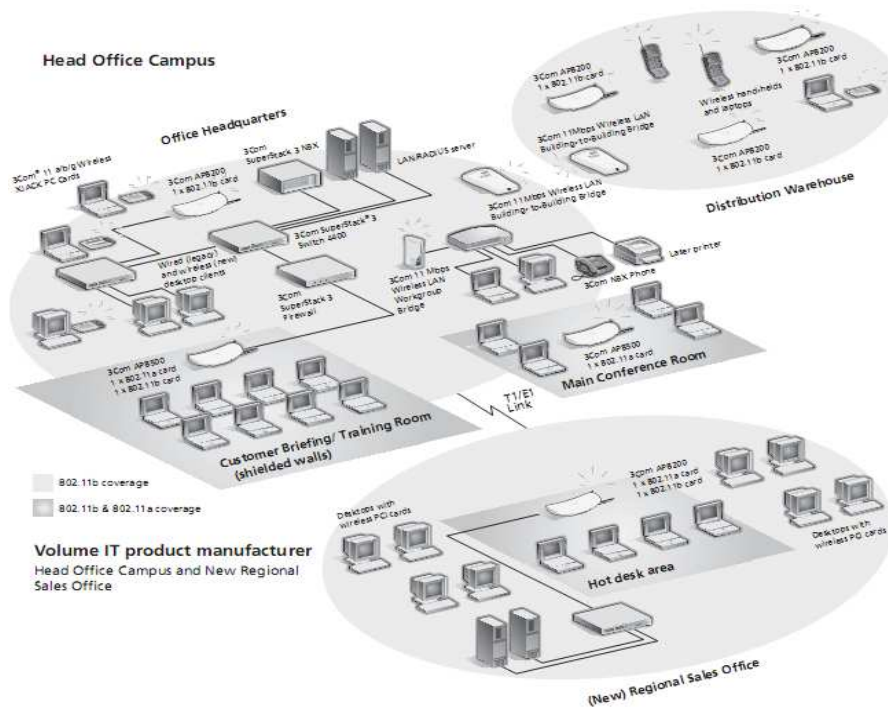


Figura 1 – Exemplo de aplicabilidade de WLAN

Visto o amplo crescimento das tecnologias e a proliferação das WLANs (por sua simplicidade de configuração básica e não exigir muitos recursos) foram determinados padrões para que sua utilização fosse eficaz e coerente. Assim sendo, através da IEEE (*Institute of Electrical and Electronics Engineers*) foi desenvolvido o padrão 802.11 para rede wireless.

## 4.2 PADRÕES

O padrão 802.11 é um membro da família IEEE 802, que trata de especificações para as tecnologias de redes locais (LAN). De acordo com as informações encontradas em (3COM, 2003), o padrão IEEE 802.11 original, estabelecido em junho de 1997, definia um sistema cuja banda fosse 2,4GHz com um *data rate* máximo de 2Mbps. Esta tecnologia ainda existe, mas não deve ser considerada para novas implantações. Hoje em dia, existem duas categorias básicas no padrão IEEE 802.11. A primeira são aquelas que especificam os protocolos fundamentais para um sistema wireless completo: 802.11a, 802.11b e 802.11g. Já a segunda categoria, é composta por extensões endereçadas às fragilidades ou para adicionar novos atributos aos padrões da primeira categoria. São eles: 802.11d, 802.11e, 802.11f, 802.11h, 802.11i, 802.11j. A tabela 1, também disponível em (3COM, 2003), mostra maiores detalhes a respeito da primeira categoria:


	Standard	Radio Band	Modulation	Max. Link Coverage	Max. Data Rate	Max. # Non-overlapping channels	Other Issues
More established standard  Newer standard	802.11b	2.4 GHz	DSSS	100m/328ft	11 Mbps	3	• 802.11b networks have the largest installed base.
	802.11a	5 GHz	OFDM	50m/164ft	54 Mbps	12 (fewer in some regions)	• Needs 802.11 extensions to be used in some regions (e.g., EMEA)
	802.11g	2.4 GHz	OFDM	100m/328ft	54 Mbps	3	• Backward-compatible with 802.11b • Fully ratified

Figura 2 – Padrões 802.11a, 802.11b e 802.11g.

É importante salientar que existem algumas considerações a serem feitas quando trabalhando com estes padrões. Como por exemplo:

- 802.11b: não indicado para aplicações que utilizem muita banda, porém se a intenção é uma maior cobertura, deve ser considerada, além do custo dos equipamentos que utilizem este padrão ser inferior aos dos demais.

Como principal desvantagem, pode-se citar que a taxa de transferência deste padrão é muito baixo e, por utilizar a frequência 2,4GHz (mesma utilizada por alguns equipamentos de telefone sem fio e Bluetooth), pode ter sua capacidade reduzida e sofrer interferências.

- 802.11a: indicado nos casos de aplicações como voz (telefones IP) e vídeo, em função da alta taxa de transmissão. O grande número de possíveis canais distintos de frequência permite que vários *Access Points* sejam alocados uns mais próximos dos outros sem que haja interferência. Como desvantagem, pode-se citar que não é compatível com o padrão 802.11b e seu custo é mais elevado para se proporcionar semelhante cobertura do sinal.

- 802.11g: indicado quando se necessita executar aplicações que consomem muita banda e uma área de cobertura mais abrangente (semelhante ao padrão 802.11b). Além disto, ainda oferece compatibilidade com equipamentos padrão 802.11b. Como desvantagens têm-se alta possibilidade de interferência (por utilizar frequência semelhante ao padrão 802.11b) e, quando se operam ambos os padrões em conjunto, sua capacidade fica reduzida ao do 802.11b.

Os demais padrões seguem abaixo:

- 802.11d: garante a interoperabilidade em WLANs cujos países ainda não possuem o padrão 802.11 aplicado.

- 802.11e: define níveis de QoS (*Quality of Service*) para aplicações como áudio e vídeo.

- 802.11f: trata-se do IAPP (*Inter Access Point Protocol*). Possibilita a transição entre APs em um mesmo domínio, sem a necessidade de reassociação. Utiliza mecanismos de WDS (*Wireless Distribution System*).

