FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA”
CENTRO UNIVERSITÁRIO “EURÍPIDES DE MARÍLIA” - UNIVEM
PROGRAMA DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

FERNANDO HENRIQUE FERREIRA

PROJETO DE INFRA-ESTRUTURA DE REDE VIA WIRELESS

MARÍLIA
2006

FERNANDO HENRIQUE FERREIRA

PROJETO DE INFRA-ESTRUTURA DE REDE VIA WIRELESS

Monografia apresentada como pré-requisito de conclusão do curso de Bacharelado em Ciência da Computação do Centro Universitário "Eurípides de Marilia" - UNIVEM, tendo como orientador o Prof. João de Lucca Filho.

MARÍLIA
2006

FERNANDO HENRIQUE FERREIRA

PROJETO DE INFRA-ESTRUTURA DE REDE VIA WIRELESS

Banca examinadora da monografia apresentada à coordenação do curso de Ciência da Computação da UNIVEM/F.E.E.S.R., para obtenção do título de bacharel em Ciência da Computação.

Resultado: _____

_____

ORIENTADOR: Prof. João de Lucca Filho

_____

1° EXAMINADOR: Prof.

_____

2º EXAMINADOR: Prof.

Marília, __ de _____ de 2006.

À Deus pela iluminação e proteção em toda minha vida, e de meus queridos amados;

À minha mãe e meu pai que me educaram e me deram a oportunidade de estar concluindo este trabalho para minha formação acadêmica;

Às minhas amadas Camila e Kelly por todo o carinho e paciência;

Aos amigos da faculdade, em especial ao Rodrigo, Gustavo Rondina e Marcelo Rossi pela força dada durante todo nosso período de graduação.

AGRADECIMENTOS

Agradeço à meu professor e orientador Profº. Drº. João de Lucca Filho, pela orientação, incentivo e apoio para que o projeto fosse concluído com relevância.

A todos os professores que ajudaram com idéias, estímulo e companheirismo ao longo desta jornada.

Não poderia deixar de lado, aos amigos Kelson Ferreira, Danilo Rossato, Guilherme Scombatti, pelo incentivo, estímulo e força para que terminasse o projeto.

A todos os colegas da Fundação de Ensino “Eurípides Soares da Rocha” – UNIVEM – os quais convivi durante os últimos 5 anos.

"Tantum homo habet de scientia quantum operatur" - "O conhecimento que o homem possui é só aquele que aplica"

São Francisco de Assis

FERREIRA, Fernando Henrique. **Projeto de Infra-Estrutura de Rede via Wireless**. 2006. 66 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação). Centro Universitário Eurípides de Marília, Marília, 2006.

RESUMO

Esta monografia tem como objetivo apresentar um projeto para a instalação de rede de computadores para o Instituto Superior de Tecnologia (IST) do Centro Universitário Eurípides de Marília (UNIVEM). Foram abordadas muitas questões, como o levantamento das necessidades dos usuários, as topologias física e lógica, o projeto de rede sem fio lan, o detalhamento da infra-estrutura, a segmentação e a segurança da rede.

Palavras-chave: Rede Local, LAN, Projeto de Rede, Topologia, Segmentação, Wireless.

FERREIRA, Fernando Henrique. **Projeto de Infra-Estrutura de Rede via Wireless**. 2006. 66 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação). Centro Universitário Eurípides de Marília, Marília, 2006.

ABSTRACT

This monography has as objective the presentation of the project for the installation of computer network for the Superior Institute of Technology (IST) of the University Center Eurípides de Marília (UNIVEM). Many questions have been approached, as the survey of the necessities of the users, the physical and logical topologies, the project of wireless lan, the detailing of the infrastructure, the segmentation and the security of the net.

Key words: LAN, Network Project, Topology, Segmentation, Wireless.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AP: Access Point - Ponto de Acesso

BNC: Bayonet Neill-Concelman - Nome do Criador do Cabo Coaxial

BSA: Basic Service Area - Área de Serviço Básica

BSS: Basic Service Set - Grupo de Serviço Básico

BSS-ID: Basic Service Set Identification - Identificação do Grupo de Serviço

CIEM: Centro Incubador de Empresas de Marília

CRC: Cyclic Redundancy Check – Verificação de Redundância Cíclica

CSMA/CD: Carrier Sense Multiple Access / Collision Detect

DHCP: Dynamic Host Configuration Protocol – Protocolo de Configuração de Host Dinâmico

DSSS: Direct Sequence Spread Spectrum

ESA: Extend Service Area - Área Estendida de Serviço

ESS: Extend Service Set - Grupo estendido de Serviço

ESS-ID: Extend Service Set Identification - Identificação do Grupo estendido de serviço

GBPS: Gigabits por segundo

HAP: Hardware Access Point - Ponto de Acesso de Hardware Host

IEEE: Institute of Electrical and Electronics Engineers - Instituto de Engenheiros da Elétrica e Eletrônica

ISO: International Organization for Standardization

IST: Instituto Superior de Tecnologia

LAN: Local Area Network

MAC: Media Access Control

Mbps: Megabits por segundo

OSI: Open System Interconnection

P2P: Point-to-Point

SSID: Service Set Identifier – Identificador de Grupo de Serviço

TCP/IP: Transfer Control Protocol / Internet Protocol - Protocolo de Controle de transferência / Protocolo de Internet

TG: Task Group – Grupo de Tarefa

TIA: Telecommunications Industry Association

USB: Universal Serial Bus

UTP: Unshield Twisted Pair - Par Trançado Não Blindado

UTP: Unshielded Twisted Pair

VLAN: Virtual Local Area Network

WAN: Wide Area Network

WEP: Wired Equivalent Privacy - Privacidade Equivalente à Cabeada

WLAN: Wireless LAN – LAN Sem Fio

SUMÁRIO

1. REDES SEM FIO

Uma WLAN ou Wireless LAN é uma forma de transmissão de dados que pode ser utilizada como alternativa para substituir ou complementar as redes cabeadas, considerando que a mesma não utiliza fios. Os dados são transmitidos através de ondas eletromagnéticas. [ZANNETI 2006]

A WLAN é uma Rede Local Sem Fio que atende uma área restrita, com o objetivo de manter conectados todos os equipamentos wireless que estão em sua área de abrangência.

Existem várias versões do padrão inicialmente denominado IEEE 802.11 (O IEEE será descrito no capítulo 3), como o IEEE 802.11a, que possibilita uma transmissão de até 54Mbps, operando na freqüência de 5Ghz, também se tem o padrão IEEE 802.11b, padrão muito utilizado atualmente e que permite taxa de transmissão de 11Mbps, utilizando a freqüência de 2,4Ghz e ainda o padrão IEEE 802.11g, que está se destacando por reunir o que há de melhor nos dois outros padrões, ou seja, a taxa de transmissão do IEEE 802.11a com a freqüência do IEEE 802.11b, resultando em um padrão com a taxa de transmissão de 54Mbps e na freqüência de 2.4Ghz, possibilitando assim, a compatibilidade com o padrão 802.11b.

1.1 Evolução das redes sem fio

A primeira rede a utilizar a comunicação sem fio foi desenvolvida no Havaí, no início da década de 1970. O objetivo era interligar os *campi* que se situavam em 4 ilhas com o computador central, que ficava na ilha de Oahu. Apesar daquele projeto não ter sido utilizado em massa frente a fatores como: baixa taxa de transmissão e do custo elevado para a época, ele despertou o interesse permitindo assim, aperfeiçoar tal tecnologia para então torná-la viável. As primeiras redes sem fio utilizavam transmissão *spread spectrum* (uma técnica de

codificação para a transmissão digital de sinais) ou infravermelha difusa. No entanto, tinha uma baixa interoperabilidade devido ao fato dos fabricantes utilizarem padrões proprietários. Uma vez que a falta de padronização atrasava o desenvolvimento e, sobretudo, a popularização da técnica, em maio de 1991 foi submetido ao IEEE a criação de um grupo de pesquisa para criar um padrão único para as redes sem fio. Esse padrão, denominado de Padrão 802.11, à medida que foi elaborado, foi sendo adotado pelos fabricantes de equipamentos para redes sem fio, que então passaram a elaborar seus produtos baseando-se nas normas do 802.11, uma vez que a padronização oferece interoperabilidade, confiabilidade e diminuição nos custos provendo assim uma boa aceitação do mercado. [GAST 2002]

Foi então lançado, oficialmente, em 1997, o primeiro padrão para redes locais sem fio, o IEEE 802.11. O padrão oferecia taxa de transmissão de dados de até 2 Mbps, utilizando a técnica de transmissão de FHSS (*Frequency-Hopping Spread-Spectrum*) ou DSSS (*Direct Sequence Spread Spectrum*). Apesar da significante elevação da taxa de transmissão de poucos Kbps para 2 Mbps, esse valor já não atendia satisfatoriamente a necessidade das empresas. Era então preciso melhorar o padrão. Foi então que surgiu em 1999, o 802.11b, que possuía a mesma tecnologia e arquitetura, mas com taxa de transmissão aumentada para até 11 Mbps, o que permitia alcançar valores aproximados aos da ethernet naquele momento. Esse padrão impulsionou de vez a indústria a investir em tecnologia e produtos para as redes sem fio. [OFDM 2006]

Ao mesmo tempo em que estava sendo “criado” o padrão IEEE 802.11b, também se trabalhava concomitantemente o 802.11a, que permitia uma taxa de dados de até 54 Mbps, no entanto, utilizando a freqüência de 5 Ghz. Esse padrão, que oferecia uma boa taxa de dados, não conquistou o seu espaço no mercado devido à sua incompatibilidade com o padrão 802.11b, oferecendo alcance reduzido e também por ter sido lançado no mercado 6 meses após o lançamento de seu concorrente, que então já estava se consagrando nas grandes empresas.

Apesar de já existir no mercado um padrão com uma boa taxa de transmissão, havia a

necessidade de se criar uma nova estrutura capaz de aumentar a taxa de dados do padrão 802.11b, mantendo a compatibilidade com o mesmo. Foi então que o Grupo de Tarefa G do IEEE criou o padrão IEEE 802.11g, tendo sido aprovado em junho de 2003, possibilitando uma taxa de dados de até 54 Mbps na freqüência de 2.4 Ghz, a mesma utilizada no padrão 802.11b, mantendo assim, a compatibilidade com o mesmo.

1.2 Vantagens e Desvantagens da Rede Sem Fio

Dentre as vantagens de rede sem fio destacam-se [MATHIAS 2006]:

- *Flexibilidade*: A estação pode se mover sem problemas, desde que fique dentro da área de cobertura.
- *Robustez*: uma rede sem fio pode sobreviver intacta em caso de um desastre (por exemplo, um terremoto); a comunicação continuaria garantida.
- *Velocidade e Facilidade:* A instalação de uma rede sem fio é muito mais rápida, pois não precisa de qualquer alteração para passar cabos.
- *Redução do custo agregado*: facilidade de expansão, menos necessidade de manutenção, robustez e outros fatores que ajudam a amenizar o tempo necessário para recuperar os recursos inicialmente empregados.
- *Diversas topologias*: podem ser configuradas em uma variedade de topologias para atender a aplicações específicas. As configurações são facilmente alteradas.

Dentre as desvantagens comparando redes sem fio com as cabeadas destacam-se [MATHIAS 2006]:

- *QoS*: a qualidade do serviço provido ainda é menor que a das redes cabeadas
- *Custo:* os preços dos equipamentos de Redes sem Fio são mais altos que os equivalentes em redes cabeadas.

- *Segurança:* é um dos motivos na demora da popularização das redes em fio.
- *Baixa transferência de dados:* embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é baixa se comparada com as redes cabeadas.