-802.11h: adiciona um melhor controle entre potência de transmissão e seleção de canais no padrão 802.11a.

-802.11i: prove melhoria de segurança, incluindo a utilização do protocolo de autenticação 802.1x e algoritmo criptográfico AES (*Advanced Encryption Standard*).

-802.11j: adição dos endereços canal de 4.9GHz para 5GHz para o padrão 802.11 (apenas no Japão).

### 4.3 MODELO OSI

Nos primórdios das redes de dados, as soluções para comunicação entre computadores eram proprietárias, ou seja, apenas o próprio fabricante era capaz de permitir a comunicação entre diferentes equipamentos.

Desta forma, segundo (WIKIPEDIA, 2007) para que a comunicação fosse viabilizada entre equipamentos de fabricantes diferentes, a ISO (*International Standards Organization*) desenvolveu um modelo de referência conhecido como OSI (*Open Systems Interconnection*). Este modelo divide-se em 7 camadas hierárquicas, ou seja, cada uma destas camadas utiliza suas próprias funções ou da camada anterior, ilustrado pela figura 3.

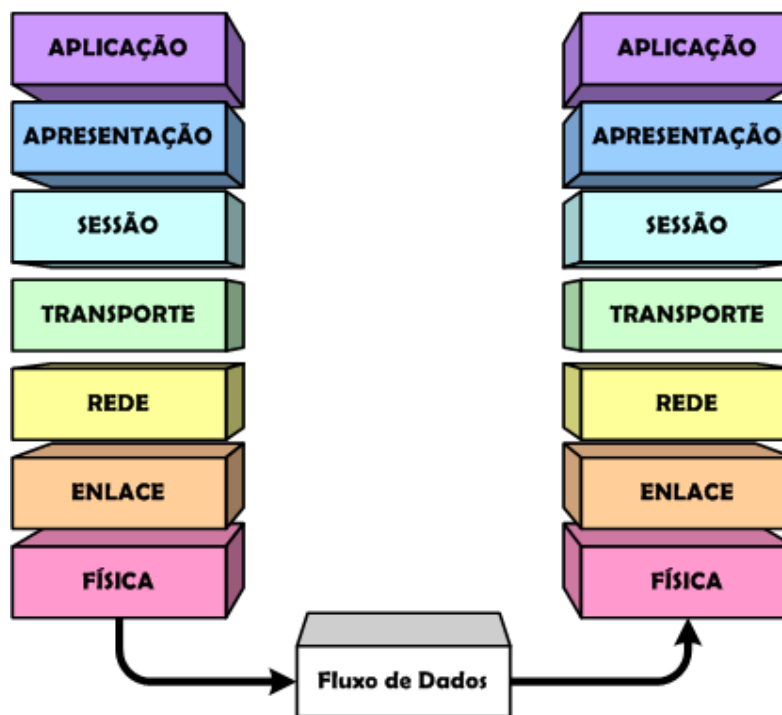


Figura 3 – Modelo OSI

Seguem, abaixo, maiores detalhes de cada uma das camadas do modelo OSI, de acordo com o apresentado por (PICCININ, 2007) e (DUBENDORF, 2003):

**Camada Física (*Physical Layer*)** - é responsável por prover características físicas, elétricas, funcionais e procedimentos para ativar, manter

e desativar conexões entre duas partes. Está diretamente ligada à transmissão dos dados por um canal de comunicação.

Trata-se da única camada que possui acesso físico ao meio de transmissão da rede devendo, portanto, se preocupar com fatores como as especificações elétricas, mecânicas, funcionais e procedurais da interface física entre o equipamento e o meio de transmissão, ou seja, a camada física tem como função básica a adaptação do sinal ao meio de transmissão.

**Camada de Enlace (*Data Link Layer*)** - tem por função detectar e, opcionalmente, corrigir erros que possam ocorrer no nível físico. É responsável, ainda, pela transmissão e recepção de quadros e pelo controle de fluxo. Ela também estabelece um protocolo de comunicação entre sistemas diretamente conectados.

**Camada de Rede (*Network Layer*)** - é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos (ou IP), de forma que os pacotes consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades.

**Camada de Transporte (*Transport Layer*)** – como função principal, esta camada aceita dados da camada de sessão, os quebra em unidades menores (caso seja necessário), os encaminha para a camada de rede e assegurar que todas as partes chegarão corretamente ao outro extremo. Protocolos de transporte são empregados para estabelecimento, manutenção e liberação de conexões de transporte que representam um caminho duplo para os dados entre dois endereços de transporte.

**Camada de Sessão (*Session Layer*)** – Através de “conexões virtuais” (estabelecidas quando a estação transmissora troca informações com a receptora) esta camada é capaz de gerenciar as atividades das camadas inferiores, informando que deve se iniciar e manter um link de comunicação. Seria algo semelhante ao que ocorre quando alguém se conecta a uma rede. Uma vez logado, a conexão é mantida até que o logoff seja executado, mesmo sem acesso contínuo à rede.

**Camada de Apresentação (*Presentation Layer*)** – converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Um exemplo comum é a conversão do padrão de caracteres (código de página) quando, por exemplo, o dispositivo transmissor usa um padrão diferente do ASCII, por exemplo. Pode ter outros usos, como compressão de dados e criptografia.

**Camada de Aplicação (*Application Layer*)** – opera como interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede. Por exemplo, ao solicitar a recepção de e-mails através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede efetuando tal solicitação. Tudo nesta camada é direcionada aos aplicativos.

#### 4.4 802.11 E AS CAMADAS DO MODELO OSI

A figura 4, baseada em (3COM, 2000), demonstra em que ponto os padrões da família 802.11 operam dentro do modelo OSI.

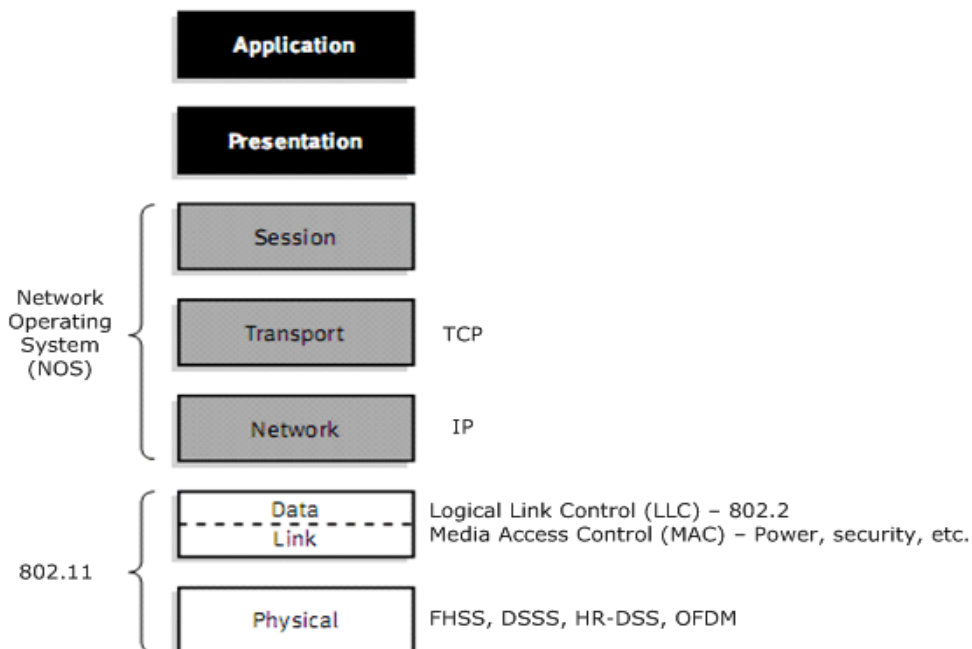


Figura 4 – Padrões 802.11 e as camadas OSI

Segundo (GAST, 2002), poder-se-ia dizer que o IEEE 802.11 é apenas mais uma camada de link que pode utilizar o 802.2/LLC (*Logical Link Control*), o que omitiria alguns detalhes. Entretanto, são estes detalhes que fazem com que este padrão funcione tão bem. A especificação original do 802.11 incluía o 802.11 MAC (*Media Access Control*) e duas camadas físicas: FHSS (*Frequency-Hopping Spread-Spectrum*) e DSSS (*Direct-Sequence Spread-Spectrum*). Revisões posteriores à 802.11 adicionaram outras camadas físicas, como, por exemplo, o 802.11b, que especifica o HR/DSSS (*High-Rate Direct-Sequence Spread Spectrum*), ou o 802.11a, que descreve uma camada física baseada em OFDM (*Orthogonal Frequency Division Multiplexing*).

Ainda de acordo com (GAST,2002), 802.11 permite acesso à rede para dispositivos móveis e, para isso, uma série de melhorias foram implementadas no MAC. Como resultado, o MAC 802.11 é extremamente mais complexo que os MAC dos demais padrões da família IEEE 802.

Já a figura 5, (JAVVIN, 2007), demonstra maiores detalhes destas camadas, inclusive com os níveis de autenticação, que serão abordados ao decorrer deste TCC.

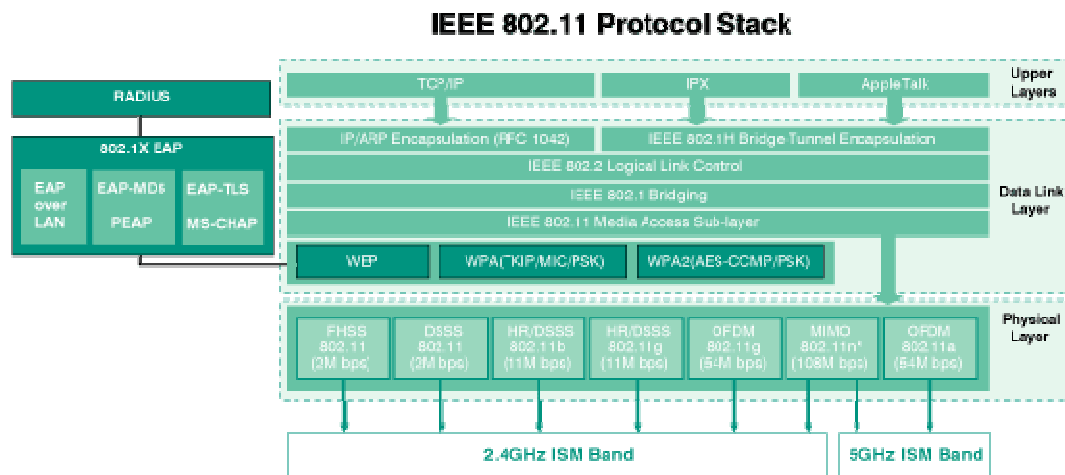


Figura 5 – Padrões 802.11, as camadas OSI e Autenticação

## 4.5 AUTENTICAÇÃO

O padrão IEEE 802.11 oferece dois métodos para garantir a segurança dos dados: criptografia e autenticação. Sendo existentes, neste último, dois métodos de autenticação: *Open System* e *Shared Key*.

**Open System** – é o sistema padrão de autenticação. Neste, qualquer estação que solicitar a associação à rede será aceita. Trata-se de um sistema nulo de autenticação.

**Shared key** – neste método, tanto a estação que solicita acesso quanto a autenticadora (seja um AP ou outra estação) necessitam que uma chave secreta seja compartilhada entre elas.

Conforme já mencionado, após a determinação do padrão 802.11i, foi adicionado o suporte a autenticação 802.1x as redes wireless, onde eram utilizados novos protocolos e métodos de autenticação. A tabela 1 ilustra o “relacionamento” entre todos estes métodos, protocolos e tipos de criptografia.