1.3 Interferências em Redes sem fio

Outra importante consideração a ser levada em conta quando se implementa uma rede sem fio é a questão da interferência que esse tipo de rede pode sofrer.

Segundo Fortes (2005), um dos equipamentos mais perigosos (por ser muito utilizado) é o telefone sem fio de 2,4Ghz, porque ele utiliza justamente a mesma faixa de transmissão dos equipamentos 802.11b e 802.11g. Em ambientes com esse tipo de telefone a qualidade do sinal pode ficar comprometida.

Outro equipamento que gera uma interferência preocupante se for utilizado no ambiente é o Bluetooth, um sistema de transmissão de dados de curta distância (aproximadamente 10 metros) e com velocidade de 1Mbps. Esse equipamento gera interferência em uma rede WLAN, visto que opera na mesma freqüência de 2.4Ghz. E também, deve ser considerado o forno de microondas pelo mesmo motivo.

1.4 APLICAÇÃO PARA A REDE SEM FIO

A mobilidade é um dos fortes aspectos das redes sem fio, pois permite que as estações de trabalho em atividade nas redes sejam utilizadas em várias situações:

- Nas universidades: estudantes de posse de seus equipamentos móveis conseguem fazer acesso a informações úteis em relação ao estudo, até mesmo durante a aula;

- Nos hospitais: médicos e enfermeiras podem repassar informações sobre seus pacientes em tempo real, bem como saber de várias características de seus pacientes, que estão armazenadas no banco de dados do hospital utilizando seus handhelds (Computadores de Mão);

- Em construções antigas e Prédios Históricos: pode-se efetuar a comunicação sem que necessite fazer alterações na estrutura predial;

- Nos restaurantes: pode-se fazer o atendimento aos clientes com mais agilidade, qualidade e eficiência, considerando que os garçons não precisam ir até a copa para registrar os pedidos ou o concluir operações de pagamento;

- Durante conferências: permite aos executivos a comunicação imediata;

- Consultores e auditores: permite aumentar a produtividade considerando o fato de estarem constantemente conectados em rede.

Enfim, uma rede sem fio pode ser utilizada em qualquer lugar onde é necessário fazer o acesso a informação aliado a mobilidade.

Este capítulo abordou as vantagens e desvantagens em relação as redes sem fio , bem como sua utilização. No próximo capítulo, será abordado sobre a arquitetura usada em redes sem fio.

2. ARQUITETURA DA REDE 802.11

O padrão IEEE 802.11 definiu uma arquitetura para redes sem fio. Essa arquitetura descreve elementos como: Grupos Tarefas, BSA, BSS, DS, AP, ESA, ESS, redes com e sem infra-estrutura.

De acordo com o IEEE (2006), o *Institute of Electrical and Electronics Engineers* (Instituto dos Engenheiros Elétricos e Eletrônicos), é uma associação sem fins lucrativos possuindo mais de 380.000 membros em aproximadamente 150 países.

Esse instituto é a autoridade principal em várias áreas, que variam desde a tecnologia biomédica até setores como eletrônica aeroespacial e comercial, entre outros. Um exemplo do que é o IEEE, é que 30% da literatura mundial sobre engenharia elétrica e computadores foram feitos por este instituto, sem falar nas 300 conferenciais anuais e nos 900 padrões ativos e 700 em desenvolvimento [IEEE 2006].

Conforme o IEEE (2006), o instituto tem como visão, melhorar a prosperidade global, promovendo a inovação tecnológica, sem falar na sua missão, que tem como objetivo promover o processo de criação, desenvolvimento e integração das tecnologias elétricas e de informação para o benefício da humanidade.

O IEEE forma então, grupos de tarefas para desenvolver e aperfeiçoar os mais diversos padrões. Esses grupos de tarefas [ZYREN 2003] são designados com letras do alfabeto, à medida que forem sendo criados (TGa, TGb, TGc, ...), onde TG significa *Task Group* (Grupo de Tarefa).

Para se ter uma idéia de quanto o padrão IEEE 802.11 está sendo aperfeiçoado, foram formados nada menos do que 11 grupos de tarefas, como é apresentado no Quadro 2.0. Padrões IEEE 802.11.

Tabela 2.0: Padrões IEEE 802.11

Grupo	Atividade	Status
802.11 Original	Desenvolveu o MAC e PHY para WLAN. Suportava taxas de dados de 1 e 2 Mbps na banda de 2.4 GHz	Concluído em 1997 (IEEE 802.11)
TGa	Extensões do PHY para banda de 5 GHz. Suporta mais canais (até 12 não-sobrepostos) e maior taxa de dados (até 54 Mbps)	Concluído em 1999 (IEEE 802.11a)
TGb	Extensões do PHY para banda de 2.4 GHz. Aumento da taxa de dados para 11 Mbps e compatibilidade com o 802.11	Concluído em 1999 (IEEE 802.11b)
TGc	Suplemento ao 802.1d (spanning tree) para suportar frames 802.11	Concluído em 2000
TGd	*Regulatory Domain Update* (Atualização de Domínio Regulatório) – Adiciona a capacidade aos rádios 802.11 de dinamicamente se adaptar a diferentes domínios regulatórios	Concluído em 2000
TGe	Melhora do MAC para QoS (Qualidade de Serviço) Em andamento	estimativa para o 2ºsemestre de 2003
TGf	Práticas recomendadas para protocolos Inter Access Point	estimativa para o 2ºsemestre de 2003
TGg	Extensão do PHY para banda de 2.4 GHz. Aumenta a taxa de dados para 54 Mbps e preserva a compatibilidade com o 802.11b	Concluído em Junho de 2003
TGh	Extensão do PHY para incluir Dynamic Frequency Selection e Transmit Power Control para obedecer a regulamentação Européia para banda de 5 GHz	Em andamento, estimativa para o 2º semestre de 2004
TGi	Acrescentar medidas de segurança (encriptação, autenticação e gerenciamento de chaves)	Em andamento, estimativa para o 2º semestre de 2004
TGj	Extensão do PHY para prover a canalização para incluir alocações japonesas de 4.9 a 5.1 GHz	Em andamento, estimativa para o 2º semestre de 2004
TGk	Gerenciamento de recursos de rádio	Em andamento, estimativa para o 1º semestre de 2005

2.1 BSA (*Basic Service Area*)

Uma rede sem fio IEEE 802.11 tem sua área coberta dividida em células. As células, chamadas de BSA ou Área de Serviço Básica, são áreas que têm tamanho variável dependendo de fatores como a potência dos transmissores e receptores, sem falar nas características do ambiente, como por exemplo, a disposição física dos móveis.

2.2 BSS (*Basic Service Set*)

O BSS ou Grupo de Serviço Básico é um grupo de estações que se comunicam via rádio difusão ou infravermelho em uma célula.

2.3 DS (*Distribution System*)

Apesar de ser possível a existência de uma rede sem fio com apenas 1 célula (conhecida como Ad- Hoc), normalmente as redes sem fio são formadas por várias células. Nesse caso, múltiplas BSAs são interligadas através de um DS ou Sistema de Distribuição. Tal sistema pode ser uma rede que possui um meio de transmissão sem fio, ou mesmo outro meio, como UTP/STP (*Unshield Twisted Pair / Shield Twisted Pair* – Par Trançado Não Blindado e Par Trançado Blindado), BNC – *Bayonet Neill-Concelman*, mais conhecido como cabo Coaxial e Fibra Ótica, utilizando um Ponto de Acesso para fazer a interligação entre o Sistema de Distribuição e o BSA. Resumindo, o Sistema de Distribuição é o componente lógico utilizado para enviar os quadros ao seu destino.

2.4 AP (*Access Point*)

O AP (Ponto de Acesso) é um equipamento especial que captura as transmissões realizadas pelas estações de sua BSA e retransmite ao destino, localizado em outra BSA, utilizando o Sistema de Distribuição. Um Ponto de Acesso é comparado a um concentrador das redes cabeadas e tem várias funções. Tem a capacidade de trabalhar como roteador ou concentrador, distribuir endereços lógicos (DHCP).

2.4.1 Autenticação, Associação e Re-Associação

Permite que as estações continuem conectadas à infra-estrutura, mesmo quando se movimentam entre BSAs. Para se manterem conectadas, tais estações utilizam procedimentos de varredura para determinar qual é o melhor Ponto de Acesso, considerando potência do sinal, qualidade de recepção e dos quadros enviados, ou seja, uma estação só pode ser associada a um único Ponto de Acesso em um determinado tempo. Um exemplo prático [MENEZES, 2002] nesse caso é quando uma estação verifica que o link ao qual está associado não está bom. A estação decide interligar-se a outro Ponto de Acesso (efeito conhecido como *Roaming*), a mesma envia um pedido de re-associação a um novo Ponto de Acesso. Se a resposta for positiva, a estação migra para o novo Ponto de Acesso.

2.4.2 Gerenciamento de Energia

Como um dos principais problemas dos sistemas sem fio é tem-se a energia, as estações devem operar economizando energia. Uma vez que existem estações que estão no modo *Stand-By* (não recebem dados no momento, pois estão economizando energia), assim que o Ponto de Acesso verifica que uma informação tem como destino uma estação em modo *Stand-By*, o Ponto de Acesso armazena temporariamente tais quadros de informações para mais tarde enviá-las ao seu destino.

2.4.3 Sincronização

As estações associadas a um Ponto de Acesso devem estar sincronizadas por um relógio comum. Tal associação é implementada enviando-se periodicamente quadros (*beacons*), que carregam o valor do relógio do AP. A sincronização é necessária para casos como a questão do gerenciamento de potência.

Para finalizar, vale apresentar que um Ponto de Acesso pode ser um hardware (HAP – *Hardware Access Point*) ou *software* rodando em computadores equipados com placa de interface de rede sem fio.

2.5 ESA (*Extend Service Area*)

Como somente com um BSA não é possível cobrir uma grande área foi criado o ESA (Área de Serviço Estendida), que são diversos BSAs interligados pelo Sistema de Distribuição, via Ponto de Acesso.

2.6 ESS (Extend Service Set)

O ESS (Grupo Estendido de Serviço) é definido pela união de vários BSSs, conectados pelo Sistema de Distribuição.

A identificação da rede é feita da seguinte forma: como cada ESS recebe uma identificação (ESS-ID), e cada BSS dentro dessa ESS também recebe uma identificação(BSS-ID), o Network-ID de uma rede sem fio é obtido pelo (ESS-ID e o BSS-ID).

Este capítulo abordou a arquitetura usada em redes sem fio e o funcionamento dos Access Point. No próximo capítulo, será abordado serão abordados os componentes necessários para a produção de redes sem fio.

3. COMPONENTES PARA REDES WLAN

Os componentes utilizados em uma rede WLAN são basicamente os mesmos que os utilizados em uma rede Ethernet cabeada, com a diferença física de não terem cabos e serem específicas para as redes sem fio. São eles: NIC, antenas com a intenção de captar e difundir os sinais de rádio, Ponto de Acesso e Roteadores.

Os NIC (Cartão de Interface de Rede) são conectados às estações para receberem o sinal de rádio-freqüência. Podem ser encontrados em 3 padrões. **Padrão PCMCIA**: Utilizado em Notebooks. Exemplo de NIC é exibido na figura 3.0.

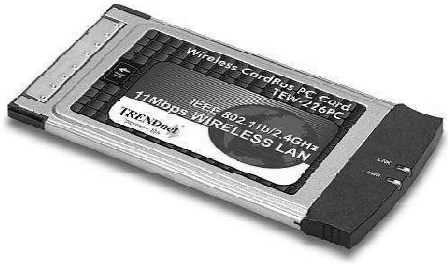

Figura 3.0: Exemplo de NIC no padrão PCMCIA.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

O NIC no padrão PCMCIA também podem ser utilizado em computadores de mesa utilizando um adaptador PCI, como é mostrado na figura 3.1.