Tabela 1 – Métodos, Protocolos e Tipos de Criptografia

Support 802.1x	Protocol	Authentication	Encryption
<b>DISABLED</b>		Open	None
	WEP WPA	Shared	RC4 TKIP AES-CCMP
<b>ENABLED</b>	EAP	FAST LEAP PEAP SIM TLS	

Desta forma, vamos a algumas definições, segundo (DÍGITRO, 2007) e (WIKIPEDIA, 2007):

**WEP (Wired Equivalency Privacy)** – protocolo de autenticação que utiliza criptografia RC4. Por utilizar a mesma chave para todos que utilizem a mesma rede, caracteriza-se por um protocolo não muito seguro mas ainda em uso, principalmente em residências.

**RC4** – algoritmo de criptografia de fluxo muito utilizado em softwares e protocolos como o SSL (*Secure Socket Layers*).

**WPA (*Wi-Fi Protected Access*)** - substituto do WEP, melhorando a atribuição de chaves dinâmicas, a força da criptografia, a não repetição de chaves e o uso de funções *hash* nas mensagens assegurando a integridade dos dados.

**TKIP (*Temporal Key Integrity Protocol*)** – Algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a freqüente mudanças de chaves que garante mais segurança.

**WPA2 (*Wi-Fi Protected Access 2*)** – evolução do WPA especificado pelo padrão IEEE 802.11i. Melhora a criptografia através da utilização do AES.

**AES (*Advanced Encryption Standard*)** – técnica de criptografia de dados simétrica (256bits).

**EAP (*Extensible Authentication Protocol*)** – Protocolo de autenticação para controle de acesso a rede que suporta diversos métodos (senhas, *token*, Kerberos, certificados digitais, chave pública, etc...).

**EAP-FAST (*Flexible Authentication via Secure Tunneling*)** – Método proposto pela Cisco em substituição ao LEAP. Utiliza uma chave pré-compartilhada chamada PAC (*Protected Authentication Credential*).

**EAP-PEAP (*Protected Extensible Authentication Protocol*)** - Método de autenticação que utiliza certificado digital e outros sistemas, como a própria senha do usuário.

**EAP-LEAP (*Lightweight Extensible Authentication Protocol*)** - Método de autenticação que utiliza senhas e servidores RADIUS.

**EAP-SIM** – Mecanismo para autenticação e distribuição de chave de sessão utilizando GSM-SIM (*Global System for Mobile Communications – Subscriber Identity Module*).

**EAP-TLS (*Transport Layer Security*)** – Método de autenticação que utiliza certificado digital.

## 5. LOCALIZAÇÃO DE ESTAÇÕES SEM FIO

Existem, atualmente, dois modelos para que se possa localizar uma estação sem fio, conhecidos como *Mobile Based* e *Network based*. No primeiro modelo, o cliente obtém a sua localização a partir de informações adquiridas da própria infra-estrutura de rede (AP's cuja localização sejam conhecidas). Já no segundo modelo, a infra-estrutura efetua “consultas” nas estações para determinar sua localização.

Desta forma, (SURIS, 2007) existem três meios de se localizar uma estação móvel, de acordo com os modelos expostos, sendo eles baseados na potência do sinal, na diferença do tempo de chegada do sinal ou no ângulo em que o sinal chega à estação. Estas técnicas são conhecidas, respectivamente, como AMPOA (*Amplitude of Arrival*), TOA (*Time of Arrival*) e AOA (*Angle of Arrival*). É importante ressaltar que a eficácia destes sistemas está diretamente relacionada ao ambiente, ou seja, torna-se mais complexo de acordo com as interferências sofridas pelo sinal, as reflexões, refrações e a atenuação.

Abaixo, uma sucinta explicação a respeito de cada uma destas três técnicas:

**AMPOA** – mede-se a amplitude com que o sinal chega à estação. Neste caso, normalmente, utiliza-se ferramentas como o *NetStumbler* ou comando IWLIST (disponível em algumas distribuições do Linux) para se determinar esta amplitude.

**TOA** – mede-se o tempo entre o envio do sinal do ponto de referência até a estação que se deseja localizar, possibilitando determinar o raio equivalente à distancia entre tais pontos. Considerando que as ondas eletromagnéticas transitam a uma velocidade constante, semelhante a da luz, é imprescindível que os relógios (estação e AP) estejam perfeitamente sincronizados, caso contrário haverá erros no cálculo.

**AOA** – mede-se o ângulo com que o sinal chega à estação baseado em antenas direcionais em cada AP. Assim, de acordo com a amplitude com que cada antena recebe o sinal, é possível traçar uma linha reta até o local onde a estação se encontra.

Maiores informações podem ser obtidas em (XIANG, 2004) e (TAHERI, 2004).

Utilizando AMPOA, existem 2 técnicas para localizar estações móveis, conhecidas como Triangulação e *Fingerprinting*, que serão explicadas a seguir.

### 5.1 TRIANGULAÇÃO

Uma vez que a amplitude com que o sinal chega à estação é sabida, é possível que a distância entre o AP e tal estação seja inferida. Assim sendo, o valor obtido representa a circunferência existente entre o ponto de referência e a estação móvel que se deseja localizar.

Para viabilizar este método de localização, é necessária a existência de outros pontos de referência (preferencialmente três ou mais), permitindo que, a partir destes, sejam inferidas novas circunferências, possibilitando, assim, a determinação do ponto de intersecção das mesmas. A figura 6 exemplifica tal situação:

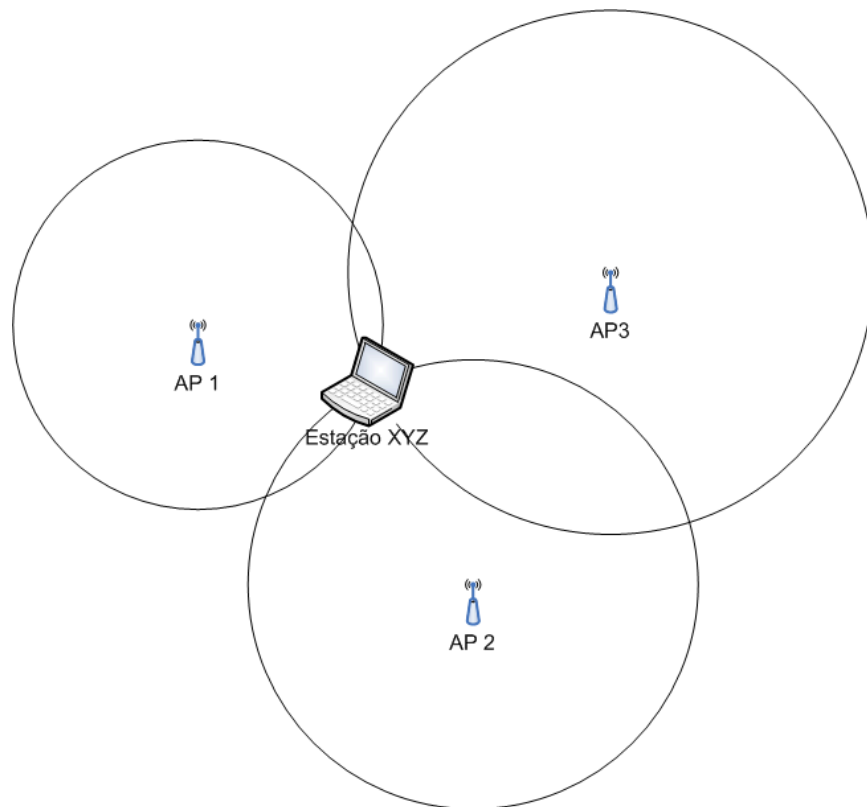


Figura 6 – Triangulação

## 5.2 FINGERPRINTING

Ainda utilizando a técnica do AMPOA, pode-se mapear todo o perímetro de cobertura do sinal, assim como um *site survey*. Neste método, a área de cobertura é dividida em espaços físicos menores (quadrantes) e é realizada uma amostragem da cobertura do sinal. Cada quadrante representa uma entrada na tabela do *fingerprinting*, assim, quando a estação informa a potencia do sinal entre o mesmo e os AP's disponíveis, o sistema efetua uma consulta em suas tabelas para determinar sua localização.

A figura 7 (BAHL, 2000) exemplifica o mapeamento através da técnica de *fingerprinting*.

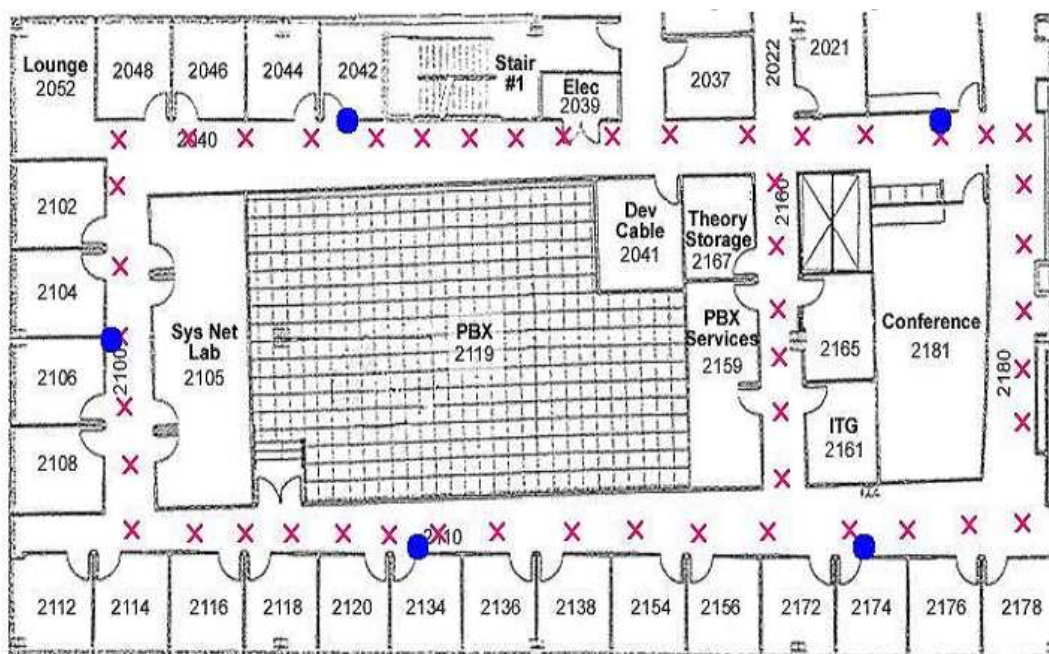


Figura 7 – *Fingerprinting*

## 5.3 SISTEMA DE LOCALIZAÇÃO DE ESTAÇÕES SEM FIO

Na ULBRA *campus* Guaíba já está em uso um sistema de localização de estações sem fio, baseado na técnica de *fingerprinting*, devidamente desenvolvido e documentado por (SURIS, 2007). Atualmente, tal sistema, contempla a área do LABIN (Laboratório de Informática), onde cada uma das

dependências foi mapeada em nove pontos (coletadas três amostras intercaladas em dez segundos e tirada a média). Abaixo, figura 8, também disponível em (SURIS, 2007), o mapeamento realizado:

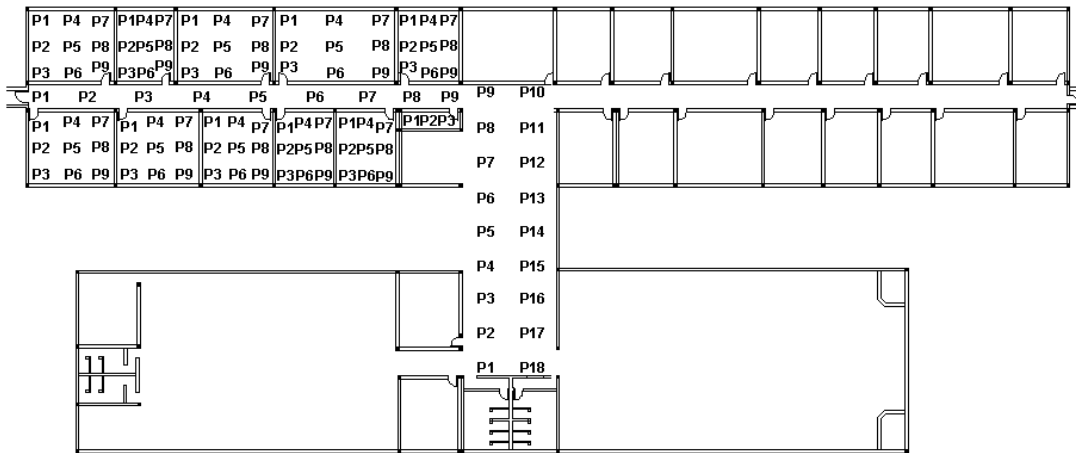


Figura 8 – Pontos mapeados no LABIN por *Fingerprinting*

Já as figuras 9 e 10, respectivamente, demonstram a localização dos *Access Points* e suas abrangências.