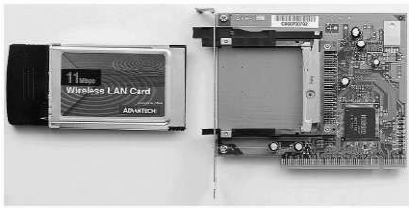

Figura 3.1: Exemplo de NIC com adaptador PCI.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

Padrão PCI: É utilizado somente em computadores de mesa, sendo uma placa PCI. Um exemplo pode ser visto da figura 3.2.

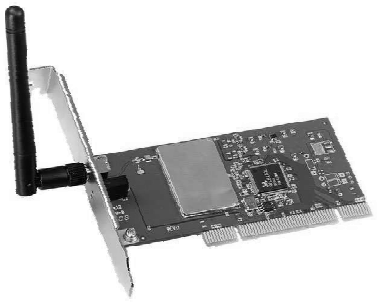

Figura 3.2: Exemplo de NIC Wireless no Padrão PCI.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

Padrão USB: Consiste de um equipamento a ser ligado em uma porta USB. Ele pode, por exemplo, ser pendurado na parede, aumentando assim o seu alcance, uma vez que ele geralmente estará livre (sem nenhum equipamento ou móvel para interferir). Um exemplo pode ser visto na figura 3.3.

Figura 3.3: Exemplos de NIC Wireless USB.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

3.1 Antenas

Para um bom funcionamento de um projeto de rede sem fio deve-se escolher corretamente o modelo de antena, considerando alguns aspectos considerados críticos.

- **Distância** - A antena a ser escolhida deve cobrir uma distância maior que a

aplicação necessária. Se a antena estiver operando em sua capacidade máxima, provavelmente os sinais chegarão mais fracos que o exigido pela aplicação.

- **Largura da onda** - Expressa em graus, a largura de onda denota o alcance de um sinal. Geralmente, quanto mais larga for a onda, mais curta será a área de cobertura. Por outro lado, as ondas mais largas compensam os fatores ambientais, como o vento, que afetam adversamente a performance da antena.

- **Ganho** - Expresso em dBi é o aumento da potência do sinal depois de processado por um dispositivo eletrônico. Usualmente, ganhos maiores revertem em distâncias maiores, contudo maiores distâncias exigem largura de onda menor e margem de erro muito maior. Para evitar esses problemas, alguns fatores como vento e prédios existentes no trajeto do sinal devem ser considerados no projeto da rede sem fio.

3.1.1 Tipos de Antenas

Fundamentalmente existem dois tipos de antenas para aplicações sem fio: omnidirecional e direcional.

Omnidirecional: As antenas omnidirecionais cobrem 360º no plano horizontal. Elas trabalham excepcionalmente bem em áreas amplas ou em aplicações multiponto. Usualmente, este tipo de antena é utilizado em estações base, com estações remotas colocadas ao seu redor.

Direcional: As antenas direcionais concentram o sinal em uma única direção. Seu sinal pode ter alcance curto e amplo, ou longo e estreito. Via de regra, quanto mais estreito o sinal, maiores distâncias ele alcançará. Normalmente, este tipo de antena é

utilizado em estações remotas para fazer a comunicação entre estas estações com uma ou mais estações base.

3.1.2 Modelos de Antenas

Hoje existem vários modelos de antenas, cada modelo possui uma característica diferente e desenvolvida para situaçõe diferentes. Os modelos mais utilizados são Parabólica, Setorial e Yagi.

Parabólica: As antenas parabólicas canalizam o sinal em forma de cone, sendo indicadas para aplicações de longa distância. A antena semi parabólica, uma variação da parabólica, emite o sinal de forma elíptica. Os modelos *grid* (grelha) são menos susceptíveis a ação dos ventos em razão dos mesmos passarem através da estrutura em forma de gaiola, seu sinal pode chegar de 40 a 50 Km em condições eletricamente visuais. Um exemplo pode ser visto na figura 3.4.

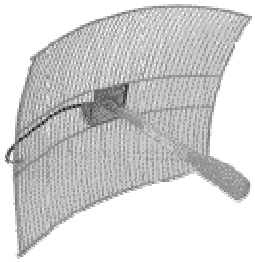

Figura 3.4: Exemplo de Antena Parabólica

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

Setorial: As antenas setoriais têm formato amplo e plano, e são, normalmente, montadas em paredes podendo ser interna ou externa. São mais recomendadas para *links* entre prédios com distâncias de até 8 km. Algumas podem operar até 3 Km dependendo do ganho especifico no projeto. Um exemplo pode ser visto na figura 3.5

Figura 3.5: Exemplo de Antena Setorial

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

Yagi: São antenas rígidas usadas externamente em ambientes de condições hostís. Foram projetadas para resistir a formação de gelo, chuva pesada, neve e ventos fortes. Os sinais podem chegar a 30 Km, em condições eletricamente visual. Um exemplo pode ser visto na figura 3.6.

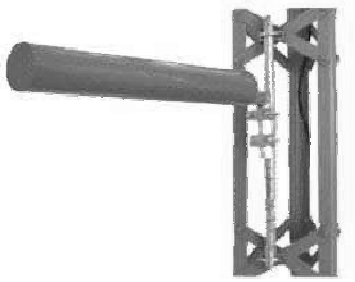

Figura 3.6: Exemplo de Antena Yagi.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

3.2 Ponto de Acesso (*Access Point*)

O *Access Point* é um equipamento com um rádio transmissor/receptor que atua como uma bridge transparente, permitindo a comunicação entre estações wireless e uma estrutura de rede convencional. A figura 3.7 mostra um exemplo de access point.

Figura 3.7: Exemplo de *Access Point*.

(Fonte: www.cisco.com/web/learning/netacad/index.html. Acesso em 10/06/2006)

Deve ser ressaltado que para ligação física dos *Access Point* é necessário a presença de cabos. Um rede sem fio é um segmento de uma rede cabeada, ou seja, trabalha também com cabos para interligação até os ativos de redes gerenciais como concentradores e roteadores.

Este capítulo apresentou os dispositivos utilizados em redes sem fio: antenas, *Access Point*, placas de rede. No próximo capítulo, será abordado as considerações físicas e lógicas para a elaboração do projeto de redes sem fio.

4. TOPOLOGIAS FÍSICA E LÓGICA

Através do estudo da planta do IST, foi possível determinar as distâncias e, conseqüentemente, os locais das instalações de rede, bem como as topologias: física e lógica.

4.1. Planta Baixa do 2° Andar

A planta baixa do 2° andar (Figura 4.0) identifica 3 laboratórios de informática e 9 salas de aula.

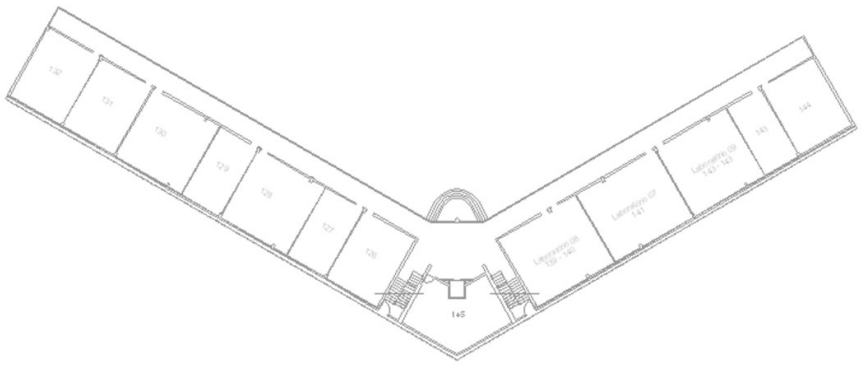

Figura 4.0: Planta Baixa do 2° Andar
(Fonte: Coordenação do IST)

4.2. Planta Baixa do 1° Andar

No 1° andar, é observado que só existem salas de aula (Figura 4.1), totalizando 13 salas.

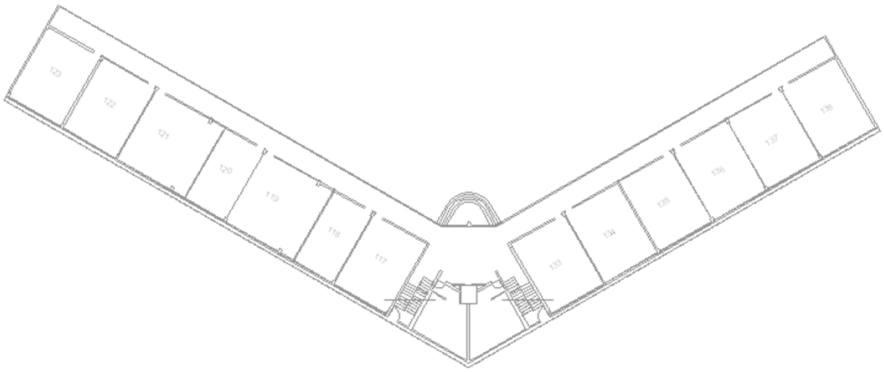

Figura 4.1: Planta Baixa do 1° Andar
(Fonte: Coordenação do IST)

4.3. Planta Baixa do Térreo

No andar térreo (Figura 4.2), têm-se a existência de 20 salas (relativas ao CIEM), a secretaria e o anfiteatro.

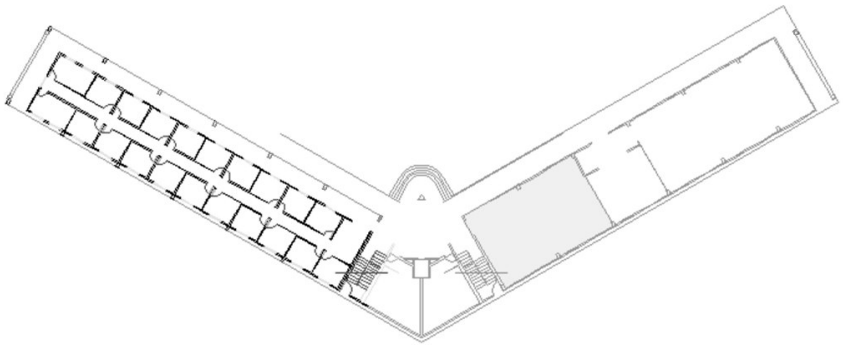

Figura 4.2: Planta Baixa do Térreo
(Fonte: Coordenação do IST)

4.4. Topologia Física do 2° Andar

Através do estudo da planta, definiu-se a IDF (Instalação de Distribuição Intermediária) do 2° andar em uma sala que se localiza no meio do mesmo (Figura 5.4). Isso porque a distância máxima do ponto de rede mais distante até a IDF respeita a distância máxima permitida para o cabeamento UTP CAT6, que é de 100 metros. Além disso, pode-se aproveitar o fosso do elevador para os lances do cabeamento vertical (*backbone*) que saem dessa IDF para a MDF (Instalação de Distribuição Principal) localizada no térreo.

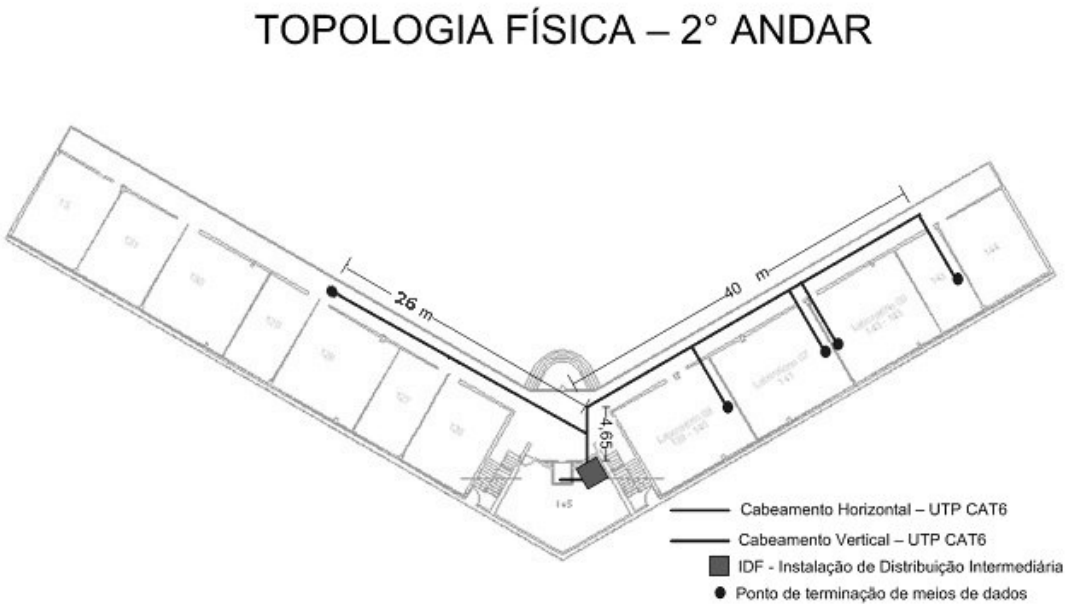

Figura 4.3: Topologia Física do 2° Andar

Nota-se que este andar possui 9 salas de aula e 3 laboratórios. Para uma futura expansão do número de laboratórios, este andar seria o escolhido para receber essa expansão por já possuir esses 3 laboratórios.

4.5. Topologia Física do 1° Andar

Através do estudo da planta, também se definiu a IDF (Instalação de Distribuição Intermediária) do 1° andar em uma sala que se localiza no meio do mesmo (Figura 5.5). Isso porque a distância máxima do ponto de rede mais distante até a IDF respeita a distância máxima permitida para o cabeamento UTP CAT6, que é de 100 metros. Além disso, pode-se aproveitar o fosso do elevador para os lances do cabeamento vertical (*backbone*) que saem dessa IDF para a MDF (Instalação de Distribuição Principal) localizada no térreo.

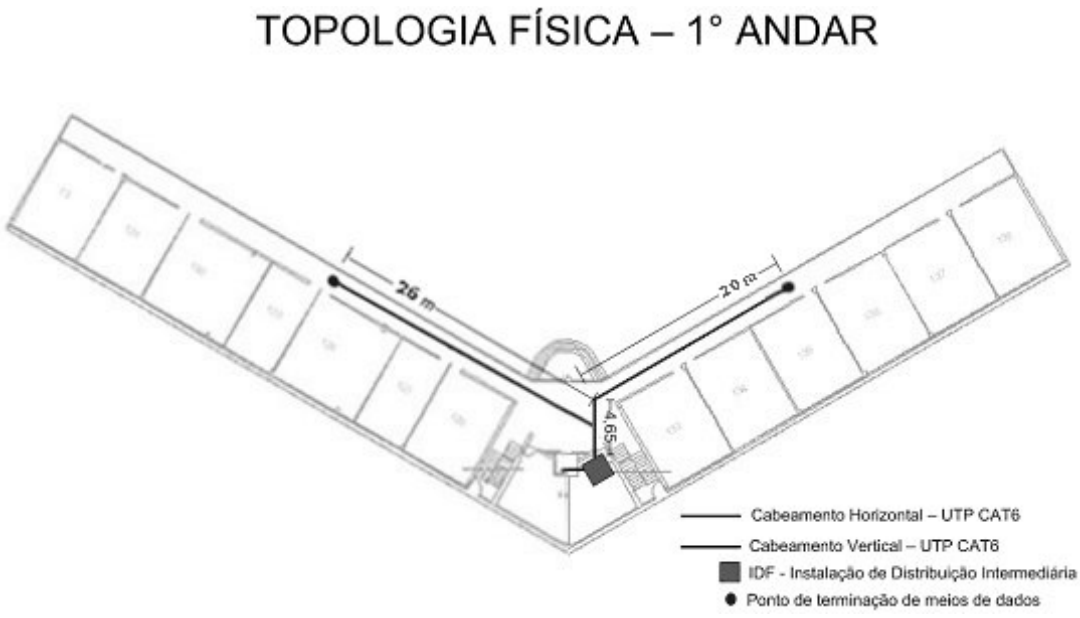

Figura 4.4: Topologia Física do 1° Andar

Nota-se que este andar possui somente salas de aula, totalizando 13 salas.

4.6. Topologia Física do Térreo

Através do estudo da planta, definiu-se uma IDF exclusiva para o CIEM (Centro

Incubador de Empresas de Marília) neste andar (Figura 4.5). Isso ocorreu porque o comprimento máximo do cabeamento proveniente da sala mais distante até a MDF (que serve como uma IDF ao mesmo tempo) extrapolaria as especificações de distância máxima permitida (100 metros). No caso da Secretaria e do Anfiteatro, a MDF serve como uma IDF para os lances de cabo que chegam desses locais.

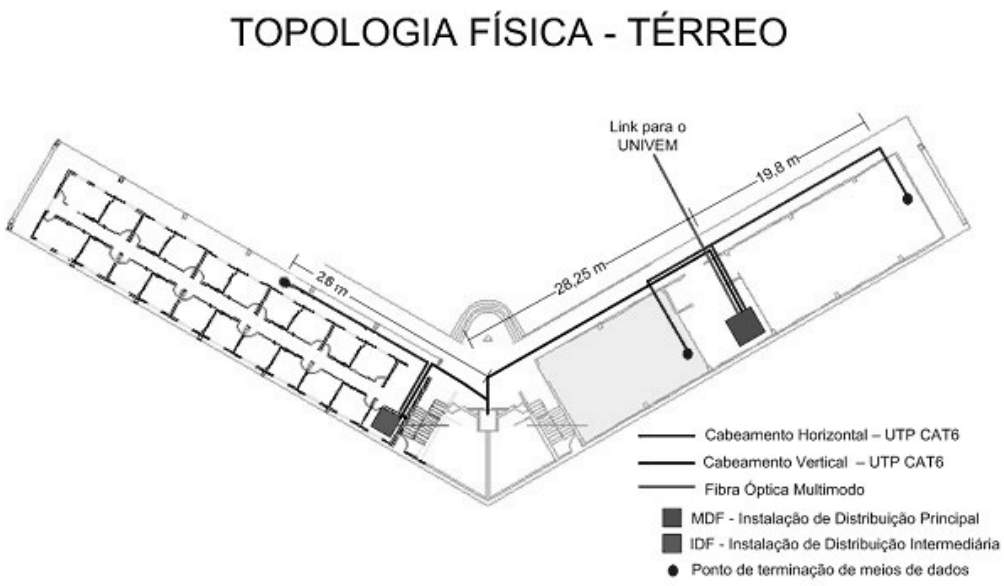

Figura 4.5: Topologia Física do Térreo

Nota-se que o cabeamento vertical (*backbone*) que chega das IDFs do 1° e 2° andar e do CIEM é direcionado para a MDF. A partir da MDF, o cabeamento é interligado ao servidor principal do UNIVEM através de fibra óptica multimodo, pois é o cabeamento recomendado entre prédios. Isso permite um melhor desempenho entre os *links* de Internet da Instituição.

4.7. Topologia Lógica do 2° Andar

No 2° andar, em cada laboratório, existe um *Access Point* que é interligado a IDF

mais próxima através de um cabo UTP CAT6. As salas de aula são alimentadas através de um *Access Point* somente, o qual está localizado em ponto favorável a ter sinal com qualidade alta.

As taxas que devem ser alcançadas são de 54 Mbps para as salas de aula e para o uso interno dos laboratórios, e de 100 Mbps para a interligação dos *Access Point* dos laboratórios com a IDF e da interligação da IDF com a MDF (*backbone*).

4.8. Topologia Lógica do 1° Andar

No 1° andar, nota-se que só existem salas de aula, portanto somente um cabo para alimentar cada *Access Point*.

As taxas são de 54 Mbps para as salas de aula e de 100 Mbps para a interligação do Access Point com a MDF (*backbone*) localizada no Térreo.

4.9. Topologia Lógica do Térreo

No térreo, existe a interligação de todas as IDFs existentes no prédio para a MDF. Os cabos provenientes das IDFs se encontram na MDF com a utilização de 2 switch interligados entre si (do tipo *stackable*), com a carga distribuída entre eles para que não haja um gargalo na rede.

Existe 3 *Access Point* para servir ao CIEM, secretaria e Anfiteatro. Há necessidade de ter independência de *Acces Point* para a secretaria e para o anfiteatro por questões de segurança.

4.10. Topologia Lógica Geral

Para uma melhor visão da topologia lógica, segue abaixo um esquema da topologia lógica geral (Figura 5.10).

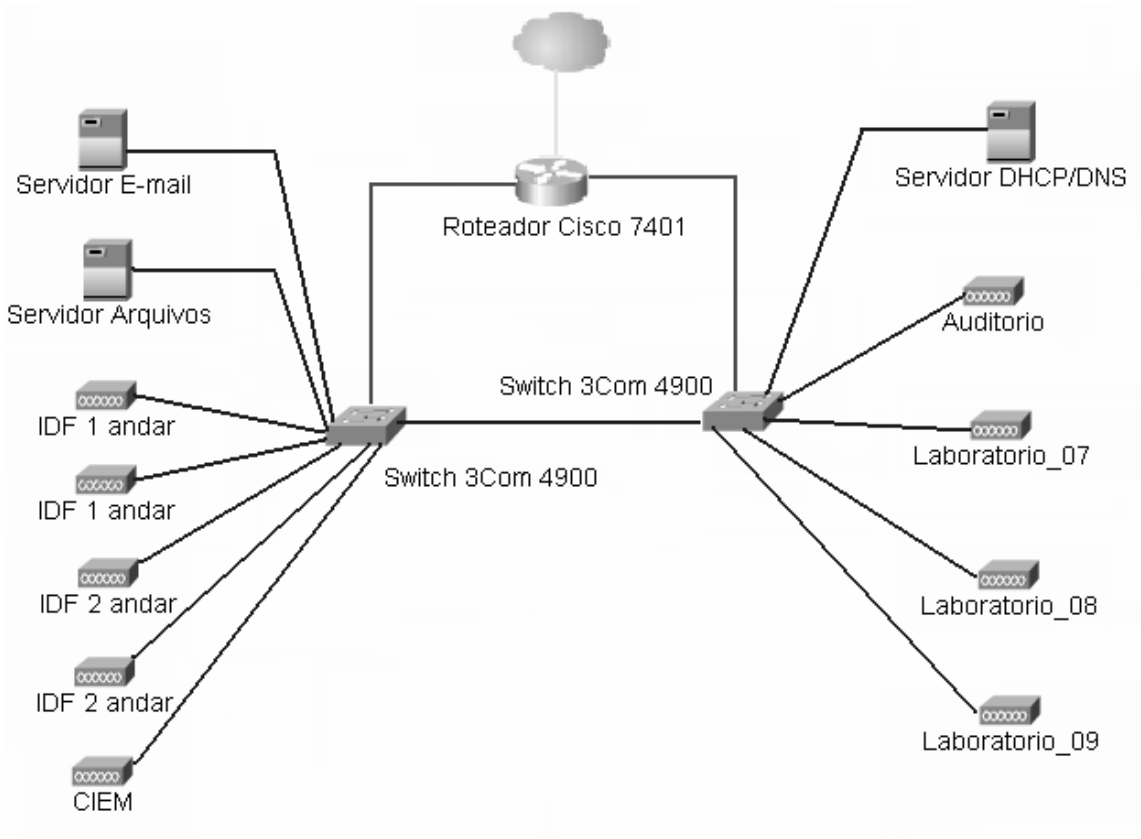

Figura 4.6: Topologia Lógica Geral do Prédio do IST

Este capítulo apresentou a disposição dos *Access Point*, pelo prédio do IST bem como o provável desempenho que a rede instalada possuirá. No próximo capítulo, será abordado os equipamentos utilizados neste projeto de redes sem fio para o IST e seu planejamento de distribuição de ips.