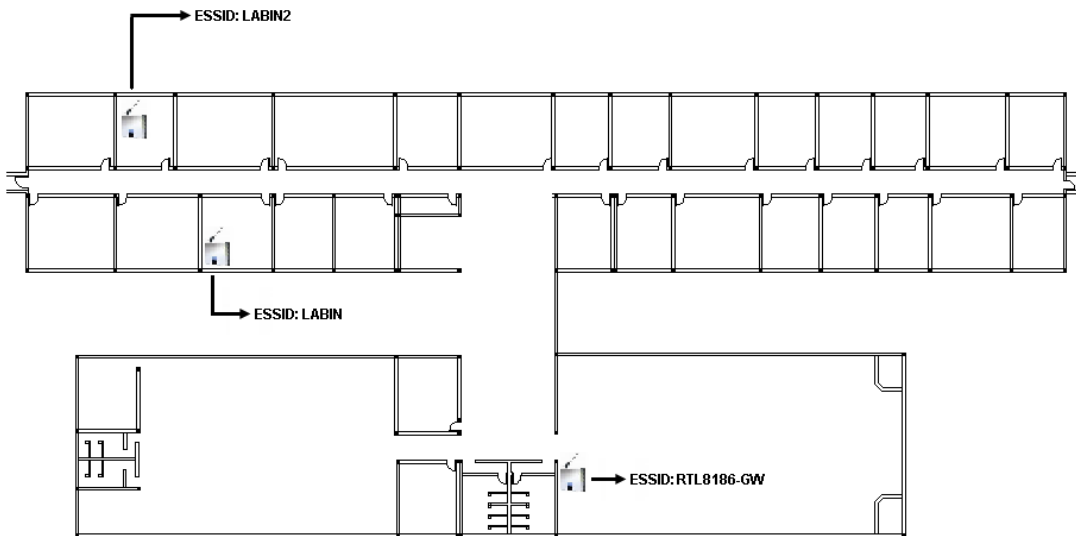


Figura 9 – Localização dos *Access Points*

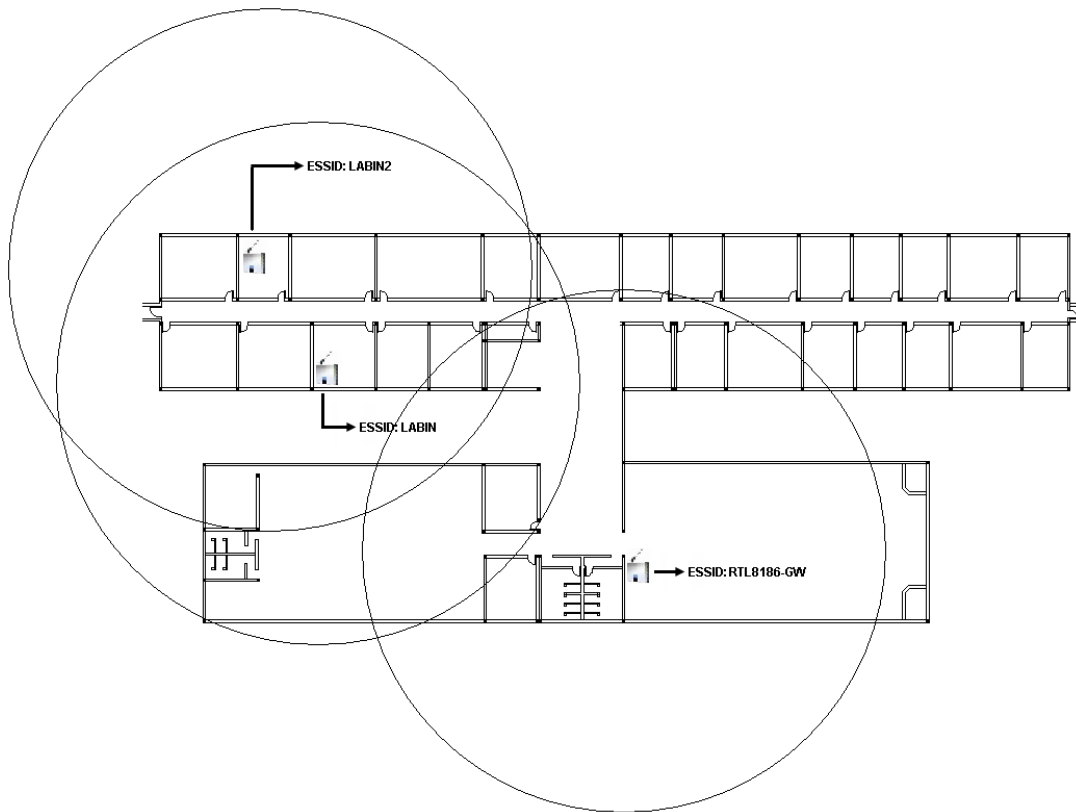


Figura 10 – Abrangência dos *Access Points*

### 5.3.1 DETALHES DO SISTEMA ATUAL

O sistema foi desenvolvido em PHP e dividido em dois módulos, cliente e servidor.