5. INFRA-ESTRUTURA FÍSICA E LÓGICA DE REDE

5.1. Infra-estrutura do 2° Andar

Cabeamento:

- Tipo: UTP CAT6 Furukawa
- Total de cabeamento: aproximadamente 200 metros

Canaleta interna:

- Marca: Pial
- Total: aproximadamente 100 metros

Acces Point dos Laboratórios:

- Quantidade: 3 unidades
- Marca: Cisco
- Modelo: 1240 AG

Acces Point para as salas:

- Quantidade: 1 unidade
- Marca: Cisco
- Modelo: 1240 AG

5.2. Infra-estrutura do 1° Andar

Cabeamento:

- Tipo: UTP CAT6 Furukawa
- Total de cabeamento: aproximadamente 90 metros

Canaleta interna:

- Marca: Pial
- Total: aproximadamente 100 metros

Acces Point para as salas:

- Quantidade: 2 unidades
- Marca: Cisco
- Modelo: 1240 AG

5.3. Infra-estrutura do Térreo

Cabeamento:

- Tipo: UTP CAT6 Furukawa e Fibra Óptica Multimodo Furukawa (somente para o uplink da MDF)
- Total de cabeamento UTP: aproximadamente 300 metros
- Total de fibra óptica: aproximadamente 100 metros.

Canaleta interna:

- Marca: Pial
- Total: aproximadamente 300 metros

Acces Point da Secretaria, Anfiteatro e do CIEM:

- Quantidade: 3 unidades
- Marca: Cisco
- Modelo: 1240 AG

Switches da MDF:

- Quantidade: 2 unidades
- Marca: 3Com
- Modelo: 4900
- Portas: 12 portas 10/100/1000 (RJ-45)

Roteador da MDF:

- Quantidade: 1 unidade
- Marca: Cisco
- Modelo: 7401
- Portas: 2 portas 10/100/1000 (RJ-45) e 1 porta SFP (fibra óptica)

Servidores:

- Quantidade: 3 unidades
- Marca: HP
- Modelo: Proliant ML150
- Características: Controladora Ultra 320 SCSI, Memória 2GB, 2 Placas de Rede 10/100/1000, 2 processadores Intel Xeon 3,0 GHz, 2 HDs de 72 GB Hot Plug , 1 Placa SCSI RAID ML110 - HP

5.4. Equipamentos de Rede

Todos os equipamentos de rede inseridos no projeto (Tabela 5.1) possuem qualidade comprovada pelo mercado. Além disso, possuem as características necessárias para dar suporte às especificações desse projeto.

Tabela 5.1 – Equipamentos de Rede

Equipamento	Marca	Modelo	Características	Local
Roteador	Cisco	7401	2 portas 10/100/1000 RJ-45 1 porta SFP (fibra)	MDF (Térreo)
Switch	3Com	4900	12 portas 10/100/1000 RJ-45 Switch camada 3	MDF (Térreo)
Switch	3Com	4900	12 portas 10/100/1000 RJ-45 Switch camada 3	MDF (Térreo)
Servidor	HP	Proliant ML 150	Controladora: Ultra 320 SCSI Memória: 2GB 2 placas de rede: 10/100/1000 2 processadores Intel Xeon 3,0 2 HDs 72 GB Hot Plug 1 Placa SCSI RAID ML 110 - HP	MDF (Térreo)
Servidor	HP	Proliant ML 150	Controladora: Ultra 320 SCSI Memória: 2GB 2 placas de rede: 10/100/1000 2 processadores Intel Xeon 3,0 2 HDs 72 GB Hot Plug 1 Placa SCSI RAID ML 110 - HP	MDF (Térreo)
Servidor	HP	Proliant ML 150	Controladora: Ultra 320 SCSI Memória: 2GB 2 placas de rede: 10/100/1000 2 processadores Intel Xeon 3,0 2 HDs 72 GB Hot Plug 1 Placa SCSI RAID ML 110 - HP	MDF (Térreo)

5.5. Levantamento de Custos

Tabela 5.2 – Levantamento de Custos

PRODUTO	UNITÁRIO	QUANTIDADE	CUSTO
CABO UTP CAT6 FURUKAWA (Caixa - 300 m)	380,00	3	1.140,00
CANALETA PIAL 50X20X2,20	25,00	170	4.250,00
FIBRA MULTIMODO (2 pares) – 62,5 X 1,25	3,29	100	329
CONECTOR LC	62,42	1	62,42
PATCH PANEL FURUKAWA 24 PORTAS CAT. 6	600,00	2	1200
RACK 8U METÁLICO C/PORTA E CHAVE	330,00	3	990
SERVIDOR PROLIANT ML 150	9.750,00	3	29.250,00
ROTEADOR CISCO 7401	10.000,00	1	10.000,00
Acces Point Aironet 1240 AG	1.400,00	9	12.600,00
SWITCH 3Com 4900	3.050,00	2	6.100,00
		TOTAL	65.921,42

O levantamento de custos do projeto (Tabela 5.2) levou em consideração somente os custos relativos à infra-estrutura, aos equipamentos e ao cabeamento. A mão-de-obra ficou de fora desse levantamento porque é uma medida muito variável, a qual normalmente é medida em percentuais em relação ao valor e tipo de projeto. Somente empresas especializadas na área poderiam definir esse custo com base no projeto elaborado por elas mesmas.

5.6. Segmentação e Endereçamento

A segmentação da rede será feita através da implementação de VLANs. A VLAN1 será destinada à rede administrativa (funcionários e docentes), e a VLAN2 será destinada à rede curricular (alunos). O tráfego da rede curricular será proibido na rede administrativa, salvo as necessidades especiais de acesso.

Para que a segmentação através de VLANs possa ser feita, será necessário configurar e documentar as portas dos switch com suas respectivas VLANs (Tabela 5.3).

Tabela 5.3 – Atribuição de portas a VLANs

Local	Equipamento	Porta	Vlan
Laboratório 7 – 2º andar	*Acces Point Aironet* 1240 AG	Porta1	2
Laboratório 8 – 2º andar	*Acces Point Aironet* 1240 AG	Porta2	2
Laboratório 9 – 2º andar	*Acces Point Aironet* 1240 AG	Porta3	2
IDF – 2º andar	*Acces Point Aironet* 1240 AG	Porta4	2
IDF – 2º andar	*Acces Point Aironet* 1240 AG	Porta5	2
IDF – 1º andar	*Acces Point Aironet* 1240 AG	Porta6	2
IDF – 1º andar	*Acces Point Aironet* 1240 AG	Porta7	2
Secretaria – Térreo	*Acces Point Aironet* 1240 AG	Porta8	1
Ciem – Térreo	*Acces Point Aironet* 1240 AG	Porta9	1
MDF – Térreo	Switch 3Com 4900	Portas 1 a 4	----------
MDF – Térreo	Switch 3Com 4900	Portas 1 a 5	----------

Em relação ao endereçamento, foi definido que um endereço de Classe C é suficiente para as necessidades atuais e para um futuro crescimento do número de estações (Tabela 5.4).

Para o esquema de endereçamento, também foi definido que as estações dos servidores administrativos e do CIEM terão endereços estáticos, e as estações das salas de aula, dos laboratórios e do anfiteatro terão endereços dinâmicos (via DHCP).

Tabela 5.4 – Endereçamento IP

IP	Equipamento	Local
XXX.XXX.XXX.1	ROTEADOR	MDF – Térreo
XXX.XXX.XXX.2	Acces Point Aironet	MDF – Térreo
XXX.XXX.XXX.3	Acces Point Aironet	MDF – Térreo
XXX.XXX.XXX.4	Acces Point Aironet	IDF – 1º andar
XXX.XXX.XXX.5	Acces Point Aironet	IDF – 2º andar
XXX.XXX.XXX.6	Acces Point Aironet	Secretaria – Térreo
XXX.XXX.XXX.7	Acces Point Aironet	Ciem – Térreo
XXX.XXX.XXX.8	Acces Point Aironet	Laboratório 7 – 2º andar
XXX.XXX.XXX.9	Acces Point Aironet	Laboratório 8 – 2º andar
XXX.XXX.XXX.10	Acces Point Aironet	Laboratório 9 – 2º andar
XXX.XXX.XXX.11	SERVIDOR	MDF – Térreo
XXX.XXX.XXX.12	SERVIDOR	MDF – Térreo
XXX.XXX.XXX.13	SERVIDOR	MDF – Térreo
Os endereços de XXX.XXX.XXX.14 até XXX.XXX.XXX.20 ficam como reserva para o futuros equipamentos de rede e servidores		
De XXX.XXX.XXX.21 até XXX.XXX.XXX.40	Estações (Total=20)	Secretaria – Térreo
De XXX.XXX.XXX.41 até XXX.XXX.XXX.80	Estações (Total=40)	Ciem – Térreo
De XXX.XXX.XXX.81 até XXX.XXX.XXX.105	Estações (Total=25)	Salas de aula e anfiteatro
De XXX.XXX.XXX.106 até XXX.XXX.XXX.153	Estações (Total=48)	Laboratório 7 – 2º andar
De XXX.XXX.XXX.154 até XXX.XXX.XXX.201	Estações (Total=48)	Laboratório 8 – 2º andar
De XXX.XXX.XXX.202 até XXX.XXX.XXX.249	Estações (Total=48)	Laboratório 9 – 2º andar
Os endereços de XXX.XXX.XXX.250 até XXX.XXX.XXX.254 ficam como reserva para uma eventual necessidade		

Caso, futuramente, esse número ultrapasse os 254 endereços disponíveis, o administrador da rede deve solicitar outra faixa de endereçamento para suprir essa necessidade.

Este capítulo apresentou o material necessário para a realização do projeto. No próximo capítulo, será abordado a segurança em redes sem fio tendo como relevância o desempenho da rede.

6 SEGURANÇA PARA REDES WLAN

Uma solução de segurança deve levar em consideração o sistema de computação a ser defendido. As soluções “enlatadas”, ou seja, as soluções genéricas que são construídas para serem aplicadas a todas as empresas, não são as melhores. As boas soluções são desenvolvidas especialmente para a empresa alvo. Cada empresa tem a sua forma de trabalhar, tem a sua própria equipe e tem a sua metodologia. Não adianta uma solução que vai obrigar uma equipe a usar uma metodologia de trabalho diferente da que já vem usando há 30 anos. Essa metodologia nova tem muitíssima chance de não ser cumprida na sua totalidade. E, maioria dos casos, uma metodologia que não é cumprida à risca é tão ineficaz quanto não ter metodologia nenhuma.

Agora, deve-se ter em mente que a melhor solução é aquela que é baseada na modelagem de um provável ataque. Deve-se agir como um *hackers*, tendo assim, uma melhor visualização de todas as falhas do sistema da empresa. Considera-se um sistema seguro, o sistema que traz os seguinte benefícios:

- Privacidade
- Autenticação
- Integridade
- Não repúdio
- Controle de Acesso
- Disponibilidade

A privacidade garante que ninguém não autorizado estará “escutando” o que se está transmitindo na rede. A autenticação garante que a origem da mensagem ou do documento eletrônico foi corretamente identificada, com certeza que a identificação não é falsa. A integridade garante que o que foi transmitido não foi alterado, de forma nenhuma, durante a transmissão. Garante que o que o destinatário recebeu foi exatamente o que o remetente enviou. A não-repudiação consiste no fato de requerer que nem o remetente nem o

destinatário de uma mensagem ou de um documento eletrônico sejam capazes de negar a mensagem, nem de negar que tenha sido enviada, nem negar que tenha sido recebida, se realmente isso tenha acontecido. O Controle de Acesso requer que acesso à informação possa ser controlado pela rede que contenha a informação. Quando se quer dar acesso somente de leitura a um arquivo, tem que se garantir que o leitor não pode, de modo algum, alterar o conteúdo do que está sendo exibido. E finalmente, a disponibilidade requer que o sistema de computadores esteja disponível para qualquer pessoa autorizada em qualquer momento que ela deseje.

6.1 Tipos de Intruso

A tabela 6.1 mostra os tipos de intrusos

Tabela 6.1 – Exemplos dos objetivos de alguns intrusos.

Intruso	Objetivos
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas.
Hacker/Cracker	Testar o sistema de segurança de alguém; ou roubar dados.
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se do ex-empregador
Contador	Desfalcar dinheiro de uma empresa
Vigarista	Roubar números de cartões de créditos e revendê-los
Espião	Descobrir a força militar do inimigo
Terrorista	Roubar segredos de guerra bacteriológica
Representante de vendas	Tentar representar toda a Europa e não apenas a América
Corretor de valores	Causar prejuízo para lucrar no valor das ações

Fonte Tanenbaum, (1997, p.658).

6.1.1 *Hackers X Crackers*

Para facilitar a exposição a seguir, deve-se diferenciar os *hackers* dos *crackers*, mas deixando claro que um sistema de segurança deve prevenir contra o ataque dos dois.

A mídia, pelo menos a mais leiga, utiliza-se o termo *hacker* para o uso geral. Não tiro sua razão, pois todo *cracker* é um *hacker*. O problema é que nem todo o *hacker* é um *cracker*, ou seja, nem todo mundo que tem o conhecimento para tentar invadir um sistema de redes, é a pessoa que invade e comete crimes.

O termo *cracker* não é muito utilizado aqui no Brasil, talvez por não ser difundido pela mídia, mas talvez por ser confundido com a designação craque, que é dada ao excepcional esportista de um time ou seleção, quase sempre de futebol, ou talvez por receio de ligar o termo *cracker* ao consumidor da droga feita de cocaína.

6.1.2 Ataques

O intruso pode ter quatro comportamentos diferentes em relação às posições da origem e do destino da mensagem. Na figura 6.1, têm-se esses comportamentos:

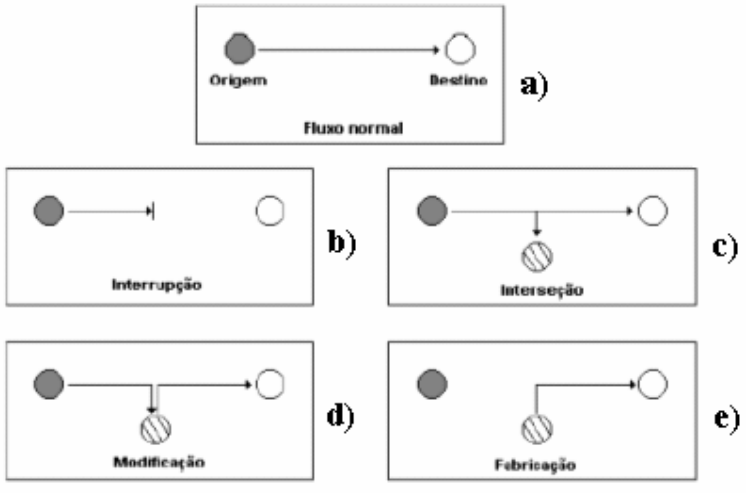

Figura 6.1: Posição do atacante em relação à origem e ao destino

- **Interrupção:** O intruso objetiva interromper o fluxo de dados que parte da origem, deixando o dispositivo destino sem receber pacotes.

- **Interseção:** Nesse tipo de invasão o intruso objetiva apenas tomar conhecimento de todo fluxo de dados que trafega por essa conexão.
- **Modificação:** Aqui, o intruso além de escutar o tráfego, intercepta os dados e os modifica, enviando-os para o destino.
- **Fabricação:** O intruso fabrica dados para enviar para o destino. O dispositivo destino não tem como saber quem está enviando esses dados.

6.1.3 O elo mais fraco

O elo mais fraco de um sistema de segurança é o ser humano. Não tem como se controlar o comportamento de um ser humano. A seguir será abordado a questão da engenharia social, uma técnica utilizada pelo *hacker* para descobrir as informações necessárias a um ataque.

É comum ouvir os especialistas dizerem que o único sistema 100% seguro é aquele que fica o tempo todo desligado. Ora, como um intruso pode invadir um computador desligado? Simples, ele pode pedir para alguém ligar o sistema. Pedir a alguém alguma coisa é uma das ferramentas da Engenharia Social.

6.1.4 Engenharia Social

O termo engenharia social foi dado ao grupo de procedimentos que se toma para convencer alguém a tomar atitudes que não pode, ou não quer tomar.

A engenharia social é considerada um tipo de ataque a uma rede. Em última instância, pode-se convencer o faxineiro de jogar um balde com água sobre o servidor de e-mail, na hora em que ninguém esteja olhando. Ou seja, *em última instância*. É lógico que foi colocado um caso extremo, considera-se que todo faxineiro sabe que circuitos eletrônicos não funcionam bem quando estão submersos, porém existem ataques mais brandos que são facilmente encontrados por aí.

O mais comum é o intruso, antes de tentar uma invasão, querer saber se a rede tem um *firewall*, qual é esse *firewall*, qual o sistema operacional que roda no roteador, qual o nome, ou o número IP de alguma máquina específica, por exemplo, o servidor de banco de dados. Essas são algumas das informações muito úteis que um intruso pode querer saber antes de um ataque.

Para saber o nome e o telefone do administrador da rede alvo do ataque, pessoa que certamente terá os dados que o atacante quer saber, basta dar uma olhada na Internet. Provavelmente esses dados estão na Home Page da empresa que contém a rede. Outro lugar de consulta pode ser a página do Registro.BR.

O Registro.BR é a entidade que controla o registro de nomes de domínios na Internet no Brasil. É lá que você registra que o nome xxxx.com.br corresponde à rede 999.999.999.0. Ao registrar essa informação, o administrador da rede deve registrar também alguns de seus dados pessoais. Na maioria esmagadora dos casos, os dados ali registrados são verídicos, mesmo porque, o serviço de registro de nome de domínio é cobrado por essa entidade (Registro.BR), e ela precisa saber os dados para onde mandar a fatura. Caso os dados estejam errados, a entidade registradora não faturará o serviço e, automaticamente, removerá o registro. Logo, salvo os registros falsos, todos os administradores cadastram seus verdadeiros dados.

Existirá uma possibilidade de, se você telefonar para o administrador, não o encontrar, e em seu lugar, encontrar o seu estagiário. O intruso pode usar de toda a sua

malícia contra o estagiário, que na maioria das vezes, é uma pessoa jovem, sem experiência, e doido para mostrar serviço ao chefe. O intruso liga identificando-se como algum controlador de tráfego do *backbone* ou de algum órgão do governo, lamenta-se por não encontrar o administrador, e duvida da capacidade do estagiário de lhe dar informações tão específicas, ou seja, desafia o estagiário a mostrar a sua capacidade de dar as informações. Na sua ingenuidade, o estagiário dará todas as informações que ele puder para provar que é capaz, acreditando, assim, ter feito um bom trabalho. Terminará o telefonema feliz, por ter conseguido prestar um bom serviço ao chefe, e deixará o intruso ainda mais contente.

6.1.5 Ex-funcionários

Uma atenção especial deve ser dada à ex-funcionários que saíram contrariados da empresa. Não há como remover os conhecimentos específicos da empresa que foram dados ao ex-funcionário, durante o tempo que ele serviu a essa empresa. Em julho de 2001, o portal de segurança da COPPE/UFRJ, o *Lockabit*, publicou um artigo sobre esse assunto, onde fala-se sobre a atenção especial que deve ser dado às informações que são dadas aos funcionários.

6.1.6 Footprint

Vão existir informações que o intruso não conseguirá coletar através de um telefonema ou um papo amigável com alguma secretária ou estagiário. Seja porque essas pessoas não detêm os conhecimentos necessários, seja porque ele não consegue ter acesso a essas pessoas ingênuas.

Aí, então, surge a segunda técnica de intrusão, conhecida como *footprint*. Consiste em, através de *softwares* específicos, conseguir informações necessárias ao ataque.

Footprint é um perfil completo da postura de segurança de uma organização que se pretende invadir. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido e convertê-lo em um conjunto específico de nomes de domínio, blocos de rede e endereços IP individuais de sistemas conectados diretamente à Internet. Embora haja diversas técnicas diferentes de *footprint*, seu objetivo primário é descobrir informações relacionadas a tecnologias de Internet, acesso remoto e extranet. A Tabela 6.2 mostra essas tecnologias e informações críticas que um atacante tentará identificar.

Tabela 6.2 – Tipos de informações procurados num footprint.

Tecnologia	***Identifica***
Internet / Intranet	Protocolos de rede em uso (por exemplo: IP, IPX, DexNET etc)
	Nomes de domínio.
	Blocos de rede.
	Endereços IP específicos de sistemas atingíveis via Internet
	Serviços TCP e UDP executados em cada sistema identificado.
	Arquitetura do sistema (por exemplo, SPARC versus X86).
	Mecanismos de controle de acesso e listas de controle de acesso (ACLs, acess control lists) relacionadas.
	Sistemas de detecção de intrusos (IDSs).
	Enumeração de sistemas (nomes de usuários e de grupos, faixas de sistemas, tabelas de roteamento, informações de SNMP).
Acesso remoto	Número de telefone analógicos/digitais.
	Tipo de acesso remoto.
	Mecanismo de autenticação.
Extranet	Origem e destino de conexões.
	Tipos de conexão.
	Mecanismos de controle de acesso.

6.1.7 Personificação

Um dos problemas que o intruso encontra quando quer entrar sem permissão em um sistema é a falta de direitos de acesso, e a maneira mais fácil de resolver esse problema é se fazer passar por um outro elemento que tem direitos de acesso ao objeto que o intruso quer invadir.

Depois do *footprint* quase sempre o intruso consegue elementos que identifiquem as pessoas que têm acesso ao objeto alvo. Daí, basta configurar o computador dele com o *login*, nome, número IP que ele deseja personificar.

6.1.8 Replay

No *replay* o intruso intercepta um pacote que vem de um usuário autenticado e reenvia-o novamente mais tarde, visando confundir os sistemas, ou causando uma parada do sistema. O sistema que está recebendo os pacotes vai ingenuamente receber os pacotes reenviados pelo intruso, acreditando que ele fora enviado pelo dispositivo origem. Como este pacote já foi recebido anteriormente ele será colocado na fila para aguardas os demais, com isso o sistemas faz a solicitação dos outros ao dispositivo de origem provocando uma sobrecarga de processamento.

6.1.9 Recusa ou impedimento de serviço

Recusa ou impedimento de serviço, cujo nome em inglês é *Deny of Service (DoS)*, é um ataque muito comum encontrado hoje. Esse ataque consiste no envio de muitos pacotes pelo intruso para um computador. Esse envio torna-se perigoso quando o número de pacotes é

muito maior do que a quantidade que o computador atacado pode tratar. Uma variação mais perigosa é o Impedimento de Serviço Distribuído. Aqui o intruso utiliza-se de outros computadores, conhecidos como computadores zumbis, para aumentar a carga de pacotes (*flood*) a serem tratados pelo computador atacado.