O módulo cliente, por meio de sua interface de rede, capta todos os pontos de acesso que estão ao seu alcance juntamente com suas respectivas potências (através do comando *IWLIST*, já comentado anteriormente). Uma vez capturados, tais dados são enviados ao servidor para que sejam realizados os cálculos necessários.

Por sua vez, o módulo servidor, recebe as informações enviadas pelo cliente e compara-as com as tabelas já mapeadas através do *fingerprinting*, determinado, assim, sua localização.

Maiores informações a respeito das técnicas empregadas neste sistema, bem como seu funcionamento, podem ser adquiridas em (SURIS, 2007).

## **6. AUTENTICAÇÃO DE ESTAÇÕES SEM FIO BASEADA NA LOCALIZAÇÃO**

Até a conclusão desta monografia, nenhuma ferramenta comercial que se propusesse a oferecer um método de autenticação baseada na localização de estações sem fio foi localizada.

## 7. MODELO PROPOSTO

Tendo conhecimento do sistema já existente e em utilização da ULBRA *campus* Guaíba – desenvolvido e documentado por (SURIS, 2007) – e com base no referencial teórico já apresentado, este TC foca o desenvolvimento e implantação de mecanismos de segurança (autenticação baseada na localização) no sistema de localização de estações sem fio padrão IEEE 802.11.

Da forma que foi planejado e desenvolvido, o módulo cliente do sistema apenas informa o servidor os pontos de acessos localizados pela estação, sua atenuação e SSID (*Service Set Identifier* – identificação da rede sem fio). No entanto, todo o sistema se baseia apenas nas informações passadas pelas estações clientes, o que caracteriza uma falha de segurança.

Para que seja possível concretizar os objetivos, o módulo cliente sofrerá alterações que ampliarão suas funcionalidades e modificarão sua forma de operar. Dentre estas alterações, pode-se citar:

- Identificar o tipo de autenticação utilizado no SSID localizado;
- Forçar a estação a se associar a todos os SSIDs identificados;
- Enviar ao servidor as informações coletadas enquanto ainda se encontra associado ao SSID corrente;
- Aguardar a validação do servidor para se desassociar do SSID corrente e se associar ao próximo SSID localizado.

Para conseguir se associar ao AP correspondente, o módulo cliente deverá utilizar o tipo de autenticação configurada (característica determinada nas configurações de cada *access point*, seja ela “*Open System*”, “*Shared Key*” ou com suporte a “802.1x”), em cada um destes aparelhos e efetuar o processo de associação. Ou seja, no momento em que a estação identifica o SSID a se associar, deverá identificar também qual o tipo de autenticação deverá utilizar para dar prosseguimento ao processo.

Esta modificação no fluxo se deve, também, em função das alterações que serão realizadas no módulo servidor da aplicação que, atualmente, apenas coleta estes dados e efetua os cálculos para que seja determinada a

localização da estação, mas que, a partir de agora, deverá validar a informação passada pelo cliente no próprio AP associado.

Para que o servidor consiga a informação referente à potência do sinal, a cliente precisa estar associado ao SSID correspondente ao AP que está sendo acessado (visto que no gerenciador do AP é informada quais os clientes estão associados a ele no momento e qual o endereço MAC do cliente). Uma vez obtida tal informação, ela é armazenada e informa-se ao cliente que o mesmo já pode se desassociar do SSID atual e se associar ao próximo localizado.

Realizado este processo em todos os AP que cobrem a sua área de atuação e de posse destas informações (obtidas a partir dos AP's), as mesmas serão confrontadas com as passadas pelo cliente. Caso haja coerência, a estação receberá permissão para ingressar na rede (vale lembrar que, em função de obstáculos, como pessoas caminhando no ambiente, os valores precisam ser apenas aproximados e não exatamente idênticos).

Desta forma, a solução implementará mais uma camada de segurança, não substituindo nenhuma das já existentes.

Resumidamente, o sistema será responsável por garantir que as informações referentes à atenuação e SSID passadas para o mesmo são verídicas e que sua posição no espaço coberto pela rede *wireless* é, de fato, a que a estação está informando ao sistema.

É válido mencionar que, almeja-se futuramente, que toda estação sem fio que desejar utilizar a rede *wireless* da ULBRA *campus* Guaíba, tenha, obrigatoriamente, o módulo cliente deste sistema e sua estação, caso contrário, o serviço não será disponibilizado.

## 8. CENÁRIO

O cenário para implementação destas alterações no sistema será o mesmo em que o atual já opera, ou seja, no LABIN – figura 11.

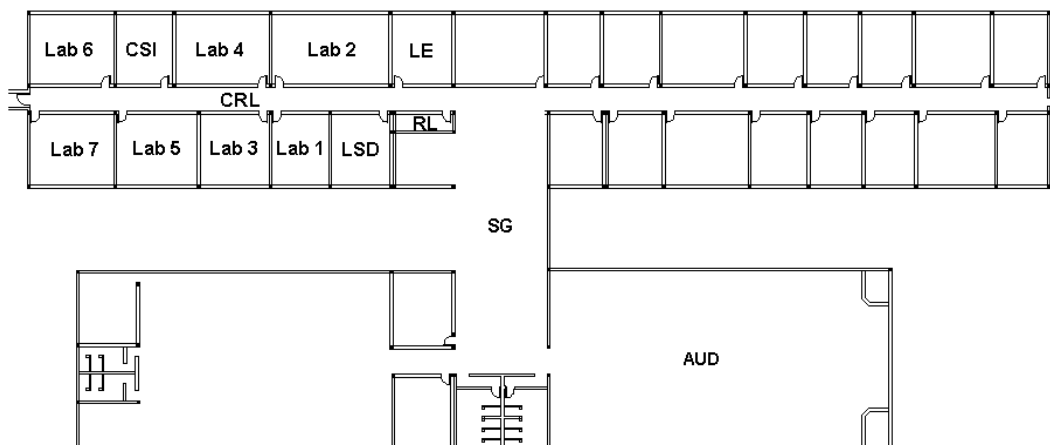


Figura 11 – Planta baixa LABIN

Em seu perímetro, três *access points* estão fisicamente instalados, sendo seus respectivos SSIDs: LABIN (localizado na sala de Pesquisa e Servidores), LABIN2 (localizado na sala da Coordenação do Curso de Sistemas de Informação) e RTL8186-GW (localizado na entrada do auditório). É importante ressaltar que, algumas estações sem fio, conseguem se associar à SSID professores, cuja localização é no andar térreo, próximo a sala dos professores do curso de Administração.