6.1.10 Armadilhas

Também conhecido como *trapdoor* ou *backdoor*. Ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando (emitido pelo intruso) ou a um evento predeterminado.

Como exemplo, pode ser citado a modificação de um processo para dispensar a verificação de senha na autenticação de um acesso, em resposta a uma combinação de teclas (Ctrl+Alt+U) ou a um evento do tipo "hora do sistema = 2:35:00" quando o acesso a qualquer usuário teria a necessidade de senha para autenticação dispensada.

6.1.11 *Script Kiddies*

Há um tipo de intruso que traz muito perigo, não por causa de seus conhecimentos avançados, mas por causa da sua aleatoriedade. Os usuários dos *script kiddies* quase todos são *hackers* iniciantes (algumas vezes, crianças, daí o nome), não tendo ainda conhecimento e experiência suficiente para fazer os seus próprios ataques, e por isso utilizam *scripts* feitos por outros *hackers*.

O principal é que um *hacker* experiente escolhe as suas vítimas, normalmente são empresas grandes e importantes que estão mais expostos ao grande público, os *scripts kiddies* escolhem suas vítimas ao acaso.

6.2 WEP

As redes sem fio, como a IEEE 802.11b, possuem um conjunto adicional de elementos de segurança, chamado WEP, que não está disponível no mundo cabeado.

O WEP foi construído originalmente para atender as seguintes necessidades:

- **Grande confiabilidade**
- **Autosincronização:** Os clientes saem freqüentemente da área de cobertura.
- **Eficiência computacional:** O WEP foi construído para funcionar tanto em *hardware* quanto em *software*.
- **Exportabilidade:** Ele pode ser usado tanto nos padrões Americanos, quanto no dos outros países.
- **Opcionalidade:** O WEP não deve ser de uso obrigatório para manter compatibilidades com outros padrões.

O WEP utiliza a mesma chave para encriptar e desencriptar os pacotes. O funcionamento do algoritmo de encriptação do WEP pode ser visto na figura 6.2:

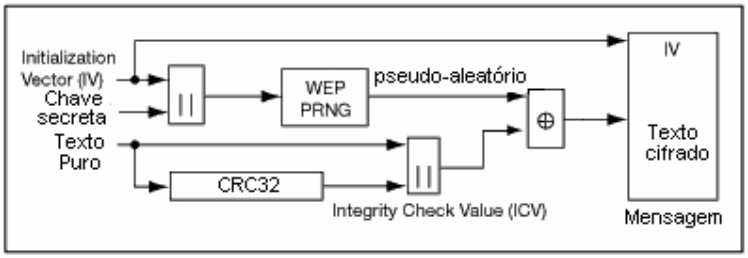

Figura 6.2: Esquema do WEP.

Dois processos são aplicados sobre o texto puro. Um deles é o processo de encriptação e o outro é um processo que visa proteger uma alteração não autorizada no texto durante a transmissão.

A chave secreta tem 40 *bits* e é concatenada com um Vetor de Inicialização (IV) de 24 *bits*, formando a chave composta que será responsável por chegar a *string* pseudo-aleatória de bits. A chave composta é inserida no algoritmo de PRNG (*Pseudo-random Number Generator*). O PRNG é baseado no algoritmo RC4 (*Ron's Cipher 4*). A saída do algoritmo PRNG é uma seqüência pseudo-aleatória de bits, baseada na chave composta. Esta saída é utilizada para encriptar o texto puro através de uma operação binária de XOR. O resultado da encriptação é exatamente do tamanho do texto puro. A este resultado é concatenado, no início do pacote, o vetor de inicialização, e no final do pacote, 4 *bytes* (32 *bits*) resultado de um processo de ICV (*integrity check value*). O algoritmo de ICV é o CRC32. Esse conjunto, texto encriptado, IV e ICV são enviados pelo canal inseguro. O CRC32 é utilizado para proteger os dados contra uma modificação não autorizada.

A estação destino, que de antemão já sabe o valor da chave secreta, usa o IV que vem no inicio do pacote para criar a mesma string gerada pelo PRNG e desencriptar o texto cifrado. Então ele roda o CRC32 sobre esse texto desencriptado e recebe um novo valor de ICV. Ele compara esse novo valor de ICV com o valor que veio no final do pacote transmitido. Se os valores forem diferentes, o pacote é descartado, pois se tem certeza que a sua integridade foi quebrada.

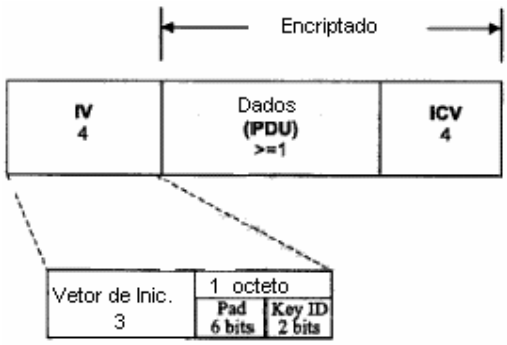

Figura 6.3: Esquema do pacote cifrado que é transmitido pelo canal inseguro.

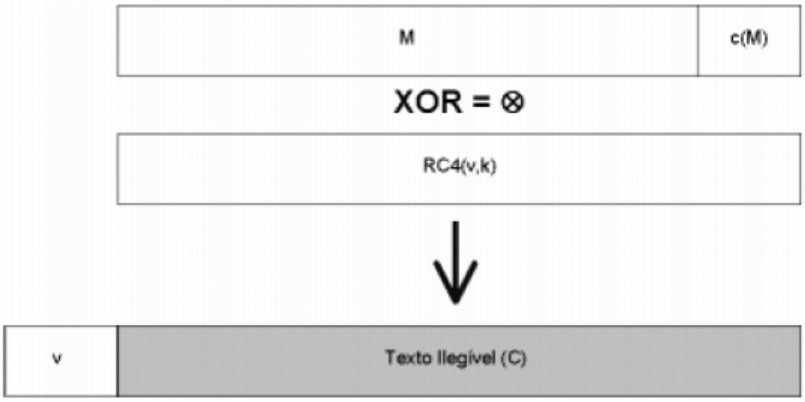

Figura 6.4: Operação lógica de Ou-exclusivo para encriptação.

No WEP, a mesma chave que é utilizada para encriptar e desencriptar é também utilizada para autenticar uma estação. Ter a mesma chave para encriptar e autenticar é considerado um risco de segurança. Existe também um método onde as estações que o ponto de acesso pode utilizar o WEP sozinho sem compartilhar a autenticação de chaves, essencialmente utilizando o WEP como encriptador.

Então, existe dois tipos de autenticação no IEEE 802.11:

- *Open system authentication*: Esse é o serviço de autenticação padrão. Não possui autenticação.

- *Shared key authentication:* Envolve uma chave secreta compartilhada para autenticar a estação a ponto de acesso.

Na *open system authentication* a estação pode associar com qualquer ponto de acesso e escutar todos os dados que são enviados sem encriptação. Isso é usado se a facilidade de conexão é o principal objetivo que o administrador e não está preocupado com segurança.

A *shared key authentication* provê um nível mais alto de autenticação. A chave secreta reside em cada estação. O protocolo 802.11 não especifica como se distribui as chaves entre as estações.

O PRNG (RC4) é o componente mais crítico do processo WEP, já que é o real responsável pela encriptação. O vetor de inicialização estende a vida da chave secreta e provê a auto-sincronização do algoritmo. A chave secreta continua constante e o IV se altera periodicamente. O IV pode variar a cada envio de pacote.

6.3 CISCO – WEP

6.3.0 Autenticação Mútua

Os produtos Cisco para redes sem fio, conhecidos como *Cisco Aironet Wireless* oferecem um serviço de autenticação mútua. Isso consiste no ato da autenticação do cliente no ponto de acesso e o ponto de acesso no cliente. A Cisco criou o protocolo de autenticação EAP para assegurar a autenticação mútua entre o cliente e o servidor RADIUS (*Access Control Server 2000 v.2.6*)

6.3.1 Derivação da chave secreta

Originalmente o WEP utiliza a chave secreta para encriptar e desencriptar, e também para a autenticação. Os produtos Cisco não utilizam a chave secreta para autenticar, ao invés disso, eles utilizam uma chave derivada para essa mútua autenticação.

6.3.2 Chaves do WEP escolhidas dinamicamente

Como exposto anteriormente, a chave do WEP costuma ser fixa, seja porque não é política da empresa trocar essas chaves, ou seja, porque o usuário é remoto e não tem

conhecimento para trocar essa senha, sem auxílio do administrador. A Cisco oferece em seus produtos um sistema para troca das chaves a cada novo usuário e a cada nova conexão. Se o mesmo usuário tentar fazer uma nova conexão este receberá uma nova chave secreta.

Assim, a Cisco impede ou dificulta que o invasor fique escutando *strings* aleatórias geradas pela mesma chave por muito tempo.

6.3.3 Política de reautenticação

A política de reautenticação consiste em forçar o usuário depois de um certo tempo, a fazer uma nova autenticação, e a nova autenticação determinará uma nova chave secreta, assim, mesmo que não se troque usuário e nem se troque uma sessão (como num processo de FTP), o cliente será obrigado a encriptar e desencriptar com outra chave secreta.

6.3.4 Alteração do Vetor de Inicialização

Como todas as implementações, os produtos da Cisco também incrementam o Vetor de Inicialização a cada pacote enviado. A diferença é que o vetor de inicialização começará a cada sessão a contagem a partir de um número escolhido aleatoriamente e não do zero como é em outras implementações.

6.4 IP Security

Uma das melhores soluções é o IP Seguro. Entre as principais vantagens desta solução está o fato de que ela é transparente para a camada de aplicação e para o usuário.

Fazendo com que, desta forma, não haja necessidade de alterar código de aplicações nem tão pouco seja preciso treinamento extra para os usuários.

6.4.1 Aspectos gerais do IPSec

O IPSec foi desenvolvido pelo IETF (*Internet Enginee-ring Task Force*). Ele pretende substituir as vulnerabilida-des do TCP/IP através da especificação dos seguintes serviços de segurança:

1. Controle de acesso
2. Integridade de pacotes
3. Autenticação da origem
4. Privacidade dos pacotes
5. Privacidade em f luxo de pacotes
6. Proteção de replays

O IPSec é de uso mandatário no IPV6.

6.4.2 Componentes do IPSec

O IPSec é composto por protocolos que são executados pelos nós da rede que se utilizam de seus serviços de segurança. Existem 3 protocolos:

- AH (*Authentication Header*)
- ESP (*Encapsulating Security Payload*)
- IKE (*Internet Key Exchange*)

O AH é o responsável pela autenticação, garantia de integridade e o combate ao *replay*. O ESP provê os serviços de criptografia e, opcionalmente, autenticação e anti-replay.

O IKE é um protocolo híbrido, formado pelo ISAKMP (*Inter-net Key Management Protocol*) e pelo Oakley, e ele é responsável por gerar um meio seguro para que haja a troca de chaves na rede.

A operação de aplicar um determinado algoritmo de criptografia num pacote é chamada no IPSec de transformação. Durante a configuração de uma conexão que usa o IPSec para comunicar pode-se definir uma ou mais transformações.

Todo o tráfego de uma comunicação via IPSec é executado sob o domínio de uma *Security Association* (SA) que é uma entidade *peer-to-peer* e *simplex* responsável por todas as informações de controle da sessão IPSec entre dois nós.

Por fim, têm-se os nós propriamente ditos que são os reais responsáveis pela inserção e/ou encaminhamento dos pacotes na rede. São eles que executam o *software / hardware* que implementa o IPSec. Existem dois tipos de nós: os *Security Gateway* (SG) e os *End Station IPSec*. Os SG disponibilizam os serviços de segurança para toda a rede (roteadores ou *firewalls*), enquanto os *End Station* fazem a segurança fim-a-fim entre os parceiros.

Para seu funcionamento o IPSec define várias estruturas de dados que são armazenadas em cada nó da rede que execute o IPSec. Este conjunto de dados forma dois bancos de dados a saber: O SPD (*Security Policy Database*) e o SAD (*Security Association Database*).

O SPD é composto por um conjunto de regras que determinam como processar os pacotes que chegam numa interface.

O SAD é composto por uma ou mais SA e armazena os parâmetros de cada uma delas. Ele é um banco de dados dinâmico, ou seja, suas entradas são excluídas após o término da SA correspondente.

Uma SA identifica somente uma associação unidirecional entre dois nós com IPSec. Se a comunicação entre os dois nós for bilateral haverá duas SAs, uma de ida e outra de volta.

Podem ter várias SAs entre dois nós. Numa mesma SA trafega somente um protocolo: AH ou ESP.

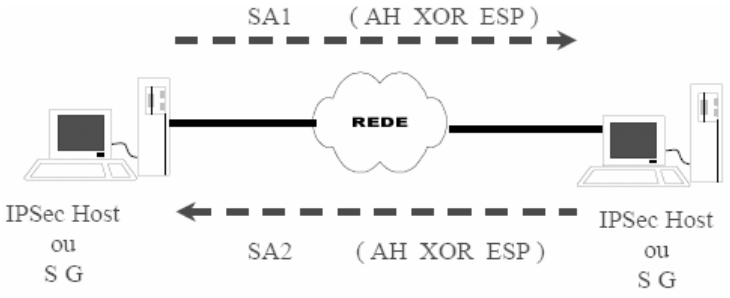

Figura 6.5: Sas entre dois nós de rede.

A SA é uma estrutura dinâmica e somente existe enquanto houver aquela conexão. As SAs podem trabalhar em dois modos: Transporte e Túnel. O modo transporte é usado para prover segurança para comunicações fim-a-fim (cliente/servidor, duas estações de trabalho ou console de gerenciamento/dispositivo gerenciado). Nesse caso, o escopo de proteção do pacote restringe-se ao *payload* do IP (segmento TCP ou UDP e pacote ICMP).

O modo túnel é usado para prover segurança para comunicações entre redes ou entre uma estação e uma rede (tipicamente aplicações VPN). Aqui o escopo de proteção é todo o pacote IP. Um novo cabeçalho é gerado e o cabeçalho original é incluso no payload do novo cabeçalho IP. O modo túnel é mandatário se uma das extremidades da conexão foi um SG.

A encriptação no ESP nunca segue um único algoritmo de criptografia (DES, RC5, IDEA, CAST, *Blowfish*). A variação é mais um modo de garantir segurança. Essa variação também é aleatória.

6.4.3 Desempenho

Logicamente com o IPSec o desempenho da comunicação cai um pouco. A fragmentação dos pacotes no IPSec tende a aumentar, pois haverá adição de cabeçalhos maiores do que no IP.

Como solução para os problemas de desempenho com redes em IPSec adota-se os seguintes procedimentos:

- Aumentar o poder de processamento de SG e *Hosts*;
- Realizar a compressão do IP *payload* através do protocolo IPPCP (*IP Payload Compression Protocol*);
- Realizar a criptografia e descriptografia em *hardware* específico.

6.5 Virtual Privacy Networks

Uma das melhores aplicações do IPSec são as VPNs. Na verdade VPN é um termo genérico para qualquer tecnologia que garanta comunicação segura sobre a internet pública.

A idéia da VPN é criar um túnel seguro entre os gateways para proteger os dados privados enquanto eles estão navegando pela internet, ou seja, enquanto eles estão trafegando por redes não confiáveis.

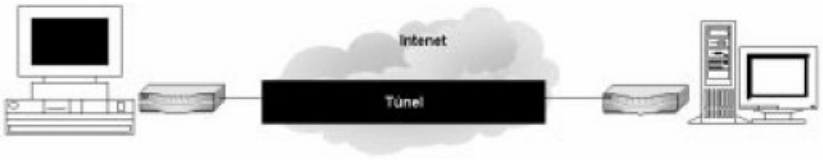

Figura 6.6: Exemplo de uma VPN que liga dois roteadores.

Dentro do túnel, todos os dados, incluindo os cabeçalhos, são encriptados. A forma como esses dados serão encriptados, quais os algoritmos de encriptação e autenticação serão utilizados, dependerá do protocolo sobre o qual a VPN está se baseando. O IPSec não é a única solução para uma VPN, existe um protocolo chamado PPTP que também se presta para esse fim com muita qualidade.

As VPNs não servem somente para ligar gateways, elas também podem conectar dispositivos às redes. A seguir têm-se os tipos de conexões que são suportadas pela VPN:

- **Cliente-Rede**: É quando um dispositivo isolado quer se conectar a uma rede. É utilizado por trabalhadores que não trabalham em um lugar fixo e necessitam de mobilidade. Se um vendedor está hospedado num hotel em outra cidade distante da sede da sua empresa e necessita fazer um *upload* da base de novos clientes com segurança ele pode fazer uma conexão local, na cidade onde se encontra, e utilizar a internet pública para chegar até os servidores da sua empresa. A VPN faz com que o trajeto do hotel até a empresa seja um túnel inviolável.

- **Rede-Rede:** A VPN é utilizada para unir duas redes. Independente da distância, há casos em que você precisa ligar dois escritórios. Normalmente essa conexão é feita através da rede de telefonia pública. A VPN faz com que haja segurança entre os dois roteadores.

- **Intranet:** Aqui a VPN é utilizada para que informações que são exclusivas de um ou mais departamentos, não seja acessadas por toda a empresa.

- **Extranet:** A VPN é utilizada para assegurar que as informações serão vistas somente pelos clientes e/ou fornecedores.

7. CONSIDERAÇÕES FINAIS

Nessa monografia foi apresentada uma proposta de projeto para a rede local do Instituto Superior de Tecnologia utilizando a tecnologia sem fio. Anteriormente havia sido apresentada proposta de projeto para a rede local do Instituto Superior de Tecnologia utilizando a tecnologia cabeada. A tecnologia cabeada além de ter um custo agregado superior também demanda maior tempo de instalação, configuração e manutenção além de não promover a mobilidade.

Tendo como ponto forte o desempenho as redes cabeadas, ainda tem sido optadas por sua maior largura de banda necessária em algumas aplicações. Já em redes sem fio a largura de banda pode ser resolvida através do acréscimo de um numero maior de *Access Point* a mesma célula de abrangência do AP.

A opção por uma arquitetura com mobilidade, menor custo agregado e também maior versatilidade, frente ao ambiente estático das redes cabeadas fazem com que as redes sem fio sejam a melhor opção para a implantação em um ambiente acadêmico onde existe a demanda de constante atualizações de equipamentos e *layouts* para a disposição das salas.

8. PROPOSTA DE TRABALHOS FUTUROS

Como sugestão para a continuidade deste projeto, pode-se fazer um levantamento para implantar a tecnologia *wireless* em todos os Laboratórios do Centro Universitário e também suas dependências de convívio comum. Este levantamento envolveria, equipamentos a serem usados, distribuição lógica das redes e também levantamento de custo. Sua realização se justificaria ao se pensar em uma proposta de reestruturação dos Laboratórios didáticos passando de uma forma de *layout* estático para uma forma de *layout* dinâmico facilitando a adequação de diferentes turmas nos mesmos.

9. CONCLUSÃO

Nessa monografia foi apresentada uma proposta de projeto para a rede local do Instituto Superior de Tecnologia utilizando a tecnologia sem fio. Como decorrência da experiência de desenvolvimento desse projeto de rede, foi possível comparar equipamentos e métodos de implantação de uma rede sem fio.

Ao longo do desenvolvimento, ficou constatado que, as definições dos equipamentos a serem utilizados devem ser realizadas através de um planejamento minucioso, pois afetará a rede atual, bem como de sua possível expansão de quantidade de usuários bem como de *layout*.

Uma das dificuldades relativas ao desenvolvimento do projeto foi a falta de equipamentos para a realização do *site survey*. Isto dificulta pontos importantes para precisar o posicionamento dos Access Point, como também a sobreposição de células para se obter comunicação continua.

Em relação aos benefícios, considerando que fosse realizada a implantação do projeto, a instituição disponibilizaria um conjunto de serviços (Internet, Intranet, E-mail e FTP) e também uma mobilidade de computadores acarretando em uma ferramenta para levar a informação de forma mais fácil e ágil.

REFERÊNCIAS BIBLIOGRÁFICAS

BREEZECOM. IEEE 802.11 Technical Tutorial. Disponível na Internet.http://www.sss-mag.com/pdf/802_11tut.pdf. 05/04/2006.

BUDRI, Amaury, BONILHA, Caio. WLAN: Arquitetura da Rede WLAN IEEE 802.11. Disponível na Internet. http://www.teleco.com.br/tutoriais/tutorialwlan/pagina_3.asp 26/05/2006.

COMMSDESIGN. IEEE 802.11g Jells As Applications Mount. Disponível na Internet. http://www.commsdesign.com/csdmag/sections/feature_article/OEG20020402S0034. 12/05/2006.

CISCO SYSTEMS, Inc. *Programa da Cisco Networking Academy: CCNA*. Disponível em: <http://www.cisco.com/web/learning/netacad/index.html>. Acessado em: 14 de novembro 2006.

COMER, Douglas E. *Interligação em Rede com TCP / IP: Volume I*. Rio de Janeiro: Campus, 1998.

FORTES, Débora. Coleção INFO 2005, WI-FI. Ed. Abril 2005

GAST, Matthew. 802.11 *Wireless Networks: The Definitive Guide*. Ed. Sebastopol, CA, USA: O'reilly, 2002.

IEEE, Conselho Brasil Disponível na Internet em 02/03/2006 http://www.ieee.org.br

JUNIOR, Aurélio Amodei. Esquemas de Modulação do IEEE 802.11. Disponível na Internet. http://www.gta.ufrj.br/seminarios/semin2003_1/aurelio/. 17/04/2006

MATHIAS, André Pimenta. IEEE 802.11 – Redes Sem Fio. Disponível na Internet. www.gta.ufrj.br/grad/00_2/ieee/ . 28/04/2006.

MENEZES, Rodrigo Saldanha de. IEEE 802.11 – Wireless. Disponível na Internet. http://www.gta.ufrj.br/grad/98_2/rodrigo/trabalho.html. 13/04/2006

OFDM. Disponível na Internet em 01/06/2006. http://www.inatel.br/revista/volume-05-n1/artigos/Artigo_Transmissao_OFDM.pdf

PINTO, Ernesto Leite, ALBUQUERQUE, Cláudio Penedo de. A Técnica de Transmissão

SOARES, Luiz Fernando Gomes et al. *Redes de Computadores: das LANs, MANs e WANs às Redes ATM*. Rio de Janeiro: Campus, 1995.

TANENBAUM, Andrew S. *Redes de Computadores*. Rio de Janeiro: Campus, 1997.

TORRES, Gabriel. *Redes de Computadores: Curso Completo*. Rio de Janeiro: Axcel Books, 2001.

ZANNETI, Alberto René, GONÇALVES, Leandro de Carvalho. Redes Locais Sem Fio. Disponível na Internet. http://www.dc.ufscar.br/~carvalho/WLAN/index.html. 22/08/2006.

ZYREN, Jim. IEEE 802.11g Offers Higher Data Rates and Longer Rates. Disponível naInternet. http://cnscenter.future.co.kr/resource/rsc-center/vendor-wp/intersil/WP0555.pdf 03/10/2006.