Existem, no mínimo, duas características interessantes neste ambiente (para fins acadêmicos). A primeira é que cada *access point* possui um SSID diferente, ou seja, uma vez sabendo qual SSID a estação está utilizando, fica óbvio a qual AP a mesma está associada. Situação que normalmente não ocorre em outros ambientes, como o corporativo, por exemplo. A segunda é o fato de não haver nenhum protocolo de autenticação ativo no momento, ou seja, a cobertura é em *broadcast* sem que sejam necessárias senhas ou criptografias específicas para sua utilização, mais uma característica pouco utilizada em empresas.

Desta forma, na fase dos testes, será imprescindível que sejam alteradas algumas características do ambiente para que o sistema seja o mais

fiel à realidade possível, como relacionar um SSID a mais de um AP e exigir a autenticação de acordo com a maior parte dos protocolos possíveis.

## 9. ROTEIRO DE TESTES

Todas as etapas apresentadas na seção “MODELO PROPOSTO” serão colocadas em prova, da seguinte forma:

- Adicionar, ao sistema desenvolvido por (SURIS, 2007), uma implementação de protocolo;
- Forçar as estações com o módulo cliente a se associarem com *access points* diferentes;
- Coletar informações de amplitude do sinal dos *access points*;
- Verificar a veracidade das informações passadas pelo cliente;
- Configurar um *firewall* para restringir o acesso à rede antes da validação das informações;
- Fazer com que o sistema libere este mesmo firewall no caso das informações validadas.

Além disso, deverá ser simulado o comportamento de estações maliciosas, como:

- Envio de informações incorretas ao servidor;
- Tentativa de entrada na rede sem o módulo cliente.

## 10. CONCLUSÕES

Através deste primeiro contato mais aprofundado com a tecnologia *wireless* pode-se concluir que é um segmento em constante evolução e que certamente trará muitos avanços. Sem dúvida, este trabalho está sendo conduzido de forma a ser tanto instrutivo quanto funcional e certamente outras melhorias serão identificadas e implementadas no sistema já existente.

Pode-se observar, ainda, que o ambiente é extremamente volátil, principalmente em sua topologia física, visto que a atenuação do sinal em uma sala cheia de pessoas é diferente de uma sala vazia, por exemplo, podendo comprometer a precisão.

A partir da proposta apresentada, elimina-se o fato do sistema confiar apenas no cliente, bem como a utilização da estrutura *wireless* da ULBRA *campus* Guaíba por estações que não sejam homologadas pela administração do LABIN. Além disso, pode-se implementar uma limitação por perímetro, onde apenas estações cujas potências representam estar dentro das limitações de determinadas salas, por exemplo, poderão acessar a rede *wireless*.

De qualquer forma, de acordo com as referências citadas e com o sistema atualmente em funcionamento, é plenamente possível a concretização das ambições deste TCC.

Para TCC II, ficou o desenvolvimento propriamente dito, os testes em laboratório, informe dos resultados e documentação.

## 11. REFERÊNCIAS BIBLIOGRÁFICAS

3COM Corporation. **Technical Paper: IEEE 802.11b Wireless LANs**. USA: 3Com Corporation, 2000.

3COM Corporation. **White Paper: Deploying 802.11 Wireless LAN**. USA: 3Com Corporation, 2003.

BAHL, Paramvir; PADMANABHAN, Venkata .N.; BALACHANDRAN, Anand. **Enhancements to the RADAR User Location and Tracking System**. USA: Microsoft Research Technical Report, 2000.

DÍGITRO Tecnologia. **Glossário Tecnológico**. Coordenação Eng. Juliano Anderson Pacheco, desenvolvida por Adm. Claudio Brancher Kerber, apresenta termos tecnológicos na área de telecomunicações - [http://www.digitro.com/glossario\\_digitro.php](http://www.digitro.com/glossario_digitro.php). Acessado em novembro 2007.

DUBENDORF, Vern A. **Wireless Data Technologies – Reference Handbook**. England: John Willey & Sons Ltd, 2003.

GAST, Matthew S. **802.11 Wireless Networks: The Definitive Guide**. UK: O'Reilly & Associates, 2002.

JAVVIN. **WLAN Wireless LAN by IEEE 802\_11, 802\_11a, 802\_11b(Wi-Fi), 802\_11g, 802\_11n** - <http://www.javvin.com/protocolWLAN.html>. Acessado em setembro de 2007.

PAHLAVAN, Kaveh; LI, Xinrong; YLIANTTILA, Mika; LATVA-AHO, Matti. **“Wireless Data Communication Systems”, Wireless Communication Technologies – New Multimedia Systems**, edited by MORINAGA, Norihiko; KOHNO, Ryuji; SAMPEI, Seiichi: KLUWER ACADEMIC PUBLISHERS, 2002. Page(s): 201-214

PICCININ. **Camadas OSI** - <http://www-usr.inf.ufsm.br/~piccinin/>. Acessado em setembro de 2007.

SURIS, Henrique A. **Localização de Estações sem Fio IEEE 802.11 – Trabalho de Conclusão de Curso** (Graduação em Sistemas de Informação), Guaíba: Universidade Luterana do Brasil, 2007.

TAHERI, Ali; SINGH, Arvider; AGU, Emmanuel. **Location Fingerprinting on Infrastructure 802.11 Wireless Local Area Networks (WLANs) using Locus\***. USA: Worcester Polytechnic Institute, 2004.

WIKIPEDIA. **Wikipedia, the free encyclopedia** - <http://en.wikipedia.org/>. Acessado em setembro de 2007.

XIANG, Z; SONG, S. **A Wireless LAN-based Indoor Positioning Technology**. USA: IBM, 204. Page(s): 617-626